Chapter 8

Introducing Algebraic Geometry

(Commutative Algebra 2)

We will develop enough geometry to allow an appreciation of the Hilbert Nullstellensatz, and look at some techniques of commutative algebra that have geometric significance. As in Chapter 7, unless otherwise specified, all rings will be assumed commutative.

8.1 Varieties

8.1.1 Definitions and Comments

We will be working in $k[X_1, \ldots, X_n]$, the ring of polynomials in n variables over the field k. (Any application of the Nullstellensatz requires that k be algebraically closed, but we will not make this assumption until it becomes necessary.) The set $A^n = A^n(k)$ of all n-tuples with components in k is called *affine n-space*. If S is a set of polynomials in $k[X_1, \ldots, X_n]$, then the zero-set of S, that is, the set $V = V(S)$ of all $x \in A^n$ such that $f(x) = 0$ for every $f \in S$, is called a *variety*. (The term "affine variety" is more precise, but we will use the short form because we will not be discussing projective varieties.) Thus a variety is the solution set of simultaneous polynomial equations.

If I is the ideal generated by S, then I consists of all finite linear combinations $\sum g_i f_i$ with $g_i \in k[X_1, \ldots, X_n]$ and $f_i \in S$. It follows that $V(S) = V(I)$, so every variety is the variety of some ideal. We now prove that we can make A^n into a topological space by taking varieties as the closed sets.

8.1.2 Proposition

(1) If $V_\alpha = V(I_\alpha)$ for all $\alpha \in T$, then $\bigcap V_\alpha = V(\bigcup I_\alpha)$. Thus an arbitrary intersection of varieties is a variety.

(2) If $V_j = V(I_j)$, $j = 1, \ldots, r$, then $\bigcup_{j=1}^{r} V_j = V(\{f_1 \cdots f_r : f_j \in I_j, 1 \leq j \leq r\})$. Thus a finite union of varieties is a variety.

(3) $A^n = V(0)$ and $\emptyset = V(1)$, so the entire space and the empty set are varieties.

Consequently, there is a topology on A^n, called the *Zariski topology*, such that the closed sets and the varieties coincide.

Proof. (1) If $x \in A^n$, then $x \in \bigcap V_\alpha$ iff every polynomial in every I_α vanishes at x iff $x \in V(\bigcup I_\alpha)$.

(2) $x \in \bigcup_{j=1}^{r} V_j$ iff for some j, every $f_j \in I_j$ vanishes at x iff $x \in V(\{f_1 \cdots f_r : f_j \in I_j$ for all $j\})$.

(3) The zero polynomial vanishes everywhere and a nonzero constant polynomial vanishes nowhere. ♣

Note that condition (2) can also be expressed as

$$\cup_{j=1}^{r} V_j = V\left(\prod_{j=1}^{r} I_j\right) = V\left(\cap_{j=1}^{r} I_j\right).$$

[See (7.6.1) for the definition of a product of ideals.]

We have seen that every subset of $k[X_1, \ldots, X_n]$, in particular every ideal, determines a variety. We can reverse this process as follows.

8.1.3 Definitions and Comments

If X is an arbitrary subset of A^n, we define the *ideal of* X as $I(X) = \{f \in k[X_1, \ldots, X_n] : f$ vanishes on $X\}$. By definition we have:

(4) If $X \subseteq Y$ then $I(X) \supseteq I(Y)$; if $S \subseteq T$ then $V(S) \supseteq V(T)$.

Now if S is any set of polynomials, define $IV(S)$ as $I(V(S))$, the ideal of the zero-set of S; we are simply omitting parentheses for convenience. Similarly, if X is any subset of A^n, we can define $VI(X)$, $IVI(X)$, $VIV(S)$, and so on. From the definitions we have:

(5) $IV(S) \supseteq S$; $VI(X) \supseteq X$.

[If $f \in S$ then f vanishes on $V(S)$, hence $f \in IV(S)$. If $x \in X$ then every polynomial in $I(X)$ vanishes at x, so x belongs to the zero-set of $I(X)$.]

If we keep applying V's and I's alternately, the sequence stabilizes very quickly:

(6) $VIV(S) = V(S)$; $IVI(X) = I(X)$.

[In each case, apply (4) and (5) to show that the left side is a subset of the right side. If $x \in V(S)$ and $f \in IV(S)$ then $f(x) = 0$, so $x \in VIV(S)$. If $f \in I(X)$ and $x \in VI(X)$ then x belongs to the zero-set of $I(X)$, so $f(x) = 0$. Thus f vanishes on $VI(X)$, so $f \in IVI(X)$.]

Since every polynomial vanishes on the empty set (vacuously), we have:

(7) $I(\emptyset) = k[X_1, \ldots, X_n]$.

The next two properties require a bit more effort.

(8) If k is an infinite field, then $I(A^n) = \{0\}$;

(9) If $x = (a_1, \ldots, a_n) \in A^n$, then $I(\{x\}) = (X_1 - a_1, \ldots, X_n - a_n)$.

Property (8) holds for $n = 1$ since a nonconstant polynomial in one variable has only finitely many zeros. Thus $f \neq 0$ implies that $f \notin I(A^1)$. If $n > 1$, let $f = a_r X_1^r + \cdots + a_1 X_1 + a_0$ where the a_i are polynomials in $X_2, \ldots, X_n$ and $a_r \neq 0$. By the induction hypothesis, there is a point $(x_2, \ldots, x_n)$ at which a_r does not vanish. Fixing this point, we can regard f as a polynomial in X_1, which cannot possibly vanish at all $x_1 \in k$. Thus $f \notin I(A^n)$.

To prove (9), note that the right side is contained in the left side because $X_i - a_i$ is 0 when $X_i = a_i$. Also, the result holds for $n = 1$ by the remainder theorem (2.5.2). Thus assume $n > 1$ and let $f = b_r X_1^r + \cdots + b_1 X_1 + b_0 \in I(\{x\})$, where the b_i are polynomials in $X_2, \ldots, X_n$ and $b_r \neq 0$. By the division algorithm (2.5.1), we have

$$f = (X_1 - a_1)g(X_1, \ldots, X_n) + h(X_2, \ldots, X_n)$$

and h must vanish at $(a_2, \ldots, a_n)$. By the induction hypothesis, $h \in (X_2 - a_2, \ldots, X_n - a_n)$, hence $f \in (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$.

Problems For Section 8.1

A variety is said to be *reducible* if it can be expressed as the union of two proper subvarieties; otherwise the variety is *irreducible*. In Problems 1–4, we are going to show that a variety V is irreducible if and only if $I(V)$ is a prime ideal.

1. Assume that $I(V)$ is not prime, and let $f_1 f_2 \in I(V)$ with $f_1, f_2 \notin I(V)$. If $x \in V$, show that $x \notin V(f_1)$ implies $x \in V(f_2)$ (and similarly, $x \notin V(f_2)$ implies $x \in V(f_1)$).
2. Show that V is reducible.
3. Show that if V and W are varieties with $V \subset W$, then $I(V) \supset I(W)$.
4. Now assume that $V = V_1 \bigcup V_2$, with $V_1, V_2 \subset V$. By Problem 3, we can choose $f_i \in I(V_i)$ with $f_i \notin I(V)$. Show that $f_1 f_2 \in I(V)$, so $I(V)$ is not a prime ideal.
5. Show that any variety is the union of finitely many irreducible subvarieties.
6. Show that the decomposition of Problem 5 is unique, assuming that we discard any subvariety that is contained in another one.
7. Assume that k is algebraically closed. Suppose that A^n is covered by open sets $A^n \setminus V(I_i)$ in the Zariski topology. Let I is the ideal generated by the I_i, so that $I = \sum I_i$, the set of all finite sums $x_{i_1} + \cdots x_{i_r}$ with $x_{i_j} \in I_{i_j}$. Show that $1 \in I$. (You may appeal to the weak Nullstellensatz, to be proved in Section 8.4.)
8. Show that A^n is compact in the Zariski topology.

8.2 The Hilbert Basis Theorem

If S is a set of polynomials in $k[X_1, \ldots, X_n]$, we have defined the variety $V(S)$ as the zero-set of S, and we know that $V(S) = V(I)$, where I is the ideal generated by S. Thus any set of simultaneous polynomial equations defines a variety. In general, infinitely many equations may be involved, but as Hilbert proved, an infinite collection of equations can always be replaced by a finite collection. The reason is that every ideal of $k[X_1, \ldots, X_n]$ has a finite set of generators, in other words, $k[X_1, \ldots, X_n]$ is a Noetherian ring. The field k is, in particular, a PID, so k is Noetherian. The key step is to show that if R is a Noetherian ring, then the polynomial ring in n variables over R is also Noetherian.

8.2.1 Hilbert Basis Theorem

If R is a Noetherian ring, then $R[X_1, \ldots, X_n]$ is also Noetherian.

Proof. By induction, we can assume $n = 1$. Let I be an ideal of $R[X]$, and let J be the ideal of all leading coefficients of polynomials in I. (The leading coefficient of $5X^2 - 3X + 17$ is 5; the leading coefficient of the zero polynomial is 0.) By hypothesis, J is finitely generated, say by $a_1, \ldots, a_n$. Let f_i be a polynomial in I whose leading coefficient is a_i, and let d_i be the degree of f_i. Let I^* consist of all polynomials in I of degree at most $d = \max\{d_i \colon 1 \leq i \leq n\}$. Then I^* is an R-submodule of the free R-module M of all polynomials $b_0 + b_1X + \cdots + b_dX^d, b_i \in R$. Now a finitely generated free R-module is a finite direct sum of copies of R, hence M, and therefore I^*, is Noetherian. Thus I^* can be generated by finitely many polynomials $g_1, \ldots, g_m$. Take I_0 to be the ideal of $R[X]$ generated by $f_1, \ldots, f_n, g_1, \ldots, g_m$. We will show that $I_0 = I$, proving that I is finitely generated.

First observe that $f_i \in I$ and $g_j \in I^* \subseteq I$, so $I_0 \subseteq I$. Thus we must show that each $h \in I$ belongs to I_0.

Case 1: $\deg h \leq d$

Then $h \in I^*$, so h is a linear combination of the g_j (with coefficients in $R \subseteq R[X]$), so $h \in I_0$.

Case 2: $\deg h = r > d$

Let a be the leading coefficient of h. Since $a \in J$, we have $a = \sum_{i=1}^n c_i a_i$ with the $c_i \in R$. Let

$$q = h - \sum_{i=1}^{n} c_i X^{r-d_i} f_i \in I.$$

The coefficient of X^r in q is

$$a - \sum_{i=1}^{n} c_i a_i = 0$$

so that $\deg q < r$. We can iterate this degree-reduction process until the resulting polynomial has degree d or less, and therefore belongs to I_0. But then h is a finite linear combination of the f_i and g_j. ♣

8.2.2 Corollary

Every variety is the intersection of finitely many *hypersurfaces* (zero-sets of single polynomials).

Proof. Let $V = V(I)$ be a variety. By (8.2.1), I has finitely many generators $f_1, \ldots, f_r$. But then $V = \bigcap_{i=1}^{r} V(f_i)$. ♣

8.2.3 Formal Power Series

The argument used to prove the Hilbert basis theorem can be adapted to show that if R is Noetherian, then the ring $R[[X]]$ of formal power series is Noetherian. We cannot simply reproduce the proof because an infinite series has no term of highest degree, but we can look at the *lowest* degree term. If $f = a_r X^r + a_{r+1} X^{r+1} + \cdots$, where r is a nonnegative integer and $a_r \neq 0$, let us say that f has degree r and leading coefficient a_r. (If $f = 0$, take the degree to be infinite and the leading coefficient to be 0.)

If I is an ideal of $R[[X]]$, we must show that I is finitely generated. We will inductively construct a sequence of elements $f_i \in R[[X]]$ as follows. Let f_1 have minimal degree among elements of I. Suppose that we have chosen $f_1, \ldots, f_i$, where f_i has degree d_i and leading coefficient a_i. We then select f_{i+1} satisfying the following three requirements:

1. f_{i+1} belongs to I;
2. a_{i+1} does not belong to $(a_1, \ldots, a_i)$, the ideal of R generated by the a_j, $j = 1, \ldots, i$;
3. Among all elements satisfying the first two conditions, f_{i+1} has minimal degree.

The second condition forces the procedure to terminate in a finite number of steps; otherwise there would be an infinite ascending chain $(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$. If stabilization occurs at step k, we will show that I is generated by $f_1, \ldots, f_k$.

Let $g = aX^d + \cdots$ be an element of I of degree d and leading coefficient a. Then $a \in (a_1, \ldots, a_k)$ (Problem 1).

Case 1: $d \geq d_k$. Since $d_i \leq d_{i+1}$ for all i (Problem 2), we have $d \geq d_i$ for $i = 1, \ldots, k$. Now $a = \sum_{i=1}^{k} c_{i0} a_i$ with the $c_{i0} \in R$. Define

$$g_0 = \sum_{i=1}^{k} c_{i0} X^{d-d_i} f_i$$

so that g_0 has degree d and leading coefficient a, and consequently $g - g_0$ has degree greater than d. Having defined $g_0, \ldots, g_r \in (f_1, \ldots, f_k)$ such that $g - \sum_{i=0}^{r} g_i$ has degree greater than $d + r$, say

$$g - \sum_{i=0}^{r} g_i = bX^{d+r+1} + \ldots .$$

(The argument is the same if the degree is greater than $d + r + 1$.) Now $b \in (a_1, \ldots, a_k)$ (Problem 1 again), so

$$b = \sum_{i=1}^{k} c_{i,r+1} a_i$$

with $c_{i,r+1} \in R$. We define

$$g_{r+1} = \sum_{i=1}^{k} c_{i,r+1} X^{d+r+1-d_i} f_i$$

so that $g - \sum_{i=0}^{r+1} g_i$ has degree greater than $d + r + 1$. Thus

$$g = \sum_{r=0}^{\infty} g_r = \sum_{r=0}^{\infty} \sum_{i=1}^{k} c_{ir} X^{d+r-d_i} f_i$$

and it follows upon reversing the order of summation that $g \in (f_1, \ldots, f_k)$. (The reversal is legal because the inner summation is finite. For a given nonnegative integer j, there are only finitely many terms of the form bX^j.)

Case 2: $d < d_k$. As above, $a \in (a_1, \ldots, a_k)$, so there is a smallest m between 1 and k such that $a \in (a_1, \ldots, a_m)$. It follows that $d \geq d_m$ (Problem 3). As in case 1 we have $a = \sum_{i=1}^{m} c_i a_i$ with $c_i \in R$. Define

$$h = \sum_{i=1}^{m} c_i X^{d-d_i} f_i \in (f_1, \ldots, f_k) \subseteq I.$$

The leading coefficient of h is a, so the degree of $g - h$ is greater than d. We replace g by $g - h$ and repeat the procedure. After at most $d_k - d$ iterations, we produce an element $g - \sum h_i$ in I of degree at least d_k, with all $h_i \in (f_1, \ldots, f_k)$. By the analysis of case 1, $g \in (f_1, \ldots, f_k)$.

Problems For Section 8.2

1. Justify the step $a \in (a_1, \ldots, a_k)$ in (8.2.3).
2. Justify the step $d_i \leq d_{i+1}$ in (8.2.3).
3. Justify the step $d \geq d_m$ in (8.2.3).
4. Let R be a subring of the ring S, and assume that S is finitely generated as an algebra over R. In other words, there are finitely many elements $x_1, \ldots, x_n \in S$ such that the smallest subring of S containing the x_i and all elements of R is S itself. Show that S is a homomorhic image of the polynomial ring $R[X_1, \ldots, X_n]$.
5. Continuing Problem 4, show that if R is Noetherian, then S is also Noetherian.

8.3 The Nullstellensatz: Preliminaries

We have observed that every variety V defines an ideal $I(V)$ and every ideal I defines a variety $V(I)$. Moreover, if $I(V_1) = I(V_2)$, then $V_1 = V_2$ by (6) of (8.1.3). But it is entirely possible for many ideals to define the same variety. For example, the ideals (f) and (f^m) need not coincide, but their zero-sets are identical. Appearances to the contrary, the two statements in part (6) of (8.1.3) are not symmetrical. A variety V is, by definition, always expressible as $V(S)$ for some collection S of polynomials, but an ideal I need not be of the

special form $I(X)$. Hilbert's Nullstellensatz says that if two ideals define the same variety, then, informally, the ideals are the same "up to powers". More precisely, if g belongs to one of the ideals, then g^r belongs to the other ideal for some positive integer r. Thus the only factor preventing a one-to-one correspondence between ideals and varieties is that a polynomial can be raised to a power without affecting its zero-set. In this section we collect some results needed for the proof of the Nullstellensatz. We begin by showing that each point of A^n determines a maximal ideal.

8.3.1 Lemma

If $a = (a_1, \ldots, a_n) \in A^n$, then $I = (X_1 - a_1, \ldots, X_n - a_n)$ is a maximal ideal.

Proof. Suppose that I is properly contained in the ideal J, with $f \in J \setminus I$. Apply the division algorithm n times to get

$$f = A_1(X_1 - a_1) + A_2(X_2 - a_2) + \cdots + A_n(X_n - a_n) + b$$

where $A_1 \in k[X_1, \ldots, X_n]$, $A_2 \in k[X_2, \ldots, X_n]$, $\ldots$, $A_n \in k[X_n]$, $b \in k$. Note that b cannot be 0 since $f \notin I$. But $f \in J$, so by solving the above equation for b we have $b \in J$, hence $1 = (1/b)b \in J$. Consequently, $J = k[X_1, \ldots, X_n]$. ♣

The following definition will allow a precise statement of the Nullstellensatz.

8.3.2 Definition

The *radical* of an ideal I (in any commutative ring R) is the set of all elements $f \in R$ such that $f^r \in I$ for some positive integer r.

A popular notation for the radical of I is $\sqrt{I}$. If f^r and g^s belong to I, then by the binomial theorem, $(f + g)^{r+s-1} \in I$, and it follows that $\sqrt{I}$ is an ideal.

8.3.3 Lemma

If I is any ideal of $k[X_1, \ldots, X_n]$, then $\sqrt{I} \subseteq IV(I)$.

Proof. If $f \in \sqrt{I}$, then $f^r \in I$ for some positive integer r. But then f^r vanishes on $V(I)$, hence so does f. Therefore $f \in IV(I)$. ♣

The Nullstellensatz states that $IV(I) = \sqrt{I}$, and the hard part is to prove that $IV(I) \subseteq \sqrt{I}$. The technique is known as the "Rabinowitsch trick", and it is indeed very clever. Assume that $f \in IV(I)$. We introduce a new variable Y and work in $k[X_1, \ldots, X_n, Y]$. If I is an ideal of $k[X_1, \ldots, X_n]$, then by the Hilbert basis theorem, I is finitely generated, say by $f_1, \ldots, f_m$. Let I^* be the ideal of $k[X_1, \ldots, X_n, Y]$ generated by $f_1, \ldots, f_m, 1 - Yf$. [There is a slight ambiguity: by $f_i(X_1, \ldots, X_n, Y)$ we mean $f_i(X_1, \ldots, X_n)$, and similarly for f.] At an appropriate moment we will essentially set Y equal to $1/f$ and come back to the original problem.

8.3.4 Lemma

If $(a_1, \ldots, a_n, a_{n+1})$ is any point in A^{n+1} and $(a_1, \ldots, a_n) \in V(I)$ (in other words, the f_i, $i = 1, \ldots, m$, vanish at $(a_1, \ldots, a_n)$), then $(a_1, \ldots, a_n, a_{n+1}) \notin V(I^*)$.

Proof. We are assuming that $f \in IV(I)$, so that f vanishes on the zero-set of $\{f_1, \ldots, f_m\}$. In particular, $f(a_1, \ldots, a_n) = 0$. The value of $1 - Yf$ at $(a_1, \ldots, a_n, a_{n+1})$ is therefore $1 - a_{n+1}f(a_1, \ldots, a_n) = 1 - a_{n+1}(0) = 1 \neq 0$. But $1 - Yf \in I^*$, so $(a_1, \ldots, a_n, a_{n+1})$ does not belong to the zero-set of I^*. ♣

8.3.5 Lemma

If $(a_1, \ldots, a_n, a_{n+1})$ is any point in A^{n+1} and $(a_1, \ldots, a_n) \notin V(I)$, then $(a_1, \ldots, a_n, a_{n+1}) \notin V(I^*)$. Consequently, by (8.3.4), $V(I^*) = \emptyset$.

Proof. By hypothesis, $f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$ for some i, and since $f_i \in I^*$, $(a_1, \ldots, a_{n+1})$ cannot belong to the zero-set of I^*. ♣

At this point we are going to assume what is called the weak Nullstellensatz, namely that if I is a proper ideal of $k[X_1, \ldots, X_n]$, then $V(I)$ is not empty.

8.3.6 Lemma

There are polynomials $g_1, \ldots, g_m, h \in k[X_1, \ldots, X_n, Y]$ such that

$$1 = \sum_{i=1}^{m} g_i f_i + h(1 - Yf). \tag{1}$$

This equation also holds in the rational function field $k(X_1, \ldots, X_n, Y)$ consisting of quotients of polynomials in $k[X_1, \ldots, X_n, Y]$.

Proof. By (8.3.4) and (8.3.5), $V(I^*) = \emptyset$, so by the weak Nullstellensatz, $I^* = k[X_1, \ldots, X_n, Y]$. In particular, $1 \in I^*$, and since I^* is generated by $f_1, \ldots, f_m, 1 - Yf$, there is an equation of the specified form. The equation holds in the rational function field because a polynomial is a rational function. ♣

8.3.7 The Rabinowitsch Trick

The idea is to set $Y = 1/f$, so that (1) becomes

$$1 = \sum_{i=1}^{m} g_i(X_1, \ldots, X_n, 1/f(X_1, \ldots, X_n)) f_i(X_1, \ldots, X_n). \tag{2}$$

Is this legal? First of all, if f is the zero polynomial, then certainly $f \in \sqrt{I}$, so we can assume $f \neq 0$. To justify replacing Y by $1/f$, consider the ring homomorphism from $k[X_1, \ldots, X_n, Y]$ to $k(X_1, \ldots, X_n)$ determined by $X_i \to X_i$, $i = 1, \ldots, n$, $Y \to 1/f(X_1, \ldots, X_n)$. Applying this mapping to (1), we get (2). Now the right side of (2) is a sum of rational functions whose denominators are various powers of f. If f^r is the highest

power that appears, we can absorb all denominators by multiplying (2) by f^r. The result is an equation of the form

$$f^r = \sum_{i=1}^{m} h_i(X_1, \ldots, X_n) f_i(X_1, \ldots, X_n)$$

where the h_i are *polynomials* in $k[X_1, \ldots, X_n]$. Consequently, $f^r \in I$. ♣

The final ingredient is a major result in its own right.

8.3.8 Noether Normalization Lemma

Let A be a finitely generated k-algebra, where k is a field. In other words, there are finitely many elements $x_1, \ldots, x_n$ in A that generate A over k in the sense that every element of A is a polynomial in the x_i. Equivalently, A is a homomorphic image of the polynomial ring $k[X_1, \ldots, X_n]$ via the map determined by $X_i \to x_i$, $i = 1, \ldots, n$.

There exists a subset $\{y_1, \ldots, y_r\}$ of A such that the y_i are algebraically independent over k and A is integral over $k[y_1, \ldots, y_r]$.

Proof. Let $\{x_1, \ldots, x_r\}$ be a maximal algebraically independent subset of $\{x_1, \ldots, x_n\}$. If $n = r$ we are finished, since we can take $y_i = x_i$ for all i. Thus assume $n > r$, in which case $x_1, \ldots, x_n$ are algebraically dependent over k. Thus there is a nonzero polynomial $f \in k[X_1, \ldots, X_n]$ such that $f(x_1, \ldots, x_n) = 0$. We can assume $n > 1$, for if $n = 1$ and $r = 0$, then $A = k[x_1]$ and we can take $\{y_1, \ldots, y_r\}$ to be the empty set.

We first assume that k is infinite and give a proof by induction on n. (It is possible to go directly to the general case, but the argument is not as intricate for an infinite field.) Decompose f into its homogeneous components (sums of monomials of the same degree). Say that g is the homogeneous component of maximum degree d. Then, regarding g as a polynomial in X_n whose coefficients are polynomials in the other X_i, we have, relabeling variables if necessary, $g(X_1, \ldots, X_{n-1}, 1) \neq 0$. Since k is infinite, it follows from (8.1.3) part (8) that there are elements $a_1, \ldots, a_{n-1} \in k$ such that $g(a_1, \ldots, a_{n-1}, 1) \neq 0$. Set $z_i = x_i - a_i x_n$, $i = 1, \ldots, n-1$, and plug into $f(x_1, \ldots, x_n) = 0$ to get an equation of the form

$$g(a_1, \ldots, a_{n-1}, 1) x_n^d + \text{terms of degree less than } d \text{ in } x_n = 0.$$

A concrete example may clarify the idea. If $f(x_1, x_2) = g(x_1, x_2) = x_1^2 x_2^3$ and $x_1 = z_1 + a_1 x_2$, then the substitution yields

$$(z_1^2 + 2a_1 z_1 x_2 + a_1^2 x_2^2) x_2^3$$

which indeed is $g(a_1, 1) x_2^5$ plus terms of degree less than 5 in x_2. Divide by $g(a_1, \ldots, a_{n-1}, 1) \neq 0$ to conclude that x_n is integral over $B = k[z_1, \ldots, z_{n-1}]$. By the induction hypothesis, there are elements $y_1, \ldots, y_r$ algebraically independent over k such that B is integral over $k[y_1, \ldots, y_r]$. But the $x_i, i < n$, are integral over B since $x_i = z_i + a_i x_n$. By transitivity (see (7.1.4)), $x_1, \ldots, x_n$ are integral over $k[y_1, \ldots, y_r]$. Thus (see (7.1.5)) A is integral over $k[y_1, \ldots, y_r]$.

Now we consider arbitrary k. As before, we produce a nonzero polynomial f such that $f(x_1, \ldots, x_n) = 0$. We assign a weight $w_i = s^{n-i}$ to the variable X_i, where s is a

large positive integer. (It suffices to take s greater than the total degree of f, that is, the sum of the degrees of all monomials in f.) If $h = \lambda X_1^{a_1} \cdots X_n^{a_n}$ is a monomial of f, we define the weight of h as $w(h) = \sum_{i=1}^n a_i w_i$. The point is that if $h' = \mu X_1^{b_1} \cdots X_n^{b_n}$, then $w(h) > w(h')$ iff $h > h'$ in the lexicographic ordering, that is, for some m we have $a_i = b_i$ for $i \leq m$, and $a_{m+1} > b_{m+1}$. We take h to be the monomial of maximum weight. (If two monomials differ in the lexicographic ordering, they must have different weights.) Set $z_i = x_i - x_n^{w_i}$, $1 \leq i \leq n-1$, and plug into $f(x_1, \ldots, x_n) = 0$ to get

$$cx_n^{w(h)} + \text{terms of lower degree in } x_n = 0.$$

For example, if $f(x_1, x_2) = h(x_1, x_2) = x_1^3 x_2^2$, then $x_1 = z_1 + x_2^{w_1}$ gives

$$(z_1^3 + 3z_1^2 x_2^{w_1} + 3z_1 x_2^{2w_1} + x_2^{3w_1})x_2^2$$

and $w(h) = 3w_1 + 2w_2 = 3w_1 + 2$ since $s^{n-2} = s^0 = 1$. Thus x_n is integral over $B = k[z_1, \ldots, z_{n-1}]$, and an induction argument finishes the proof as in the first case. ♣

8.3.9 Corollary

Let B be a finitely generated k-algebra, where k is a field. If I is a maximal ideal of B, then B/I is a finite extension of k.

Proof. The field k can be embedded in B/I via $c \to c + I$, $c \in k$. [If $c \in I$, $c \neq 0$, then $c^{-1}c = 1 \in I$, a contradiction.] Since $A = B/I$ is also a finitely generated k-algebra, it follows from (8.3.8) that there is a subset $\{y_1, \ldots, y_r\}$ of A with the y_i algebraically independent over k and A integral over $k[y_1, \ldots, y_r]$. Now A is a field (because I is a maximal ideal), and therefore so is $k[y_1, \ldots, y_r]$ (see the Problems in Section 7.1). But this will lead to a contradiction if $r \geq 1$, because $1/y_1 \notin k[y_1, \ldots, y_r]$. (If $1/y_1 = g(y_1, \ldots, y_r) \in k[y_1, \ldots, y_r]$, then $y_1 g(y_1, \ldots, y_r) = 1$, contradicting algebraic independence.) Thus r must be 0, so A is integral, hence algebraic, over the field k. Therefore A is generated over k by finitely many algebraic elements, so by (3.3.3), A is a finite extension of k. ♣

8.3.10 Corollary

Let A be a finitely generated k-algebra, where k is a field. If A is itself a field, then A is a finite extension of k.

Proof. As in (8.3.9), with B/I replaced by A. ♣

Problems For Section 8.3

1. Let S be a multiplicative subset of the ring R (see (2.8.1)). If I is an ideal that is disjoint from S, then by Zorn's lemma, there is an ideal J that is maximal among ideals disjoint from S. Show that J must be prime.

2. Show that the radical of the ideal I is the intersection of all prime ideals containing I. [If $f^r \in I \subseteq P$, P prime, then $f \in P$. Conversely, assume $f \notin \sqrt{I}$. With a clever choice of multiplicative set S, show that for some prime ideal P containing I, we have $f \notin P$.]
3. An *algebraic curve* is a variety defined by a nonconstant polynomial in two variables. Show (using the Nullstellensatz) that the polynomials f and g define the same algebraic curve iff f divides some power of g and g divides some power of f. Equivalently, f and g have the same irreducible factors.
4. Show that the variety V defined over the complex numbers by the two polynomials $Y^2 - XZ$ and $Z^2 - X^2Y$ is the union of the line L given by $Y = Z = 0$, X arbitrary, and the set W of all (t^3, t^4, t^5), $t \in \mathbb{C}$.
5. The *twisted cubic* is the variety V defined over the complex numbers by $Y - X^2$ and $Z - X^3$. In parametric form, $V = \{(t, t^2, t^3) \colon t \in \mathbb{C}\}$. Show that V is irreducible. [The same argument works for any variety that can be parametrized over an infinite field.]
6. Find parametrizations of the following algebraic curves over the complex numbers. (It is permissible for your parametrizations to fail to cover finitely many points of the curve.)
   (a) The unit circle $x^2 + y^2 = 1$;
   (b) The cuspidal cubic $y^2 = x^3$;
   (c) The nodal cubic $y^2 = x^2 + x^3$.
7. Let f be an irreducible polynomial, and g an arbitrary polynomial, in $k[x, y]$. If f does not divide g, show that the system of simultaneous equations $f(x, y) = g(x, y) = 0$ has only finitely many solutions.

8.4 The Nullstellensatz: Equivalent Versions And Proof

We are now in position to establish the equivalence of several versions of the Nullstellensatz.

8.4.1 Theorem

For any field k and any positive integer n, the following statements are equivalent.

(1) **Maximal Ideal Theorem** The maximal ideals of $k[X_1, \ldots, X_n]$ are the ideals of the form $(X_1 - a_1, \ldots, X_n - a_n)$, $a_1, \ldots, a_n \in k$. Thus maximal ideals correspond to points.

(2) **Weak Nullstellensatz** If I is an ideal of $k[X_1, \ldots, X_n]$ and $V(I) = \emptyset$, then $I = k[X_1, \ldots, X_n]$. Equivalently, if I is a proper ideal, then $V(I)$ is not empty.

(3) **Nullstellensatz** If I is an ideal of $k[X_1, \ldots, X_n]$, then

$$IV(I) = \sqrt{I}.$$

(4) k is algebraically closed.

Proof. (1) implies (2). Let I be a proper ideal, and let J be a maximal ideal containing I. By (8.1.3), part (4), $V(J) \subseteq V(I)$, so it suffices to show that $V(J)$ is not empty. By (1), J has the form $(X_1 - a_1, \ldots, X_n - a_n)$. But then $a = (a_1, \ldots, a_n) \in V(J)$. [In fact $V(J) = \{a\}$.]

(2) implies (3). This was done in Section 8.3.

(3) implies (2). We use the fact that the radical of an ideal I is the intersection of all prime ideals containing I; see Section 8.3, Problem 2. Let I be a proper ideal of $k[X_1, \ldots, X_n]$. Then I is contained in a maximal, hence prime, ideal P. By the result just quoted, $\sqrt{I}$ is also contained in P, hence $\sqrt{I}$ is a proper ideal. By (3), $IV(I)$ is a proper ideal. But if $V(I) = \emptyset$, then by (8.1.3) part (7), $IV(I) = k[X_1, \ldots, X_n]$, a contradiction.

(2) implies (1). If I is a maximal ideal, then by (2) there is a point $a = (a_1, \ldots, a_n) \in V(I)$. Thus every $f \in I$ vanishes at a, in other words, $I \subseteq I(\{a\})$. But $(X_1 - a_1, \ldots, X_n - a_n) = I(\{a\})$; to see this, decompose $f \in I(\{a\})$ as in the proof of (8.3.1). Therefore the maximal ideal I is contained in the maximal ideal $(X_1 - a_1, \ldots, X_n - a_n)$, and it follows that $I = (X_1 - a_1, \ldots, X_n - a_n)$.

(4) implies (1). Let I be a maximal ideal of $k[X_1, \ldots, X_n]$, and let $K = k[X_1, \ldots, X_n]/I$, a field containing an isomorphic copy of k via $c \to c + I$, $c \in k$. By (8.3.9), K is a finite extension of k, so by (4), $K = k$. But then $X_i + I = a_i + I$ for some $a_i \in k$, $i = 1, \ldots, n$. Therefore $X_i - a_i$ is zero in $k[X_1, \ldots, X_n]/I$, in other words, $X_i - a_i \in I$. Consequently, $I \supseteq (X_1 - a_1, \ldots, X_n - a_n)$, and we must have equality by (8.3.1).

(1) implies (4). Let f be a nonconstant polynomial in $k[X_1]$ with no root in k. We can regard f is a polynomial in n variables with no root in A^n. Let I be a maximal ideal containing the proper ideal (f). By (1), I is of the form $(X_1 - a_1, \ldots, X_n - a_n) = I(\{a\})$ for some $a = (a_1, \ldots, a_n) \in A^n$. Therefore f vanishes at a, a contradiction. ♣

8.4.2 Corollary

If the ideals I and J define the same variety and a polynomial g belongs to one of the ideals, then some power of g belongs to the other ideal.

Proof. If $V(I) = V(J)$, then by the Nullstellensatz, $\sqrt{I} = \sqrt{J}$. If $g \in I \subseteq \sqrt{I}$, then $g^r \in J$ for some positive integer r. ♣

8.4.3 Corollary

The maps $V \to I(V)$ and $I \to V(I)$ set up a one-to-one correspondence between varieties and *radical ideals* (defined by $I = \sqrt{I}$).

Proof. By (8.1.3) part 6, $VI(V) = V$. By the Nullstellensatz, $IV(I) = \sqrt{I} = I$ for radical ideals. It remains to prove that for any variety V, $I(V)$ is a radical ideal. If $f^r \in I(V)$, then f^r, hence f, vanishes on V, so $f \in I(V)$. ♣

8.4.4 Corollary

Let $f_1, \ldots, f_r, g \in k[X_1, \ldots, X_n]$, and assume that g vanishes wherever the f_i all vanish. Then there are polynomials $h_1, \ldots, h_r \in k[X_1, \ldots, X_n]$ and a positive integer s such that $g^s = h_1 f_1 + \cdots + h_r f_r$.

Proof. Let I be the ideal generated by $f_1, \ldots, f_r$. Then $V(I)$ is the set of points at which all f_i vanish, so that $IV(I)$ is the set of polynomials that vanish wherever all f_i vanish. Thus g belongs to $IV(I)$, which is $\sqrt{I}$ by the Nullstellensatz. Consequently, for some positive integer s, we have $g^s \in I$, and the result follows. ♣

Problems For Section 8.4

1. Let f be a polynomial in $k[X_1, \ldots, X_n]$, and assume that the factorization of f into irreducibles is $f = f_1^{n_1} \cdots f_r^{n_r}$. Show that the decomposition of the variety $V(f)$ into irreducible subvarieties (Section 8.1, Problems 5 and 6) is given by $V(f) = \cup_{i=1}^{r} V(f_i)$.
2. Under the hypothesis of Problem 1, show that $IV(f) = (f_1 \cdots f_r)$.
3. Show that there is a one-to-one correspondence between irreducible polynomials in $k[X_1, \ldots, X_n]$ and irreducible hypersurfaces (see (8.2.2))in $A^n(k)$, if polynomials that differ by a nonzero multiplicative constant are identified.
4. For any collection of subsets X_i of A^n, show that $I(\cup_i X_i) = \cap_i I(X_i)$.
5. Show that every radical ideal I of $k[X_1, \ldots, X_n]$ is the intersection of finitely many prime ideals.
6. In Problem 5, show that the decomposition is unique, subject to the condition that the prime ideals P are *minimal*, that is, there is no prime ideal Q with $I \subseteq Q \subset P$.
7. Suppose that X is a variety in A^2, defined by equations $f_1(x, y) = \cdots = f_m(x, y) = 0$, $m \geq 2$. Let g be the greatest common divisor of the f_i. If g is constant, show that X is a finite set (possibly empty).
8. Show that every variety in A^2 except for A^2 itself is the union of a finite set and an algebraic curve. 9. Give an example of two distinct irreducible polynomials in $k[X, Y]$ with the same zero-set, and explain why this cannot happen if k is algebraically closed. 10. Give an explicit example of the failure of a version of the Nullstellensatz in a non-algebraically closed field.

8.5 Localization

8.5.1 Geometric Motivation

Suppose that V is an irreducible variety, so that $I(V)$ is a prime ideal. A polynomial g will belong to $I(V)$ if and only if it vanishes on V. If we are studying rational functions f/g in the neighborhood of a point $x \in V$, we must have $g(x) \neq 0$. It is very convenient to have every polynomial $g \notin I(V)$ available as a legal object, even though g may vanish at some points of V. The technical device that makes this possible is the construction of the ring of fractions $S^{-1}R$, the localization of R by S, where $R = k[X_1, \ldots, X_n]$ and S is the multiplicative set $R \setminus I(V)$. We will now study the localization process in general.

8.5.2 Notation

Recalling the setup of Section 2.8, let S be a multiplicative subset of the ring R, and $S^{-1}R$ the ring of fractions of R by S. Let h be the natural homomorphism of R into $S^{-1}R$, given by $h(a) = a/1$. If X is any subset of R, define $S^{-1}X = \{x/s\colon x \in X, s \in S\}$. We will be especially interested in such a set when X is an ideal.

If I and J are ideals of R, the *product* of I and J, denoted by IJ, is defined (as in (7.6.1)) as the set of all finite sums $\sum_i x_i y_i$, $x_i \in I$, $y_i \in J$. It follows from the definition that IJ is an ideal. The *sum* of two ideals has already been defined in (2.2.8).

8.5.3 Lemma

If I is an ideal of R, then $S^{-1}I$ is an ideal of $S^{-1}R$. If J is another ideal of R, the

(i) $S^{-1}(I + J) = S^{-1}I + S^{-1}J$;

(ii) $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$;

(iii) $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$;

(iv) $S^{-1}I$ is a proper ideal iff $S \cap I = \emptyset$.

Proof. The definition of addition and multiplication in $S^{-1}R$ implies that $S^{-1}I$ is an ideal, and that in (i), (ii) and (iii), the left side is contained in the right side. The reverse inclusions in (i) and (ii) follow from

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}.$$

To prove (iii), let $a/s = b/t$ where $a \in I$, $b \in J$, $s, t \in S$. There exists $u \in S$ such that $u(at - bs) = 0$. Then $a/s = uat/ust = ubs/ust \in S^{-1}(I \cap J)$.

Finally, if $s \in S \cap I$ then $1/1 = s/s \in S^{-1}I$, so $S^{-1}I = S^{-1}R$. Conversely, if $S^{-1}I = S^{-1}R$, then $1/1 = a/s$ for some $a \in I$, $s \in S$. There exists $t \in S$ such that $t(s - a) = 0$, so $at = st \in S \cap I$. ♣

Ideals in $S^{-1}R$ must be of a special form.

8.5.4 Lemma

If J is an ideal of $S^{-1}R$ and $I = h^{-1}(J)$, then I is an ideal of R and $S^{-1}I = J$.

Proof. I is an ideal by the basic properties of preimages of sets. Let $a/s \in S^{-1}I$, with $a \in I$ and $s \in S$. Then $a/1 \in J$, so $a/s = (a/1)(1/s) \in J$. Conversely, let $a/s \in J$, with $a \in R$, $s \in S$. Then $h(a) = a/1 = (a/s)(s/1) \in J$, so $a \in I$ and $a/s \in S^{-1}I$. ♣

Prime ideals yield sharper results.

8.5.5 Lemma

If I is any ideal of R, then $I \subseteq h^{-1}(S^{-1}I)$, with equality if I is prime and disjoint from S.

Proof. If $a \in I$, then $h(a) = a/1 \in S^{-1}I$. Thus assume that I is prime and disjoint from S, and let $a \in h^{-1}(S^{-1}I)$. Then $h(a) = a/1 \in S^{-1}I$, so $a/1 = b/s$ for some $b \in I$, $s \in S$. There exists $t \in S$ such that $t(as - b) = 0$. Thus $ast = bt \in I$, with $st \notin I$ since $S \cap I = \emptyset$. Since I is prime, we have $a \in I$. ♣

8.5.6 Lemma

If I is a prime ideal of R disjoint from S, then $S^{-1}I$ is a prime ideal of $S^{-1}R$.

Proof. By (8.5.3), part (iv), $S^{-1}I$ is a proper ideal. Let $(a/s)(b/t) = ab/st \in S^{-1}I$, with $a, b \in R$, $s, t \in S$. Then $ab/st = c/u$ for some $c \in I$, $u \in S$. There exists $v \in S$ such that $v(abu - cst) = 0$. Thus $abuv = cstv \in I$, and $uv \notin I$ because $S \cap I = \emptyset$. Since I is prime, $ab \in I$, hence $a \in I$ or $b \in I$. Therefore either a/s or b/t belongs to $S^{-1}I$. ♣

The sequence of lemmas can be assembled to give a precise conclusion.

8.5.7 Theorem

There is a one-to-one correspondence between prime ideals P of R that are disjoint from S and prime ideals Q of $S^{-1}R$, given by

$$P \to S^{-1}P \text{ and } Q \to h^{-1}(Q).$$

Proof. By (8.5.4), $S^{-1}(h^{-1}(Q)) = Q$, and by (8.5.5), $h^{-1}(S^{-1}P) = P$. By (8.5.6), $S^{-1}P$ is a prime ideal, and $h^{-1}(Q)$ is a prime ideal by the basic properties of preimages of sets. If $h^{-1}(Q)$ meets S, then by (8.5.3) part (iv), $Q = S^{-1}(h^{-1}(Q)) = S^{-1}R$, a contradiction. Thus the maps $P \to S^{-1}P$ and $Q \to h^{-1}(Q)$ are inverses of each other, and the result follows. ♣

8.5.8 Definitions and Comments

If P is a prime ideal of R, then $S = R \setminus P$ is a multiplicative set. In this case, we write $R(P)$ for $S^{-1}R$, and call it the *localization of R at P*. (The usual notation is R_P, but it's easier to read without subscripts.) If I is an ideal of R, we write $I(P)$ for $S^{-1}I$. We are going to show that $R(P)$ is a *local ring*, that is, a ring with a unique maximal ideal. First we give some conditions equivalent to the definition of a local ring.

8.5.9 Proposition

For a ring R, the following conditions are equivalent.

(i) R is a local ring;

(ii) There is a proper ideal I of R that contains all nonunits of R;

(iii) The set of nonunits of R is an ideal.

Proof. (i) implies (ii). If a is a nonunit, then (a) is a proper ideal, hence is contained in the unique maximal ideal I.

(ii) implies (iii). If a and b are nonunits, so are $a+b$ and ra. If not, then I contains a unit, so $I = R$, a contradiction.

(iii) implies (i). If I is the ideal of nonunits, then I is maximal, because any larger ideal J would have to contain a unit, so that $J = R$. If H is any proper ideal, then H cannot contain a unit, so $H \subseteq I$. Therefore I is the unique maximal ideal. ♣

8.5.10 Theorem

$R(P)$ is a local ring.

Proof. Let Q be a maximal ideal of $R(P)$. Then Q is prime, so by (8.5.7), $Q = I(P)$ for some prime ideal I of R that is disjoint from S, in other words, contained in P. Thus $Q = I(P) \subseteq P(P)$. If $P(P) = R(P)$, then by (8.5.3) part (iv), P is not disjoint from $S = R\backslash P$, which is impossible. Therefore $P(P)$ is a proper ideal containing every maximal ideal, so it must be the unique maximal ideal. ♣

If R is an integral domain and S is the set of all nonzero elements of R, then $S^{-1}R$ is the quotient field of R. In this case, $S^{-1}R$ is a local ring, because any field is a local ring. ($\{0\}$ is the unique maximal ideal.) Alternatively, we can appeal to (8.5.10) with $P = \{0\}$.

8.5.11 Localization of Modules

If M is an R-module and S a multiplicative subset of R, we can essentially repeat the construction of Section 2.8 to form the localization $S^{-1}M$ of M by S, and thereby divide elements of M by elements of S. If $x, y \in M$ and $s, t \in S$, we call (x, s) and (y, t) equivalent if for some $u \in S$, $u(tx - sy) = 0$. The equivalence class of (x, s) is denoted by x/s, and addition is defined by

$$\frac{x}{s} + \frac{y}{t} = \frac{tx + sy}{st}.$$

If $a/s \in S^{-1}R$ and $x/t \in S^{-1}M$, we define

$$\frac{a}{s}\frac{x}{t} = \frac{ax}{st}.$$

In this way, $S^{-1}M$ becomes an $S^{-1}R$-module. Exactly as in (8.5.3), if M and N are submodules of a module L, then

$$S^{-1}(M + N) = S^{-1}M + S^{-1}N \text{ and } S^{-1}(M \cap N) = S^{-1}M \cap S^{-1}N.$$

Further properties will be given in the exercises.

Problems For Section 8.5

1. Let M be a maximal ideal of R, and assume that for every $x \in M$, $1 + x$ is a unit. Show that R is a local ring (with maximal ideal M). [Show that if $x \notin M$, then x is a unit, and apply (8.5.9).]
2. Show that if p is prime and n is a positive integer, then $\mathbb{Z}_{p^n}$ is a local ring with maximal ideal (p).
3. Let R be the ring of all n by n matrices with coefficients in a field F. If A is a nonzero element of R and 1 is the identity matrix, is $\{1, A, A^2, \dots\}$ always a multiplicative set?

Let S be a multiplicative subset of the ring R. We are going to construct a mapping from R-modules to $S^{-1}R$-modules, and another mapping from R-module homomorphisms to $S^{-1}R$-module homomorphisms, as follows. If M is an R-module, we let $M \to S^{-1}M$. If $f\colon M \to N$ is an R-module homomorphism, we define $S^{-1}f\colon S^{-1}M \to S^{-1}N$ by

$$\frac{x}{s} \to \frac{f(x)}{s}.$$

Since f is a homomorphism, so is $S^{-1}\ f$.

4. If $g\colon N \to L$ and composition of functions is written as a product, show that $S^{-1}(gf) = S^{-1}(g)S^{-1}(f)$, and if 1_M is the identity mapping on M, then $S^{-1}(1_M) = 1_{S^{-1}M}$. We say that S^{-1} is a *functor* from the *category* of R-modules to the category of $S^{-1}R$-modules. This terminology will be explained in great detail in Chapter 10.
5. If

$$M \overset{f}{\to} N \overset{g}{\to} L$$

is an exact sequence, show that

$$S^{-1}M \overset{S^{-1}f}{\to} S^{-1}N \overset{S^{-1}g}{\to} S^{-1}L$$

is exact. We say that S^{-1} is an *exact functor*. Again, we will study this idea in Chapter 10.

6. Let R be the ring of rational functions f/g with $f, g \in k[X_1, \dots, X_n]$ and $g(a) \neq 0$, where $a = (a_1, \dots, a_n)$ is a fixed point in A^n. Show that R is a local ring, and identify the unique maximal ideal.
7. If M is an R-module and S is a multiplicative subset of R, denote $S^{-1}M$ by M_S. If N is a submodule of M, show that $(M/N)_S \cong M_S/N_S$.

8.6 Primary Decomposition

We have seen that every radical ideal in $k[X_1, \dots, X_n]$ can be expressed as an intersection of finitely many prime ideals (Section 8.4, Problem 5). A natural question is whether a similar result holds for arbitrary ideals. The answer is yes if we generalize from prime to primary ideals.

8.6.1 Definitions and Comments

The ideal Q in the ring R is *primary* if Q is proper and whenever a product ab belongs to Q, either $a \in Q$ or $b^n \in Q$ for some positive integer n. [The condition on b is equivalent to $b \in \sqrt{Q}$.] An equivalent statement is that $R/Q \neq 0$ and whenever $(a+Q)(b+Q) = 0$ in R/Q, either $a+Q = 0$ or $(b+Q)^n = 0$ for some positive integer n. This says that if $b+Q$ is a zero-divisor in R/Q, then it is *nilpotent*, that is, some power of $b+Q$ is 0.

It follows from the definition that every prime ideal is primary. Also, if Q is primary, then $\sqrt{Q}$ is the smallest prime ideal containing Q. [Since $\sqrt{Q}$ is the intersection of all prime ideals containing Q (Section 8.3, Problem 2), it suffices to show that $\sqrt{Q}$ is prime. But if $a^n b^n \in Q$, then $a^n \in Q$ or $b^{nm} \in Q$ for some m, so either a or b must belong to $\sqrt{Q}$. Note also that since Q is proper, it is contained in a maximal, hence prime, ideal, so $\sqrt{Q}$ is also proper.]

If Q is primary and $\sqrt{Q} = P$, we say that Q is *P-primary.*

8.6.2 Examples

1. In $\mathbb{Z}$, the primary ideals are $\{0\}$ and (p^r), where p is prime. In $\mathbb{Z}_6$, 2 and 3 are zero-divisors that are not nilpotent, and a similar situation will occur in $\mathbb{Z}_m$ whenever more than one prime appears in the factorization of m.

2. Let $R = k[X,Y]$ where k is any field, and take $Q = (X, Y^3)$, the ideal generated by X and Y^3. This is a nice example of analysis in quotient rings. We are essentially setting X and Y^3 equal to zero, and this collapses the ring R down to polynomials $a_0 + a_1 Y + a_2 Y^2$, with the $a_i \in k$ and arithmetic mod Y^3. Formally, R/Q is isomorphic to $k[Y]/(Y^3)$. The zero-divisors in R/Q are of the form $cY + dY^2$, $c \in k$, and they are nilpotent. Thus Q is primary. If $f \in R$, then the only way for f not to belong to the radical of Q is for the constant term of f to be nonzero. Thus $\sqrt{Q} = (X,Y)$, a maximal ideal by (8.3.1).

Now we claim that Q cannot be a power of a prime ideal; this will be a consequence of the next result.

8.6.3 Lemma

If P is a prime ideal, then for every positive integer n, $\sqrt{P^n} = P$.

Proof. Since P is a prime ideal containing P^n, $\sqrt{P^n} \subseteq P$. If $x \in P$, then $x^n \in P^n$, so $x \in \sqrt{P^n}$. ♣

Returning to Example 2 of (8.6.2), if $Q = (X, Y^3)$ is a prime power P^n, then its radical is P, so P must be (X,Y). But $X \in Q$ and $X \notin P^n, n \geq 2$; since Y belongs to P but not Q, we have reached a contradiction.

After a preliminary definition, we will give a convenient sufficient condition for an ideal to be primary.

8.6.4 Definition

The *nilradical* $\mathcal{N}(R)$ of a ring R is the set of nilpotent elements of R, that is, $\{x \in R: x^n = 0 \text{ for some positive integer } n\}$. Thus $\mathcal{N}(R)$ is the radical of the zero ideal, which is

the intersection of all prime ideals of R.

8.6.5 Proposition

If the radical of the ideal Q is maximal, then Q is primary.

Proof. Since $\sqrt{Q}$ is maximal, it must be the only prime ideal containing Q. By the correspondence theorem and the fact that the preimage of a prime ideal is a prime ideal (cf. (8.5.7)), R/Q has exactly one prime ideal, which must coincide with $\mathcal{N}(R/Q)$. Any element of R/Q that is not a unit generates a proper ideal, which is contained in a maximal ideal, which again must be $\mathcal{N}(R/Q)$. Thus every element of R/Q is either a unit or nilpotent. Since a zero-divisor cannot be a unit, every zero-divisor of R/Q is nilpotent, so Q is primary. ♣

8.6.6 Corollary

If M is a maximal ideal, then M^n is M-primary for all $n = 1, 2, \ldots$.

Proof. By (8.6.3), the radical of M^n is M, and the result follows from (8.6.5). ♣

Here is another useful property.

8.6.7 Proposition

If Q is a finite intersection of P-primary ideals Q_i, $i = 1, \ldots, n$, then Q is P-primary.

Proof. First note that the radical of a finite intersection of ideals is the intersection of the radicals (see Problem 1). It follows that the radical of Q is P, and it remains to show that Q is primary. If $ab \in Q$ but $a \notin Q$, then for some i we have $a \notin Q_i$. Since Q_i is P-primary, b belongs to $P = \sqrt{Q_i}$. But then some power of b belongs to Q. ♣

We are going to show that in a Noetherian ring, every proper ideal I has a primary decomposition, that is, I can be expressed as a finite intersection of primary ideals.

8.6.8 Lemma

Call an ideal I *irreducible* if for any ideals J and K, $I = J \cap K$ implies that $I = J$ or $I = K$. If R is Noetherian, then every ideal of R is a finite intersection of irreducible ideals.

Proof. Suppose that the collection $\mathcal{S}$ of all ideals that cannot be so expressed is nonempty. Since R is Noetherian, $\mathcal{S}$ has a maximal element I, necessarily reducible. Let $I = J \cap K$, where I is properly contained in both J and K. By maximality of I, the ideals J and K are finite intersections of irreducible ideals, and consequently so is I, contradicting $I \in \mathcal{S}$. ♣

If we can show that every irreducible proper ideal is primary, we then have the desired primary decomposition. Let us focus on the chain of reasoning we will follow. If I is an irreducible proper ideal of R, then by the correspondence theorem, 0 is an irreducible ideal of the Noetherian ring R/I. If we can show that 0 is primary in R/I, then again by the correspondence theorem, I is primary in R.

8.6.9 Primary Decomposition Theorem

Every proper ideal in a Noetherian ring R has a primary decomposition. (We can drop the word "proper" if we regard R as the intersection of the empty collection of primary ideals.)

Proof. By the above discussion, it suffices to show that if 0 is an irreducible ideal of R, then it is primary. Let $ab = 0$ with $a \neq 0$. Since R is Noetherian, the sequence of annihilators

$$\operatorname{ann} b \subseteq \operatorname{ann} b^2 \subseteq \operatorname{ann} b^3 \subseteq \cdots$$

stabilizes, so $\operatorname{ann} b^n = \operatorname{ann} b^{n+1}$ for some n. If we can show that

$$(a) \cap (b^n) = 0$$

we are finished, because $a \neq 0$ and the zero ideal is irreducible (by hypothesis). Thus let $x = ca = db^n$ for some $c, d \in R$. Then $bx = cab = db^{n+1} = 0$ (because $ab = 0$), so d annihilates b^{n+1}, hence d annihilates b^n. Thus $x = db^n = 0$. ♣

Problems For Section 8.6

1. If $I_1, \ldots, I_n$ are arbitrary ideals, show that
$$\sqrt{\bigcap_{i=1}^{n} I_i} = \bigcap_{i=1}^{n} \sqrt{I}_i.$$
2. Let I be the ideal $(XY - Z^2)$ in $k[X, Y, Z]$, where k is any field, and let $R = k[X, Y, Z]/I$. If P is the ideal $(X + I, Z + I)$, show that P is prime.
3. Continuing Problem 2, show that P^2, whose radical is prime by (8.6.3) and which is a power of a prime, is nevertheless not primary.
4. Let $R = k[X, Y]$, and let $P_1 = (X)$, $P_2 = (X, Y)$, $Q = (X^2, Y)$. Show that P_1 is prime and P_2^2 and Q are P_2-primary.
5. Continuing Problem 4, let $I = (X^2, XY)$. Show that $P_1 \cap P_2^2$ and $P_1 \cap Q$ are both primary decompositions of I.

Notice that the radicals of the components of the primary decomposition (referred to as the primes *associated* with I) are P_1 and P_2 in both cases. [P_1 is prime, so $\sqrt{P}_1 = P_1$; $P_2 \subseteq \sqrt{Q}$ and P_2 is maximal, so $P_2 = \sqrt{Q}$;] Uniqueness questions involving primary decompositions are treated in detail in textbooks on commutative algebra.

6. We have seen in Problem 5 of Section 8.4 that every radical ideal in $R = k[X_1, \ldots, X_n]$ is the intersection of finitely many prime ideals. Show that this result holds in an arbitrary Noetherian ring R.

7. Let $R = k[X, Y]$ and let I_n be the ideal (X^3, XY, Y^n). Show that for every positive integer n, I_n is a primary ideal of R.

8.7 Tensor Product of Modules Over a Commutative Ring

8.7.1 Motivation

In many areas of algebra and its applications, it is useful to multiply, in a sensible way, an element x of an R-module M by an element y of an R-module N. In group representation theory, M and N are free modules, in fact finite-dimensional vector spaces, with bases $\{x_i\}$ and $\{y_j\}$. Thus if we specify that multiplication is linear in each variable, then we need only specify products of x_i and y_j. We require that the these products, to be denoted by $x_i \otimes y_j$, form a basis for a new R-module T.

If $f\colon R \to S$ is a ring homomorphism and M is an S-module, then M becomes an R-module via $rx = f(r)x$, $r \in R$, $x \in M$. This is known as restriction of scalars. In algebraic topology and algebraic number theory, it is often desirable to reverse this process. If M is an R-module, we want to extend the given multiplication rx, $r \in R$, $x \in M$, to multiplication of an arbitrary $s \in S$ by $x \in M$. This is known as extension of scalars, and it becomes possible with the aid of the tensor product construction.

The tensor product arises in algebraic geometry in the following way. Let M be the coordinate ring of a variety V in affine space A^m, in other words, M is the set of all polynomial functions from V to the base field k. Let N be the coordinate ring of the variety W in A^n. Then the cartesian product $V \times W$ is a variety in A^{m+n}, and its coordinate ring turns out to be the tensor product of M and N.

Let's return to the first example above, where M and N are free modules with bases $\{x_i\}$ and $\{y_j\}$. Suppose that f is a bilinear map from $M \times N$ to an R-module P. (In other words, f is R-linear in each variable.) Information about f can be completely encoded into a function g of one variable, where g is an R-module homomorphism from T to P. We take $g(x_i \otimes y_j) = f(x_i, y_j)$ and extend by linearity. Thus f is the composition of the bilinear map h from $M \times N$ to T specified by $(x_i, y_j) \to x_i \otimes y_j$, followed by g. To summarize:

Every bilinear mapping on $M \times N$ can be factored through T.

The R-module T is called the tensor product of M and N, and we write $T = M \otimes_R N$. We are going to construct a tensor product of arbitrary modules over a commutative ring, and sketch the generalization to noncommutative rings.

8.7.2 Definitions and Comments

Let M and N be arbitrary R-modules, and let F be a free R-module with basis $M \times N$. Let G be the submodule of F generated by the "relations"

$$(x + x', y) - (x, y) - (x', y); \quad (x, y + y') - (x, y) - (x, y');$$
$$(rx, y) - r(x, y); \quad (x, ry) - r(x, y)$$

where $x, x' \in M$, $y, y' \in N$, $r \in R$. Define the *tensor product* of M and N (over R) as

$$T = M \otimes_R N = F/G$$

and denote the element $(x, y) + G$ of T by $x \otimes y$. Thus the general element of T is a finite sum of the form

$$t = \sum_i x_i \otimes y_i \tag{1}$$

with $x_i \in M$ and $y_i \in N$. It is important to note that the representation (1) is not necessarily unique.

The relations force $x \otimes y$ to be linear in each variable, so that

$$x \otimes (y + y') = x \otimes y + x \otimes y', \ (x + x') \otimes y = x \otimes y + x' \otimes y, \tag{2}$$
$$r(x \otimes y) = rx \otimes y = x \otimes ry. \tag{3}$$

See Problem 1 for details. Now if f is a bilinear mapping from $M \times N$ to the R-module P, then f extends uniquely to a homomorphism from F to P, also called f. Bilinearity means that the kernel of f contains G, so by the factor theorem, there is a unique R-homomorphism $g\colon T \to P$ such that $g(x \otimes y) = f(x, y)$ for all $x \in M$, $y \in N$. As in (8.7.1), if we compose the bilinear map $h\colon (x, y) \to x \otimes y$ with g, the result is f. Again, we say that

Every bilinear mapping on $M \times N$ can be factored through T.

We have emphasized this sentence, known as a *universal mapping property* (abbreviated UMP), because along with equations (1), (2) and (3), it indicates how the tensor product is applied in practice. The detailed construction we have just gone through can now be forgotten. In fact any two R-modules that satisfy the universal mapping property are isomorphic. The precise statement and proof of this result will be developed in the exercises.

In a similar fashion, using multilinear rather than bilinear maps, we can define the tensor product of any finite number of R-modules. [In physics and differential geometry, a tensor is a multilinear map on a product $M_1 \times \cdots \times M_r$, where each M_i is either a finite-dimensional vector space V or its dual space V^*. This suggests where the terminology "tensor product" comes from.]

In the discussion to follow, M, N and P are R-modules. The ring R is assumed fixed, and we will usually write $\otimes$ rather than $\otimes_R$.

8.7.3 Proposition

$M \otimes N \cong N \otimes M$.

Proof. Define a bilinear mapping $f\colon M \times N \to N \otimes M$ by $f(x,y) = y \otimes x$. By the UMP, there is a homomorphism $g\colon M \otimes N \to N \otimes M$ such that $g(x \otimes y) = y \otimes x$. Similarly, there is a homomorphism $g'\colon N \otimes M \to M \otimes N$ with $g'(y \otimes x) = x \otimes y$. Thus g is an isomorphism (with inverse g'). ♣

8.7.4 Proposition

$M \otimes (N \otimes P) \cong (M \otimes N) \otimes P$.

Proof. Define $f\colon M \times N \times P \to (M \otimes N) \otimes P$ by $f(x,y,z) = (x \otimes y) \otimes z$. The UMP produces $g\colon M \times (N \otimes P) \to (M \otimes N) \otimes P$ with $g((x,(y \otimes z))) = (x \otimes y) \otimes z$. [We are applying the UMP for each fixed $x \in M$, and assembling the maps to produce g.] Since g is bilinear (by Equations (2) and (3)), the UMP yields $h\colon M \otimes (N \otimes P) \to (M \otimes N) \otimes P$ with $h(x \otimes (y \otimes z)) = (x \otimes y) \otimes z$. Exactly as in (8.7.3), we can construct the inverse of h, so h is the desired isomorphism. ♣

8.7.5 Proposition

$M \otimes (N \oplus P) \cong (M \otimes N) \oplus (M \otimes P)$.

Proof. Let f be an arbitrary bilinear mapping from $M \times (N \oplus P)$ to Q. If $x \in M$, $y \in N$, $z \in P$, then $f(x, y+z) = f(x,y) + f(x,z)$. The UMP gives homomorphisms $g_1\colon M \otimes N \to Q$ and $g_2\colon M \otimes P \to Q$ such that $g_1(x \otimes y) = f(x,y)$ and $g_2(x \otimes z) = f(x,z)$. The maps g_1 and g_2 combine to give $g\colon (M \otimes N) \oplus (M \otimes P) \to Q$ such that

$$g((x \otimes y) + (x' \otimes z)) = g_1(x \otimes y) + g_2(x' \otimes z).$$

In particular, with $x' = x$,

$$g((x \otimes y) + (x \otimes z)) = f(x, y+z),$$

so if $h\colon M \times (N \oplus P) \to M \otimes (N \oplus P)$ is defined by

$$h(x, y+z) = (x \otimes y) + (x \otimes z),$$

then $f = gh$. Thus $(M \otimes N) \oplus (M \otimes P)$ satisfies the universal mapping property, hence must be isomorphic to the tensor product. ♣

8.7.6 Proposition

Regarding R as a module over itself, $R \otimes_R M \cong M$.

Proof. The map $(r,x) \to rx$ of $R \times M \to M$ is bilinear, so there is a homomorphism $g\colon R \otimes M \to M$ such that $g(r \otimes x) = rx$. Define $h\colon M \to R \otimes M$ by $h(x) = 1 \otimes x$. Then $h(rx) = 1 \otimes rx = r1 \otimes x = r \otimes x$. Thus g is an isomorphism (with inverse h). ♣

8.7.7 Corollary

Let R^m be the direct sum of m copies of R, and M^m the direct sum of m copies of M. Then $R^m \otimes M \cong M^m$.

Proof. By (8.7.5), $R^m \otimes M$ is isomorphic to the direct sum of m copies of $R \otimes M$, which is isomorphic to M^m by (8.7.6). ♣

8.7.8 Proposition

$R^m \otimes R^n \cong R^{mn}$. Moreover, if $\{x_1, \ldots, x_m\}$ is a basis for R^m and $\{y_1, \ldots, y_n\}$ is a basis for R^n, then $\{x_i \otimes y_j, i = 1, \ldots, m, j = 1, \ldots, n\}$ is a basis for R^{mn}.

Proof. This follows from the discussion in (8.7.1). [The first assertion can also be proved by taking $M = R^n$ in (8.7.7).] ♣

8.7.9 Tensor Product of Homomorphisms

Let $f_1 \colon M_1 \to N_1$ and $f_2 \colon M_2 \to N_2$ be R-module homomorphisms. The map $(x_1, x_2) \to f_1(x_1) \otimes f_2(x_2)$ of $M_1 \times M_2$ into $N_1 \otimes N_2$ is bilinear, and induces a unique $f \colon M_1 \otimes M_2 \to N_1 \otimes N_2$ such that

$$f(x_1 \otimes x_2) = f_1(x_1) \otimes f_2(x_2),\ x_1 \in M_1, x_2 \in M_2.$$

We write $f = f_1 \otimes f_2$, and call it the *tensor product* of f_1 and f_2. Similarly, if $g_1 \colon N_1 \to P_1$ and $g_2 \colon N_2 \to P_2$, then we can compose $g_1 \otimes g_2$ with $f_1 \otimes f_2$, and

$$(g_1 \otimes g_2)(f_1 \otimes f_2)(x_1 \otimes x_2) = g_1 f_1(x_1) \otimes g_2 f_2(x_2),$$

hence

$$(g_1 \otimes g_2) \circ (f_1 \otimes f_2) = (g_1 \circ f_1) \otimes (g_2 \circ f_2).$$

When $M_1 = N_1 = V$, a free R-module of rank m, and $M_2 = N_2 = W$, a free R-module of rank n, there is a very concrete interpretation of the tensor product of the endomorphisms $f \colon V \to V$ and $g \colon W \to W$. If f is represented by the matrix A and g by the matrix B, then the action of f and g on basis elements is given by

$$f(v_j) = \sum_i a_{ij} v_i, \quad g(w_l) = \sum_k b_{kl} w_k$$

where i and j range from 1 to m, and k and l range from 1 to n. Thus

$$(f \otimes g)(v_j \otimes w_l) = f(v_j) \otimes g(w_l) = \sum_{i,k} a_{ij} b_{kl} (v_i \otimes w_k).$$

The mn by mn matrix representing the endomorphism $f \otimes g \colon V \otimes W \to V \otimes W$ is denoted by $A \otimes B$ and called the *tensor product* or *Kronecker product* of A and B. It is given by

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ \vdots & & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{bmatrix}.$$

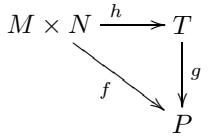
The ordering of the basis of $V \otimes W$ is

$$v_1 \otimes w_1, \ldots, v_1 \otimes w_n, \ldots, v_m \otimes w_1, \ldots, v_m \otimes w_n.$$

To determine the column of $A \otimes B$ corresponding to $v_j \otimes w_l$, locate the $a_{ij}B$ block ($i = 1, \ldots, m$; j fixed) and proceed to column l of B. As we move down this column, the indices i and k vary according to the above ordering of basis elements. If this road map is not clear, perhaps writing out the entire matrix for $m = 2$ and $n = 3$ will help.

Problems For Section 8.7

1. Verify Equations (2) and (3) of (8.7.2).
2. If m and n are relatively prime, show that $\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n = 0$.
3. If A is a finite abelian group and $\mathbb{Q}$ is the additive group of rationals, show that $A \otimes_{\mathbb{Z}} \mathbb{Q} = 0$. Generalize to a wider class of abelian groups A.
4. The definition of $M \otimes_R N$ via a universal mapping property is as follows. The tensor product is an R-module T along with a bilinear map $h\colon M \times N \to T$ such that given any bilinear map $f\colon M \times N \to P$, there is a unique R-homomorphism $g\colon T \to P$ such that $f = gh$. See the diagram below.



   Now suppose that another R-module T', along with a bilinear mapping $h'\colon M \times N \to T'$, satisfies the universal mapping property. Using the above diagram with $P = T'$ and f replaced by h', we get a unique homomorphism $g\colon T \to T'$ such that $h' = gh$. Reversing the roles of T and T', we get $g'\colon T' \to T$ such that $h = g'h'$.

   Show that T and T' are isomorphic.
5. Consider the element $n \otimes x$ in $\mathbb{Z} \otimes \mathbb{Z}_n$, where x is any element of $\mathbb{Z}_n$ and we are tensoring over $\mathbb{Z}$, i.e., $R = \mathbb{Z}$. Show that $n \otimes x = 0$.
6. Continuing Problem 5, take $x \neq 0$ and regard $n \otimes x$ as an element of $n\mathbb{Z} \otimes \mathbb{Z}_n$ rather than $\mathbb{Z} \otimes \mathbb{Z}_n$. Show that $n \otimes x \neq 0$.
7. Let M, N, M', N' be arbitrary R-modules, where R is a commutative ring. Show that the tensor product of homomorphisms induces a linear map from $\mathrm{Hom}_R(M, M') \otimes_R \mathrm{Hom}_R(N, N')$ to $\mathrm{Hom}_R(M \otimes_R N, M' \otimes_R N')$.
8. Let M be a free R-module of rank m, and N a free R-module of rank n. Show that there is an R-module isomorphism of $\mathrm{End}_R(M) \otimes_R \mathrm{End}_R(N)$ and $\mathrm{End}_R(M \otimes N)$.

8.8 General Tensor Products

We now consider tensor products of modules over noncommutative rings. A natural question is "Why not simply repeat the construction of (8.7.2) for an arbitrary ring R?".

But this construction forces

$$rx \otimes sy = r(x \otimes sy) = rs(x \otimes y)$$

and

$$rx \otimes sy = s(rx \otimes y) = sr(x \otimes y)$$

which cannot hold in general if R is noncommutative. A solution is to modify the construction so that the tensor product T is only an abelian group. Later we can investigate conditions under which T has a module structure as well.

8.8.1 Definitions and Comments

Let M be a right R-module and N a left R-module. (We often abbreviate this as M_R and ${}_RN$.) Let $f\colon M \times N \to P$, where P is an abelian group. The map f is *biadditive* if it is additive in each variable, that is, $f(x+x', y) = f(x, y)+f(x', y)$ and $f(x, y+y') = f(x, y)+f(x, y')$ for all $x, x' \in M$, $y, y' \in N$. The map f is *R-balanced* if $f(xr, y) = f(x, ry)$ for all $x \in M$, $y \in N$, $r \in R$. As before, the key idea is the *universal mapping property*: Every biadditive, R-balanced map can be factored through the tensor product.

8.8.2 Construction of the General Tensor Product

If M_R and ${}_RN$, let F be the free abelian group with basis $M \times N$. Let G be the subgroup of R generated by the relations

$$\begin{aligned}&(x + x', y) - (x, y) - (x', y);\\ &(x, y + y') - (x, y) - (x, y');\\ &(xr, y) - (x, ry)\end{aligned}$$

where $x, x' \in M$, $y, y' \in N$, $r \in R$. Define the *tensor product* of M and N over R as

$$T = M \otimes_R N = F/G$$

and denote the element $(x, y) + G$ of T by $x \otimes y$. Thus the general element of T is a finite sum of the form

$$t = \sum_i x_i \otimes y_i. \tag{1}$$

The relations force the map $h\colon (x, y) \to x \otimes y$ of $M \times N$ into T to be biadditive and R-balanced, so that

$$x \otimes (y + y') = x \otimes y + x \otimes y',\ (x + x') \otimes y = x \otimes y + x' \otimes y, \tag{2}$$

$$xr \otimes y = x \otimes ry. \tag{3}$$

If f is a biadditive, R-balanced mapping from $M \times N$ to the abelian group P, then f extends uniquely to an abelian group homomorphism from F to P, also called f. Since f is biadditive and R-balanced, the kernel of f contains G, so by the factor theorem there is a unique abelian group homomorphism $g\colon T \to P$ such that $g(x \otimes y) = f(x, y)$ for all $x \in M$, $y \in N$. Consequently, $gh = f$ and we have the universal mapping property:

Every biadditive, R-balanced mapping on $M \times N$ can be factored through T.

As before, any two abelian groups that satisfy the universal mapping property are isomorphic.

8.8.3 Bimodules

Let R and S be arbitrary rings. We say that M is an $S - R$ *bimodule* if M is both a left S-module and a right R-module, and in addition a compatibility condition is satisfied: $(sx)r = s(xr)$ for all $s \in S$, $r \in R$. We often abbreviate this as ${}_SM_R$.

If $f\colon R \to S$ is a ring homomorphism, then S is a left S-module, and also a right R-module by restriction of scalars, as in (8.7.1). The compatibility condition is satisfied: $(sx)r = sxf(r) = s(xr)$. Therefore S is an $S - R$ bimodule.

8.8.4 Proposition

If ${}_SM_R$ and ${}_RN_T$, then $M \otimes_R N$ is an $S - T$ bimodule.

Proof. Fix $s \in S$. The map $(x, y) \to sx \otimes y$ of $M \times N$ into $M \otimes_R N$ is biadditive and R-balanced. The latter holds because by the compatibility condition in the bimodule property of M, along with (3) of (8.8.2),

$$s(xr) \otimes y = (sx)r \otimes y = sx \otimes ry.$$

Thus there is an abelian group endomorphism on $M \otimes_R N$ such that $x \otimes y \to sx \otimes y$, and we use this to define scalar multiplication on the left by s. A symmetrical argument yields scalar multiplication on the right by t. To check the compatibility condition,

$$[s(x \otimes y)]t = (sx \otimes y)t = sx \otimes yt = s(x \otimes yt) = s[(x \otimes y)t]. \quad \clubsuit$$

8.8.5 Corollary

If ${}_SM_R$ and ${}_RN$, then $M \otimes_R N$ is a left S-module. If M_R and ${}_RN_T$, then $M \otimes_R N$ is a right T-module.

Proof. The point is that every module is, in particular, an abelian group, hence a $\mathbb{Z}$-module. Thus for the first statement, take $T = \mathbb{Z}$ in (8.8.4), and for the second statement, take $S = \mathbb{Z}$. $\clubsuit$

8.8.6 Extensions

As in Section 8.7, we can define the tensor product of any finite number of modules using multiadditive maps (additive in each variable) that are balanced. For example, suppose that M_R, ${}_RN_S$ and ${}_SP$. If $f\colon M \times N \times P \to G$, where G is an abelian group, the condition of balance is

$$f(xr, y, z) = f(x, ry, z) \text{ and } f(x, ys, z) = f(x, y, sz)$$

for all $x \in M$, $y \in N$, $z \in P$, $r \in R$, $s \in S$. An argument similar to the proof of (8.7.4) shows that

(a) $M \otimes_R N \otimes_S P \cong (M \otimes_R N) \otimes_S P \cong M \otimes_R (N \otimes_S P)$.

If M is a right R-module, and N and P are left R-modules, then

(b) $M \otimes_R (N \oplus P) \cong (M \otimes_R N) \oplus (M \otimes_R P)$.

This is proved as in (8.7.5), in fact the result can be extended to the direct sum of an arbitrary (not necessarily finite) number of left R-modules.

If M is a left R-module, then exactly as in (8.7.6) and (8.7.7), we have

(c) $R \otimes_R M \cong M$ and

(d) $R^m \otimes M \cong M^m$.

Let M_1 and M_2 be right R-modules, and let N_1 and N_2 be left R-modules. If $f_1 \colon M_1 \to N_1$ and $f_2 \colon M_2 \to N_2$ are R-module homomorphisms, the tensor product $f_1 \otimes f_2$ can be defined exactly as in (8.7.9). As before, the key property is

$$(f_1 \otimes f_2)(x_1 \otimes x_2) = f_1(x_1) \otimes f_2(x_2)$$

for all $x_1 \in M_1$, $x_2 \in M_2$.

8.8.7 Tensor Product of Algebras

If A and B are algebras over the commutative ring R, then the tensor product $A \otimes_R B$ becomes an R-algebra if we define multiplication appropriately. Consider the map of $A \times B \times A \times B$ into $A \otimes_R B$ given by

$$(a, b, a', b') \to aa' \otimes bb', \ a, a' \in A, \ b, b' \in B.$$

The map is 4-linear, so it factors through the tensor product to give an R-module homomorphism $g \colon A \otimes B \otimes A \otimes B \to A \otimes B$ such that

$$g(a \otimes b \otimes a' \otimes b') = aa' \otimes bb'.$$

Now let $h \colon (A \otimes B) \times (A \otimes B) \to A \otimes B \otimes A \otimes B$ be the bilinear map given by

$$h(u, v) = u \otimes v.$$

If we apply h followed by g, the result is a bilinear map $f \colon (A \otimes B) \times (A \otimes B) \to A \otimes B$ with

$$f(a \otimes b, a' \otimes b') = aa' \otimes bb',$$

and this defines our multiplication $(a \otimes b)(a' \otimes b')$ on $A \otimes B$. The multiplicative identity is $1_A \otimes 1_B$, and the distributive laws can be checked routinely. Thus $A \otimes_R B$ is a ring that is also an R-module. To check the compatibility condition, note that if $r \in R$, $a, a' \in A$, $b, b' \in B$, then

$$r[(a \otimes b)(a' \otimes b')] = [r(a \otimes b)](a' \otimes b') = (a \otimes b)[r(a' \otimes b')];$$

all three of these expressions coincide with $raa' \otimes bb' = aa' \otimes rbb'$.

Problems For Section 8.8

We will use the tensor product to define the *exterior algebra* of an R-module M, where R is a commutative ring. If p is a positive integer, we form the tensor product $M \otimes_R \cdots \otimes_R M$ of M with itself p times, denoted by $M^{\otimes p}$. Let N be the submodule of $M^{\otimes p}$ generated by those elements $x_1 \otimes \cdots \otimes x_p$, with $x_i \in M$ for all i, such that $x_i = x_j$ for some $i \neq j$. The p^{th} *exterior power* of M is defined as

$$\Lambda^p M = M^{\otimes p}/N.$$

In most applications, M is a free R-module with a finite basis $x_1, \ldots, x_n$ (with $1 \leq p \leq n$), and we will only consider this case. To simplify the notation, we write the element $a \otimes b \otimes \cdots \otimes c + N$ of $\Lambda^p M$ as $ab \cdots c$. (The usual notation is $a \wedge b \wedge \cdots \wedge c$.)

1. Let $y_1, \ldots, y_p \in M$. Show that if y_i and y_j are interchanged in the product $y_1 \cdots y_p$, then the product is multiplied by -1.
2. Show that the products $x_{i_1} \cdots x_{i_p}$, where $i_1 < \cdots < i_p$, span $\Lambda^p M$.
3. Let $f\colon M^p \to Q$ be a multilinear map from M^p to the R-module Q, and assume that f is *alternating*, that is, $f(m_1, \ldots, m_p) = 0$ if $m_i = m_j$ for some $i \neq j$. Show that f can be factored through $\Lambda^p M$, in other words, there is a unique R-homomorphism $g\colon \Lambda^p M \to Q$ such that $g(y_1 \cdots y_p) = f(y_1, \ldots, y_p)$.

Let $y_i = \sum_{j=1}^n a_{ij} x_j$, $i = 1, \ldots, n$. Since $\{x_1, \ldots, x_n\}$ is a basis for M, y_i can be identified with row i of A. By the basic properties of determinants, the map $f(y_1, \ldots, y_n) = \det A$ is multilinear and alternating, and $f(x_1, \ldots, x_n) = 1$, the determinant of the identity matrix.

4. Show that $x_1 \cdots x_n \neq 0$ in $\Lambda^n M$, and that $\{x_1 \cdots x_n\}$ is a basis for $\Lambda^n M$.

Let $I = \{i_1, \cdots, i_p\}$, where $i_1 < \cdots < i_p$, and write the product $x_{i_1} \cdots x_{i_p}$ as x_I. Let J be the complementary set of indices. (For example, if $n = 5$, $p = 3$, and $I = \{1, 2, 4\}$, then $J = \{3, 5\}$.) Any equation involving $x_I \in \Lambda^p M$ can be multiplied by x_J to produce a valid equation in $\Lambda^n M$.

5. Show that the products x_I of Problem 2 are linearly independent, so that $\Lambda^p M$ is a free R-module of rank $\binom{n}{p}$.

Roughly speaking, the exterior algebra of M consists of the $\Lambda^p M$ for all p. By construction, $\Lambda^1 M = M$ and $\Lambda^p M = 0$ for $p > n$, since some index must repeat in any element of $\Lambda^p M$. By convention, we take $\Lambda^0 M = R$. Formally, the exterior powers are assembled into a *graded R-algebra*

$$A_0 \oplus A_1 \oplus A_2 \oplus \cdots$$

where $A_p = \Lambda^p M$. Multiplication is defined as in the discussion after Problem 4, that is, if $y_1 \cdots y_p \in A_p$ and $z_1 \cdots z_q \in A_q$, then the *exterior product* $y_1 \cdots y_p z_1 \cdots z_q$ belongs to A_{p+q}.

A ring R is said to be *graded* if, as an abelian group, it is the direct sum of subgroups R_n, $n = 0, 1, 2, \ldots$, with $R_m R_n \subseteq R_{n+m}$ for all $m, n \geq 0$. [Example: $R =$

$k[X_1, \ldots, X_n]$, R_n = all homogeneous polynomials of degree n.] By definition, R_0 is a subring of R (because $R_0 R_0 \subseteq R_0$), and each R_n is a module over R_0 (because $R_0 R_n \subseteq R_n$).

6. Suppose that the ideal $I = \oplus_{n \geq 1} R_n$ is generated over R by finitely many elements $x_1, \ldots, x_r$, with $x_i \in R_{n_i}$. Show that $R_n \subseteq S = R_0[x_1, \ldots, x_r]$ for all $n = 0, 1, \ldots$, so that $R = S$.
7. Show that R is a Noetherian ring if and only if R_0 is Noetherian and R is a finitely generated R_0-algebra.