COMMUTATIVE RINGS

Course Notes for 18.732
Spring, 1966
M.I.T.
by M. Artin

CONTENTS

These notes are for the second term of a first year graduate algebra course, which presupposed an undergraduate course of some sort. The first term consisted of a "review" of group theory, then field theory (galois theory) and Wedderburn theory and some material on representations of finite groups. Lang's book was used as a text. The second term is devoted entirely to commutative ring theory.

I think the choice of material was fairly good, i.e., I would not change it basically. However, I would make the following two changes in the ordering:

(i) The students didn't like to accept without proof a naive description of the spectrum of a polynomial ring, etc. in Section 1. I encountered very strong resistance to this, and of course they are absolutely right. Therefore, I would move Section 8, in which the material was presented, to the beginning.

(ii) I would do the flat descent early, before the sheaf theory on the spectrum. It is true that they will not fully understand the material, especially the proof, right away. That is why I postponed it in the course. However, I found that they couldn't follow the proof of the sheaf axiom (pp. 3.7-3.9) anyway, hence why not do it right, if at all. That way, the descent theory can be used to prove the sheaf axiom, and so it has some application. I would soften the presentation somewhat, and suppress Section 9 entirely, introducing as a section of 10 what is explicitly needed.

The arrangement, with these changes, would be roughly as follows:

Section 1

2 A, B, C

6 A, B

8 except the last section, somewhat expanded.

10 (+ essential part of 9), softened up.

end of 2 and 3

4, 5

rest of 6, and last section of 8

7

Section 7 could be put anywhere, actually, e.g. between 8 and 10. Perhaps that is more natural.

THE SPECTRUM OF A COMMUTATIVE RING

We will work in the category of commutative rings having a multiplicative unit element 1. Homomorphisms are assumed to send 1 to 1.

A. Ideals.

Let R be a ring. Recall that an ideal I of R is a subset which is a subgroup for the additive law in R and such that $x \in I$, $a \in R \Rightarrow ax \in I$. An ideal $p \neq R$ is a prime ideal if it has the additional property

(1) $$ab \in p \Rightarrow a \in p \quad \text{or} \quad b \in p.$$

This is equivalent with saying that the residue classes R/p form an integral domain (= ring without zero divisors and with $1 \neq 0$). For, if we denote by $\bar{x}$ the residue class of an element x then the above property reads

$$\overline{ab} = 0 \Rightarrow \bar{a} = 0 \quad \text{or} \quad \bar{b} = 0,$$

and the condition $p \neq R$ insures that $1 \neq 0$ in R/p.

An ideal m of R is maximal if $m \neq R$ and if there is no ideal $\neq R$ which is larger than m. It follows from Zorn's lemma that every ideal $\neq R$ is contained in a maximal ideal.

A maximal ideal is prime. For, let I be any ideal which is not prime, so that there are elements $a,b \in R$ not in I but with $ab \in I$. Then the ideal $(a) + I$ generated by a, I is strictly larger than I. But 1 is not in $(a) + I$, since from

$$1 = ra + x \qquad r \in R,\ x \in I$$

we get

$$b = rab + sx \in I,$$

a contradiction. Thus $(a) + I \neq R$, and so I is not a maximal ideal.

B. The spectrum.

Definition 1: The spectrum of a ring R, denoted Spec R, is the set of prime ideals of R.

Let $X = \operatorname{Spec} R$. Then an element $x \in X$ is a prime ideal of R. However, we usually want to think of x as a "point" of X, and when we want to consider the prime ideal, we will write it as p_x, meaning the "prime ideal corresponding to the point $x \in X$". We leave it to the reader to arrange the logical absurdity thus introduced to his liking.

Let $x \in X$. The residue class ring R/p_x is an integral domain, and hence has a field of fractions which we will denote by $k(x)$. If a is an element of R, its residue modulo p_x determines an element of $k(x)$ which we will denote by $a(x)$, and will call the value of a at the point x. Thus we can view a as a sort of function on $X = \mathrm{Spec}\ R$, associating with x the element $a(x)$ of the field $k(x)$ (to be thought of as a "number"). Of course, the field $k(x)$ in which the values are taken varies with x.

In particular, we know what it means for a to be _zero at the point_ $x \in X$. This just means that $a(x) = 0$, which is the same thing as saying that a is an element of p_x.

C. _The Zariski Topology._

Let S be a subset of R. The _variety of_ S, or _locus of zeros_ of S is

(1) $$V(S) = \{x \in X | S \subset p_x\}$$
$$= \{x \in X | \text{ every element of } S \text{ is zero at } x\}.$$

Let I be the ideal generated by S. Clearly any ideal p_x which contains S also contains I, and conversely. Hence

(2) $$V(S) = V(I).$$

The following relations are trivial:

(3) $$S \supset S' \Rightarrow V(S) \subset V(S').$$

(4) $$V(\emptyset) = V(0) = X$$
$$V(R) = V(1) = \emptyset$$

(5) $$V(\bigcup_i S_i) = \bigcap_i V(S_i) \quad \text{for a family of sets } S_i.$$

(6) $$V(\sum_i I_i) = \bigcap_i V(I_i) \quad \text{for a family of ideals } I_i.$$

Less obvious is the following fact: If I and J are ideals then

(7) $V(I \cap J) = V(I) \cup V(J)$.

This follows immediately from

Lemma 8: If a prime ideal p contains $I \cap J$, where I and J are ideals, then $p \supset I$ or $p \supset J$.

proof: Suppose that p contains neither I nor J, and let $a \in I$, $b \in J$ be elements not in p. Then $ab \in I \cap J$, hence $ab \in p$. Since p is prime, either a or b is in p, a contradiction.

Recall that a topology on a set is a collection of subsets, called closed subsets which is closed under arbitrary intersections and finite unions. Relations (2), (4)-(7) above show that the set of subsets of $X = \operatorname{Spec} R$ which are of the form $V(S)$ for some S form a topology on $\operatorname{Spec} R$. This topology is known as the Zariski topology.

Proposition 9: $\operatorname{Spec} R$ is quasi-compact for the Zariski topology, i.e., if it is covered by a set of open sets then finitely many cover it. Equivalently, if the intersection of a set of closed sets is empty, then there is a finite number of the closed sets whose intersection is empty.

proof: $\emptyset = \bigcap_i V(S_i)$ means $\emptyset = V(\bigcup_i S_i)$, which means no prime ideal contains $\bigcup_i S_i$.

Since every proper ideal is contained in a maximal ideal, this means that the ideal generated by $\bigcup_i S_i$ is the whole ring, i.e., 1 is a linear combination of some elements of some $\bigcup_i S_i$. Thus a finite number of the S_i generate the whole ring, and so the intersection of the varieties of this finite set is empty.

Let $f:R \to R'$ be a homomorphism of rings, and let p' be a prime ideal of R'. The inverse image $p = f^{-1}(p') = \{a \in R \mid f(a) \in p'\}$ is a prime ideal, as is easily verified. Hence one obtains a map backwards

$$\text{(10)} \qquad \operatorname{Spec} R \xleftarrow{\ \phi\ } \operatorname{Spec} R'$$

by associating with a prime ideal p' of R' the prime ideal $f^{-1}(p')$ of R.

<u>Proposition 11:</u> The map ϕ is continuous for the Zariski topology.

proof: Let $C \subset \operatorname{Spec} R$ be a closed set. We need to show that $\phi^{-1}(C)$ is closed. Write $C = V(S)$. Then

$$\begin{aligned}\phi^{-1}(C) &= \{x' \in \operatorname{Spec} R' \mid f^{-1}(p_{x'}) \supset S\} \\ &= \{x' \mid p_{x'} \supset f(S)\} \\ &= V(f(S)), \text{ which is a closed set of } \operatorname{Spec} R'.\end{aligned}$$

Thus we have proved the formula

$$\text{(12)} \qquad \phi^{-1}(V(S)) = V(f(S)).$$

Suppose that $f: R \to \overline{R}$ is the canonical map of R to the residue class ring $\overline{R} = R/I$ for some ideal I of R. As is well known, the ideals of $\overline{R}$ are in one to one correspondence with those ideals of R which contain I, the correspondence being given by $\bar{J} \leftrightsquigarrow f^{-1}(\bar{J}) = J$. Clearly prime ideals correspond under this rule, whence

Corollary 13: Let $\bar{R} = R/I$, and let ϕ: Spec $\bar{R} \longrightarrow$ Spec R be the map induced by the canonical map $f: R \longrightarrow \bar{R}$. Then ϕ is a one to one map of Spec $\bar{R}$ onto $V(I)$.

It is easy to show that the Zariski topology on Spec $\bar{R}$ is actually induced by the Zariski topology on Spec R by this map. Thus Spec $\bar{R}$ is naturally homeomorphic to the closed subspace $V(I)$ of Spec R, and one frequently identifies the two spaces.

D. The radical of an ideal.

Each closed subset of $X =$ Spec R is of the form $V(I)$ for some ideal I of R. However the ideal I is in general not uniquely determined by its variety. A natural problem is to determine the ideals whose variety is a given closed subset, and we propose to study this question now.

Let Y be a subset of X, and let $\mathcal{J}(Y) = \bigcap_{x \in Y} p_x$. $\mathcal{J}(Y)$ is clearly an ideal of R, and we have

$$V(\mathcal{J}(Y)) \supset Y \qquad \text{for any } Y \subset X$$
$$\mathcal{J}(V(S)) \supset S \qquad \text{for any } S \subset R.$$

The radical of an ideal I of R is

(1) $\quad$ $\operatorname{rad} I = \{a \in R \mid a^n \in I \text{ for some } n\}$.

Proposition 2: $\operatorname{rad} I = \bigcap_{p \supset I} p$ is the intersection of prime ideals p containing I.

proof: Using the correspondence of prime ideals of R containing I and prime ideals of R/I, it is easy to reduce the problem to the corresponding one for the ring R/I and the ideal (0), i.e., to the case that I is the zero ideal. Now the radical of the zero ideal is just the set of nilpotent elements of the ring. This ideal is called the <u>nilradical</u> of R. We need therefore to show that the intersection of all prime ideals of R is the set of nilpotent elements of R, i.e., that an element of R is in every prime ideal, iff it is nilpotent. Since 0 is in any prime ideal p, it is clear that p contains every nilpotent.

Let x be an element of R which is not nilpotent, and let $\mathcal{S}$ be the set of all ideals $I \neq R$ such that $x^n \notin I$ for each integer n. $\mathcal{S}$ is not empty since (0) has the required property. If $\mathcal{S}$ is ordered by inclusion, it is easily seen to be an inductive set, hence by Zorn's lemma has a maximal element, say p.

I claim that p is a prime ideal. To see this, note first that the ideal $q = \{b | x^n b \in p, \text{ some } n\}$ does not contain x^n, hence is in $\mathcal{S}$, hence since it contains p must be equal to p. Now if $ab \in p$ but $a \notin p$, then the ideal $(a) + p$ is strictly larger than p, but unequal to R (since a maximal ideal is prime). Hence x^n is in $(a) + p$ for some n. But

$$x_n = ra + y \quad , r \in R, y \in p$$

yields

$$x^n b = rab + yb \in p,$$

hence $b \in p$. Thus p is a prime ideal. This completes the proof of the proposition.

Corollary 3: $\mathcal{I}(V(I)) = \text{rad } I$, and
$V(\mathcal{I}(Y)) = \text{closure of } Y$.

The first assertion is trivial from the proposition. For the second, note that $V(\mathcal{I}(Y))$ is closed, hence contains the closure $\overline{Y}$ of Y, and $V(\mathcal{I}(\overline{Y})) = V(\mathcal{I}(Y))$; Say $\overline{Y} = V(I)$. Then $V(\mathcal{I}(Y)) = V(\mathcal{I}(V(I))) = V(\text{rad } I) = V(I) = \overline{Y}$.

Corollary 4: Two ideals I, J of R have the same variety iff. $\text{rad } I = \text{rad } J$.

E. Products of rings, and decompositions of spectra.

If a topological space X is the union of two disjoint closed sets X_1 and X_2, one calls X_1, X_2 a decomposition of X and writes $X = X_1 \amalg X_2$. In the category of topological spaces, X is actually a coproduct of the spaces X_1, X_2. In particular, X is said to be connected if there is no such decomposition with X_1 and X_2 non-empty.

Theorem 1: There is a one to one correspondence between decompositions $X = X_1 \amalg X_2$ of $X = \text{Spec } R$ and decompositions $R = R_1 \times R_2$ of R into a product of rings, such that the canonical map $f_i : R \to R_i$ identifies $\text{Spec } R_i$ with the closed subset X_i of X.

proof: Suppose first that $R = R_1 \times R_2$, and let I_i be the kernel of the map $R \to R_i$. Then I_1, I_2 are comaximal ideals whose intersection is (0). Therefore if we set $X_i = V(I_i)$, the closed sets X_1 and X_2 are disjoint and their union is X (cf. C.4).

Suppose now that $X = X_1 \amalg X_2$, and write $X_i = V(I_i)$. Since $V(I_1 + I_2) = X_1 \cap X_2 = \emptyset$, we have $I_1 + I_2 = R$ (otherwise $I_1 + I_2$ would be in a maximal ideal). Moreover, since $V(I_1 \cap I_2) = X_1 \cup X_2 = X$, it follows that $\mathrm{rad}(I_1 \cap I_2) = \mathrm{rad}\ (0)$, i.e., that every element of $I_1 \cap I_2$ is nilpotent.

Write $1 = a_1 + a_2$ with $a_i \in I_i$. Then $(a_1a_2)^n = 0$ for large enough n since $a_1a_2 \in I_1 \cap I_2$. Now the ideals (a_i) and (a_i^n) have the same radical, hence $V(a_i) = V(a_i^n)$. Thus $V(a_1^n) \cap V(a_2^n) = \emptyset$, because $(a_1 + a_2) = R$. Now clearly $V(a_i^n) \supset X_i$. Hence $V(a_i^n) = X_i$,

Replacing I_i by (a_i^n), we are reduced to the situation where $I_1 + I_2 = R$ and $I_1I_2 = (0)$. Now for comaximal ideals, $I_1 \cap I_2 = I_1I_2$. Therefore $I_1 \cap I_2 = (0)$, and so $R \approx R/I_1 \times R/I_2$. Thus R is decomposed into a product. We leave the rest of the verification to you.

Corollary 2: X is connected if and only if R has no idempotents other than 0 and 1.

F. Irreducible closed sets.

A nonempty closed subset of a topological space is called irreducible if it is not the union of two proper closed subsets. The closure of a point is clearly irreducible.

Let $X = \operatorname{Spec} R$, and $x \in X$. The closure of x is just the irreducible set

$$(1) \qquad \overline{x} = \{y \in X \mid p_y \supset p_x\} = V(p_x).$$

Suppose that $C \subset X$ is an irreducible set. Then $\mathcal{I}(C)$ is a prime ideal. For, if $ab \in \mathcal{I}(C)$ then

$$V(a) \cup V(b) \supset C, \text{ hence}$$

$$C = (V(a) \cap C) \cup (V(b) \cap C).$$

Since C is irreducible,

$$V(a) \supset C \text{ or } V(b) \supset C, \text{ whence}$$

$$a \in \mathcal{I}(C) \text{ or } b \in \mathcal{I}(C).$$

Corollary 2: The irreducible closed subsets of $X = \operatorname{Spec} R$ are just the closures of points of X, i.e., there is one corresponding to each prime ideal of R.

In particular, the whole space X is irreducible iff. rad (0) is a prime ideal, i.e., iff. R/N (N = nilradical) is an integral domain.

(3) Note that a point x is closed, i.e., its own closure, iff. p_x contains no other prime ideal, i.e., iff. p_x is a maximal ideal.

G. Examples.

(1). The spectrum of the zero ring is empty, and no other ring has an empty spectrum, since it will contain a maximal ideal.

(2) A primary ring R is one with only one prime ideal p. Then $p = \text{rad }(0)$ (D.2), hence every element of p is nilpotent. Spec R consists of one point. Any field is an example of such a ring, as is $k[x]/(x^2)$, k a field.

(3) A ring R with dcc is a product $R \approx R_1 \times \dots \times R_n$ of primary rings. Thus (cf. E.1) Spec R is the discrete space of n points.

(4) Consider the ring $k[[t]]$ of formal power series with coefficients in a field k. It is an integral domain, hence (0) is a prime ideal. Now any power series

$$a_n t^n + a_{n+1} t^{n+1} + \dots \qquad (a_n \neq 0)$$

with a_n as its first non-zero coefficient is a product of t^n with a unit

$$a_n + a_{n+1} t + \dots$$

(why is this a unit?). Thus an ideal I which is not zero contains some power of t, and so the only non-zero ideals are the ideals (t), (t^2), ... , and (t) is the only prime ideal other than (0). Hence Spec $k[[t]]$ contains the two points x corresponding to (0) and x_o corresponding to (t). $x_o = V(t)$, and hence is closed, while the closure of x is the whole spectrum.

(5) The polynomial ring $k[t]$ has a prime ideal corresponding to each prime monic polynomial of positive degree. The zero ideal is the only other prime ideal (why?). Each prime poly. $p(t)$ corresponds to a closed point $= v(p(t))$ of Spec $k[t]$, and the closure of the point corresponding to (0) is the whole spectrum.

Note that if k is algebraically closed, the prime monic polynomials are just the linear polynomials i.e., ones of the form $t - a$ for some $a \in k$. Thus Spec $k[t]$ contains a closed point for every "number" $a \in k$. The value of a polynomial $f(t)$ at this point (cf. B.) is canonically identified with $f(a)$ (how?).

If k is not algebraically closed, there is still a closed point for every element of k, but there are also some others.

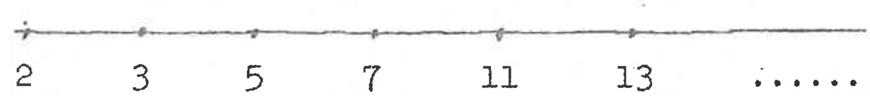
It is customary to draw Spec $k[t]$ as a line.

(6) The polynomial ring $k[x,y]$ contains, besides (0), the prime ideals generated by monic prime polynomials. There is also a prime ideal corresponding to each pair (a,b) of elements of k. This is the kernel of the map $k[x,y] \to k$ given by $f(x,y) \rightsquigarrow f(a,b)$, and such a point is closed (why?). If k is algebraically closed, these are the only prime ideals. (We will see later why this is so.) Otherwise, there are some more.

Spec $k[x,y]$ should be drawn as a plane. The point corresponding to the pair (a,b) should be drawn as usual. If $p(x,y)$ is a prime polynomial, the variety $V(p(x,y))$ will contain the point corresponding to the ideal $(p(x,y))$

and also some closed points. The point (a,b) is in $V(p(x,y))$ iff. $p(a,b) = 0$ (why?). $V(p(x,y))$ should be drawn as a curve, to represent the "zeros of $p(x,y)$".

(7) Spec $\mathbb{Z}$ has a point corresponding to each prime number, and one corresponding to the zero ideal. The ones corresponding to the primes are the closed points. This is a "picture" of Spec $\mathbb{Z}$:



The picture is supposed merely to convey the information the Spec $\mathbb{Z}$ has closed points corresponding to $2,3,...$ on it. It is drawn as a line to indicate that it has dimension 1 in a sense that will be made precise later. The point corresponding to (0) is not drawn. I think of it as being nearly anywhere, since its closure is all of Spec $\mathbb{Z}$. It is a "general point".

LOCALIZATION

A. Rings of Fractions.

Let R be a ring and S a subset of R. We want to discuss the possibility of introducing formally in R the multiplicative inverses of elements of S. The problem can be stated as follows:

(1) Find a ring $S^{-1}R$ and a homomorphism $f: R \to S^{-1}R$ such that the image $f(s)$ of every element $s \in S$ has an inverse in $S^{-1}R$, and such that any map

$$g : R \to R'$$

with $g(s)$ invertible for each $s \in S$ factors uniquely through $S^{-1}R$.

The last phrase means that there is a unique homomorphism $\bar{g} : S^{-1}R \to R'$ such that $g = \bar{g}f$. As always, such a universal property characterizes the pair $(S^{-1}R, f)$ up to unique isomorphism, because there are unique maps both ways between two pairs having the property. Moreover, it is clear that this problem has the following solution:

Let $U = \{u_s \mid s \in S\}$ be a set of "variables" indexed by the set S, and put $S^{-1}R = R[U]/I$ where $R[U]$ is the polynomial ring in the variables $\{u_s\}$ and I is the ideal generated by the set of polynomials

$$(2) \qquad s\, u_s - 1 \qquad s \in S .$$

We leave the trivial verification to the reader.

Note that if a set S of elements has inverses, so does any product of the elements of S. One sees immediately from the universal property that therefore $S^{-1}R$ depends (up to unique isomorphism) only on the multiplicative sub-semigroup S' of R consisting of 1 and of all finite products of elements of S. A subset like S' which is closed under finite products and contains 1 is called a <u>multiplicative system</u>.

Actually, the construction depends on even less than the multiplicative system S' generated by S. For instance, if S is a finite set $S = \{s_1, \ldots, s_n\}$, then adjoining inverses of all the elements of S amounts to the same thing as adjoining the inverse of the one element $s = s_1 \ldots s_n$, the product of the s_i (why?). The case that S consists of one element s is particularly agreeable. We obtain $S^{-1}R$ just by adjoining a variable u with the relation $su = 1$.

Let us denote by $\bar{a}$ the image under f of an element of R. Then the usual calculations of sums and products of fractions show that the set of elements x of $S^{-1}R$ which can be written in the form

$$(3) \qquad x = \bar{s}^{-1}\,\bar{a} \qquad a \in R\ ,\ s \in S' = \text{products from } S$$

form a subring of $S^{-1}R$. We think of $\bar{s}^{-1}\bar{a}$ as the "fraction" $\bar{a}/\bar{s}$. Since f has its image in this subring, and since every element $s \in S$ has an invertible image there, the universal property shows that this subring is all of $S^{-1}R$. Thus <u>every element of</u> $S^{-1}R$ <u>can be written</u> (not uniquely) <u>in the form</u> (3) . For this reason, the ring $S^{-1}R$ is called the <u>ring of fractions</u> of R with respect to S .

The map f is <u>not</u> injective in general. For instance, if we were silly enough to include 0 in S , we would get in the above notation,

$$-1 = 0\, u_0 - 1 \in I ,$$

hence $I = R[U]$, hence $S^{-1}R$ = the zero ring.

In general, the result is the following:

<u>Proposition 4</u>: The kernel of $f : R \to S^{-1}R$ is the set of elements $a \in R$ such that $as = 0$ for some $s \in S'$ (i.e. for some finite products of elements of S).

proof: If $as = 0$, then $f(a) = \bar{a} = (\overline{as})\bar{s}^{-1} = 0\bar{s}^{-1} = 0$. Conversely, suppose $\bar{a} = 0$. Then with the above notation, the constant polynomial a is in I , i.e., is a linear combination of the polynomials (2) . Now only a finite number of the u_s appear in this linear combination. Therefore the image of a is already zero in $S_o^{-1} R$ for some finite subset S_o of S . Hence we may assume $S = \{s_1, \ldots, s_n\}$ is finite. Hence we may assume S consists only of the element $s = s_1 \ldots s_n$. Then the fact that a is in I reads (cf. 2)

$$a = (su - 1)\, p(U)$$

for some polynomial $p(u) \in R[u]$. Write

$$p(u) = b_o + b_1 u + b_2 u^2 + \dots + b_n u^n .$$

Then

$$a = -b_o \ , \ sb_o = b_1 \ , \ \dots \ , \ sb_{n-1} = b_n \ , \ sb_n = 0 .$$

Therefore $s^{n+1} a = 0$, which completes the proof.

Corollary 5: If S contains no zero divisors, for instance if R is an integral domain, and $0 \notin S$, then $f : R \to S^{-1}R$ is injective.

In this case, $S^{-1}R$ is a subring of the field of fractions of R , which is obtained by adjoining inverses of all the non-zero elements of R . In particular, $S^{-1}R$ is an integral domain. We leave the verification of this fact to the reader.

B. The spectrum of the ring of fractions.

Let R be a ring and S a subset of R . The map $f : R \to S^{-1}R$ yields a map $\operatorname{Spec} R \leftarrow \operatorname{Spec} S^{-1}R$.

Proposition 1:

The map $J \rightsquigarrow f^{-1}(J)$ from ideals of $S^{-1}R$ to ideals of R is injective.

proof: With any ideal I of R , we can associate the ideal $(f(I))$ of $S^{-1}R$ generated by the set $f(I)$ of images of the elements of I . This gives a map from ideals of R to ideals of $S^{-1}R$, and it suffices to show that the composition of the two maps is the identity, i.e., $(f(f^{-1}(J))) = J$. It is immediate that $(f(f^{-1}(J))) \subset J$. To show the other inclusion, let $x \in J$. It suffices to show that the product of x by some unit is in $(f(f^{-1}(J)))$. But by (A.3) , x differs by a unit factor from an image of an element of R , i.e. from an element of $(f(f^{-1}(J)))$, qed.

Proposition 2: The map $\operatorname{Spec} R \leftarrow \operatorname{Spec} S^{-1}R$ is an injection, and its image is the set of those $x \in X = \operatorname{Spec} R$ such that $p_x \cap S = \emptyset$.

proof: The map is an injection because of proposition 1 . Moreover, if J is an ideal of $S^{-1}R$, not the whole ring, then J contains no unit, and hence $f^{-1}(J) \cap S = \emptyset$. Thus a prime ideal in the image of $\operatorname{Spec} S^{-1}R$ can not meet S . It remains to prove that every p such that $p \cap S = \emptyset$ is in the image.

Let I be any ideal of R , and consider the following problem: Find a ring $\widetilde{R}$ and a map $g : R \to \widetilde{R}$ such that the kernel of g contains I , such that the image in $\widetilde{R}$ of every element of S is invertible, and such that $(\widetilde{R}, g)$ is the universal solution, in the usual sense. We can solve this in two ways: First adjoin inverses of elements of S , then divide out by the ideal necessary; or, first divide out by I , then adjoin the necessary inverses. The first construction gives $S^{-1}R \,/\, (f(I))$. For the second, let $\overline{R} = R/I$, and $\overline{S}$ = the residues of the elements of S in $\overline{R}$.

Then the second construction is just $\overline{S}^{-1}\overline{R}$. Thus the two rings $S^{-1}R/(f(I))$ and $\overline{S}^{-1}\overline{R}$ are naturally isomorphic.

Now let $I = p$ where p is a prime ideal not meeting S. Then $\overline{S}$ does not contain 0, hence the map $\overline{R} \to \overline{S}^{-1}\overline{R}$ is injective by (A.5), since $\overline{R}$ is an integral domain. Therefore the kernel of the composed map $R \to \overline{R} \to \overline{S}^{-1}\overline{R}$ is just p. Therefore the kernel of the composed map $R \to S^{-1}R \to S^{-1}R/(f(I))$ is also p, i.e., $p = f^{-1}(f(I))$. Since $f(I)$ is a prime ideal (because $\overline{S}^{-1}\overline{R}$ is an integral domain), this completes the proof.

Proposition 3: The topology on Spec $S^{-1}R$ is induced from that of Spec R, i.e., every closed set of Spec $S^{-1}R$ is the inverse image of a closed set of Spec R.

proof: If $x \in S^{-1}R$, then $V(x)$ does not change if x is multiplied by a unit factor. Thus by A.(2), $V(x) = V(\overline{a})$ for some $a \in R$, But $V(\overline{a}) = \{p' \mid \overline{a} \in p'\}$ $= \{p' \mid a \in f^{-1}(p')\}$, i.e., $V(\overline{a})$ is the inverse image in Spec $S^{-1}R$ of the locus $V(a)$ in Spec R. Since every closed set is an intersection of sets $V(x)$, and since inverse image commutes with intersection, this proves the proposition.

Notation 4: If S consists of the single element s, we will write $S^{-1}R = R_s$, and if Spec $R = X$, we will frequently use the notation Spec $R_s = X_s$.

Corollary 5: For $s \in S$, the spectrum X_s = Spec R_s is homeomorphic to the open subset $X - V(s)$ of X . These open sets form a base for the topology of X .

The first assertion is an immediate consequence of propositions 2 and 3 . In view of this, it is usual to identify X_s with the open subset $X - V(s)$ of X . The last assertion means that every open subset of X is a union of sets of the form $X_s = X - V(s)$. In fact, if U is an open set, say $U = X - V(S)$ for some closed set $V(S)$, then

$$V(S) = \bigcap_{s \in S} V(s) ,$$

hence

$$U = \bigcup_{s \in S} X_s .$$

This is an important point. Remember also that a finite intersection of open sets of the form X_s is again of that form, namely

(6) $$X_{s_1} \cap \ldots \cap X_{s_n} = X_s , \quad \text{where} \quad s = s_1 \ldots s_n .$$

Do the exercise of proving this.

C. Local Rings.

A local ring R is a ring with exactly one maximal ideal M . Let R be such a ring. If $a \in R$ is an element not in M , then (a) is not contained in a maximal ideal, hence $(a) = R$, i.e., a is a unit. Thus M consists of all non-units of R. Conversely, it is clear that any ring R in which the non-units form an ideal is a local ring. The spectrum X of R contains only one closed point, and this property again characterizes local rings (cf. 1.F.3).

Now let R be any ring and p a prime ideal of R. The set of elements $R - p$ of R not in p is stable under multiplication, since p is a prime ideal, hence forms a multiplicative system S. It is customary to denote by R_p the ring of fractions $S^{-1}R$. Since $p \cap S = \emptyset$, there is a prime ideal of R_p whose inverse image in R is p (B.2), call it M_p. It is the ideal generated by the image of p (cf. B.1).

By (A.3), every element $r \in R_p$ can be written as $r = \overline{s}^{-1}\overline{a}$ with $a \in R$, $s \in S$. Now either $a \in S$, in which case r is a unit, or $a \in p$, whence $\overline{a} \in M_p$, and so $r \in M_p$. Thus M_p is the set of non-units of R_p, which is therefore a local ring. It is called the <u>localization of</u> R <u>at</u> p. If $x \in X = \operatorname{Spec} R$ is the point corresponding to p, the ring R_p is also called the <u>local ring of</u> Spec R <u>at the point</u> x. It is obtained by adjoining inverses of all the elements $a \in R$ which are not zero at x (i.e., s.t. $a \notin p$ (cf. 1.B)).

The field R_p/M_p is canonically identified with the residue field $k(x)$ (1.B) of the point $x \in \operatorname{Spec} R$

corresponding to p . For, the two fields are just solutions in two ways of the problem of inverting S and killing p universally (cf. proof of B.2).

By (B.2), the spectrum of R_p is in one to one correspondence with the set of those prime ideals q of R which do not meet S , i.e., those prime ideals which are contained in p . This set of prime ideals is not in general an open subset of Spec R . It is obtained by leaving out from Spec R all closed subsets which do not contain the point x corresponding to p , i.e., it is the intersection of all open neighborhoods of x . For, if I is an ideal of R not contained in p , then no prime ideal containing I is in p , i.e., $V(I)$ contains no point of Spec R in the image of Spec R . Conversely, if a point y is not in the image, so that p_y is not contained in p , then all of $V(p_y)$ can be left out, as above.

Example 1: Consider the local ring of $X = \text{Spec } k[x,y]$ (cf. 1.G.6) at the origin $(0,0)$. It is just the ring of those rational functions in x , y which can be written as a fraction

$$f(x,y)/g(x,y)$$

of polynomials with $g(0,0) \neq 0$. The maximal ideal consists of those functions such that when they are written as above, one has $f(0,0) = 0$. The spectrum of this local ring corresponds in a one-one way with the set of prime ideals contained in the prime corresponding to the origin (it is generated by x and y). There is one point for each prime polynomial $p(x,y)$ such that $p(0,0) = 0$, besides the points corresponding to the zero ideal and to the maximal ideal. It is obtained from Spec $k[x,y]$ by leaving out all curves $\{f(x,y) = 0\}$ not passing through the origin.

On the other hand, let x be the "general point" of Spec $k[x,y]$, i.e., the point corresponding to the zero ideal. The local ring is obtained by inverting all non-zero elements of $k[x,y]$, i.e., is the field of rational functions in x and y. Its spectrum consists of one point, and is obtained from the "plane" Spec $k[x,y]$ by leaving out all of the curves.

D. Local determination of an element of R.

As was hinted in (1.B), we want to view elements of a ring R as something like functions on Spec $R = X$. While it is not easy to get an exact description of the elements as functions, they do have a property which is analogous to the following obvious property of functions (it says that a function is determined when you know it locally):

(1) a). Let X be a topological space, and $\{U_i\}$, $i \in I$ a family of open sets which cover X. If $f, f' : X \to Y$ are two continuous maps (Y another

topological space) such that the restrictions of f and f' to U_i are equal for each i, then $f = f'$.

b) Suppose $f_i : U_i \to Y$ $(i \in I)$ are continuous maps and suppose that the restrictions of f_i and f_j to $U_i \cap U_j$ are equal for each pair $i,j \in I$. Then there is a continuous map $f : X \to Y$ (unique by a).) whose restriction to U_i is f_i $(i \in I)$.

In order not to overload the notation, we will use the following terminology when dealing with several rings of fractions:

<u>Terminology 2</u>: Let R be a ring and $S \subset R$. We will say that two elements a, a' of R are <u>equal in</u> $S^{-1}R$ if their images under the canonical map $R \to S^{-1}R$ are equal. Similarly, if $a \in R$ and $a' \in S^{-1}R$, the assertion $a = a'$ <u>in</u> $S^{-1}R$ means that the image of a in $S^{-1}R$ is a'. This allows us to suppress the $^-$ in a lot of the previous notations. Thus (A.3) reads "Every element $x \in S^{-1}R$ is of the form

$$x = s^{-1}a \quad \text{in} \quad S^{-1}R$$

for some $a \in R$ and $s \in S'$." Also to be noted is (A.4), which now reads "An element $a \in R$ is <u>zero in</u> $S^{-1}R$ if and only if $sa = 0$ in R for some $s \in S'$."

We can now state the assertion for rings analogous tc (1)

Proposition 3: Let R be a ring and $S = \{s_i \mid i \in I\}$ a subset of R. Suppose that the ideal generated by S is the "unit ideal" R, i.e, that the open sets X_{s_i} cover $X = \operatorname{Spec} R$. Put $R_i = R_{s_i}$, $R_{ij} = R_{s_i s_j}$. There are canonical maps $R \to R_i$, and $R_i \to R_{ij}$, $R_j \to R_{ij}$.

a) If $a, a' \in R$ are elements such that $a = a'$ in R_i for each $i \in I$, then $a = a'$.

b) Let $a_i \in R_i$, $i \in I$ be elements and suppose that $a_i = a_j$ in R_{ij} for each pair $i, j \in I$ (i.e., that the images in R_{ij} under the canonical maps are equal). Then there is a (unique) element $a \in R$ such that $a = a_i$ in R_i.

proof: a) Let $b = a-a'$. The assertion is just that if b is zero in R_i for each i, then $b = 0$ in R. Now $b = 0$ in R_i iff. $s_i^{n_i} b = 0$ in R for some n_i (A.4). Since S generates the unit ideal, R, so does the set $s_i^{n_i}$. This is seen by raising an equation

$$1 = \sum r_i s_i$$

to a large power. Hence, we can write

$$1 = \sum c_i \, s_i^{n_i}$$

for some finite set $c_i \in R$, whence

$$b = \sum c_i \, s_i^{n_i} b = c_i \, 0 = 0 .$$

b) First of all, we may assume that S is a finite set. For, since S generates the unit ideal $R = (1)$, so does a finite subset $S_o = \{s_1, \ldots, s_m\}$. If the result is proved when S is finite, then we can restrict the data given to the finite subset S_o and use it to construct an element a of R. Then for $\alpha \in I$ arbitrary, $a_\alpha = a_i$ in $R_{i\alpha}$ for $i = 1,\ldots,m$. Since $a = a_i$ in R_i, hence $a = a_i$ in $R_{i\alpha}$ for $i = 1,\ldots,m$, we have $a = a_\alpha$ in $R_{i\alpha}$. Now $R_{i\alpha}$ is the ring obtained from R_α by inverting the element s_i, and $s_1,\ldots,s_m$ generate the unit ideal in R, therefore in R_α. Hence by part a), it follows that $a = a_\alpha$ in R_α. So the solution for the subset S_o is also a solution for all of S. Thus we may assume that $S = S_o$ is a finite set.

Write

$$a_i = s_i^{-n} b_i \quad \text{in } R_i$$

for some $b_i \in R$ and some integer n. Since S is assumed finite, one n will work for all i. Now by assumption

$$s_i^{-n} b_i = a_i = a_j = s_j^{-n} b_j \qquad \text{in } R_{ij},$$

hence

$$s_j^n b_i = s_i^n b_j \quad \text{in } R_{ij}.$$

By (A.4),

$$(s_i s_j)^N (s_j^n b_i - s_i^n b_j) = 0 \quad \underline{\text{in } R}$$

for some large N. Replacing b_i by $s_i^N b_i$ and n by $n+N$ in the above formulas, we are reduced to the case that actually

$$s_j^n b_i = s_i^n b_j \qquad \text{in } R$$

for all i and j.

Now $\{s_1, \ldots, s_m\}$ generates the unit ideal, hence so does $\{s_1^n, \ldots, s_m^n\}$. So we can write

$$1 = \sum r_i s_i^n$$

for some $r_i \in R$. Put

$$a = \sum_i r_i b_i .$$

Then

$$s_j^n a = \sum_i r_i s_j^n b_i = \sum_i r_i s_i^n b_j = b_j \quad \text{in } R ,$$

hence

$$a = s_j^{-n} b_j = a_j \qquad \text{in } R_j ,$$

i.e., a is the required element. This completes the proof.

E. The structure sheaf.

Definition 1: Let X be a topological space. A presheaf of sets F on X consists of

(i) A set $F(U)$ for each open $U \subset X$.

(ii) For each pair $V \subset U$ of open sets a map $F(U) \to F(V)$ called the restriction map from V to U.

The sets and maps are required to satisfy the following axiom of transitivity of restriction:

If $W \subset V \subset U$ then the diagram of restriction maps

$$\begin{tikzcd} F(U) \arrow[rr, dashed] \arrow[dr] & & F(V) \arrow[dl] \\ & F(W) & \end{tikzcd}$$

commutes.

Moreover, the map $F(U) \to F(U)$ associated to the identity map on U is the identity.

The elements of $F(U)$ are called the sections of F on U. We will use the following terminology: Suppose V, U_1, U_2 are open sets with $V \subset U_i$. If $a_i \in F(U_i)$ $(i=1;2)$, we will say

$$a_1 = a_2 \text{ on } V$$

if the images in $F(V)$ of the elements a_i under the restriction maps $F(U_i) \to F(V)$ are equal.

Definition 2: A presheaf F is called a sheaf if the following sheaf axiom holds:

Suppose $\{V_i\}$ are open subsets of an open set $U \subset X$ which cover U.

a) If $a, a' \in F(U)$ satisfy $a = a'$ on V_i for all i, then $a = a'$ on U.

b) If $a_i \in F(V_i)$ are elements such that $a_i = a_j$ on $V_i \cap V_j$ for all i,j, then there is an $a \in F(U)$ with $a = a_i$ on V_i for each i.

A (pre)<u>sheaf of groups</u> (rings) is a (pre)sheaf in which each $F(U)$ is given with a group (ring) law such that the restriction maps are homomorphisms.

<u>Example 3</u>: Let X, Y be topological spaces. For U open in X, let $F(U)$ be the set of continuous maps $U \to Y$. If $V \subset U$ let $F(U) \to F(V)$ be obtained by restricting the domain of a function from U to V. Then F is a sheaf. The sheaf axiom is just assertion (D.1).

Now let R be a ring and $X = \operatorname{Spec} R$. Suppose $s,t \in R$ are elements such that $X_s \supset X_t$ (B.4), i.e., $V(s) \subset V(t)$. Then s is nowhere zero on $\operatorname{Spec} R_t = X_t$, i.e., the image of s in R_t is in no prime ideal, i.e., s <u>is a unit in</u> R_t. Therefore (A.1) there is a <u>unique</u> map $R_s \to R_t$ making the triangle

$$\begin{tikzcd} R \arrow[r] \arrow[dr] & R_s \arrow[d] \\ & R_t \end{tikzcd}$$

commute. In particular, if $X_s = X_t$, then R_s and R_t are canonically isomorphic, so that the ring is determined up to canonical isomorphism by the open set.

Clearly, this means that we get a presheaf of rings $\tilde{R}$ on X by setting $\tilde{R}(X_s) = R_s$, and letting the restriction map be the canonical one above when $X_s \supset X_t$ (the reader should verify the transitivity of restriction if $X_s \supset X_t \supset X_u$). Moreover, (D.3) just asserts that $\tilde{R}$ is actually a sheaf. It is worded so as to give the sheaf axiom (2) in the case $U = X$, but this is only a question of terminology.

There is however one trouble, namely that not every open subset U of X is of the form X_s. Hence the sections of $\tilde{R}$ on U have not been defined for all U. But this is not a serious problem. Since every U is a union of sets of the form X_s (B.5), we can define $\tilde{R}(U)$ in the only way which will give a sheaf, namely as follows:

Choose a covering $\{X_{s_i}\}$ of U by such opens, and let $\tilde{R}(U)$ contain one element for each collection of elements

$$a_i \in R_{s_i}$$

such that

$$a_i = a_j \quad \text{in} \quad R_{s_i s_j} \quad \text{for each} \quad i,j\ .$$

It is now necessary to verify that this is independent of the chosen covering $\{X_{s_i}\}$ and that it gives a sheaf of rings in a natural way. This is not an interesting point, so we omit the proof.

Definition 4. The sheaf of rings $\tilde{R}$ on $X = \operatorname{Spec} R$ defined above is called the structure sheaf of $\operatorname{Spec} R$.

LOCALIZATION OF MODULES

A. Module of fractions.

Let R be a ring, $S \subset R$, and M an R-module. If we want to get an $S^{-1}R$-module in a functorial way from M, the obvious choice is to take the tensor product $S^{-1}R \otimes_R M$ (we will use the notation $S^{-1}M = S^{-1}R \otimes_R M$), where $S^{-1}R$ is viewed as an R-algebra via $f: R \longrightarrow S^{-1}R$ (2.A.1). We want to describe the module explicitly: Any element $m \in S^{-1}M$ will be of the form

$$z = \sum x_i \otimes m_i \qquad \text{for some } x_i \in S^{-1}R, \quad m_i \in M.$$

Write (2.A.3) $x_i = s_i^{-1} a_i$ in $S^{-1}R$ ($a_i \in R$, $s_i \in S' =$ products from S). Changing a_i if necessary, we may assume that the s_i are all equal, say to s. Let $\bar{}$ denote the image in $S^{-1}R$. We have $x_i \otimes m_i = \bar{s}^{-1} \bar{a}_i \otimes m_i = \bar{s}^{-1} \otimes a_i m_i$. Put $m = \sum a_i m_i$. Then

$$(1) \qquad z = \bar{s}^{-1} \otimes m = \bar{s}^{-1}(1 \otimes m).$$

Suppose we adopt the following terminology: There is a natural R-homomorphism $M \longrightarrow S^{-1}M$, namely it sends $m \rightsquigarrow 1 \otimes m$. We will extend (2.D.2) by saying, given $m \in M$, $m' \in S^{-1}M$, then

$$(2) \qquad m = m' \quad \text{in } S^{-1}M$$

if $1 \otimes m = m'$, and we will use the same symbol m for the image $1 \otimes m$ in $S^{-1}M$. Then (1) just reads

(3) Every $z \in S^{-1}M$ can be written in the form

$$z = s^{-1} m \quad \text{in } S^{-1}M$$

for some $s \in S'$ and some $m \in M$.

For this reason, $S^{-1}M$ is called the <u>module of fractions</u>.

<u>Proposition 4</u>: The kernel of the map $M \longrightarrow S^{-1}M$ is the set of $m \in M$ such that $sm = 0$ for some $s \in S'$.

proof: The proof is analogous to that of (2.A.4). It is easy to see that S may be assumed finite, hence that $S = \{s\}$ consists of one element. Then we have maps

$$R \xrightarrow{a} R[u] \xrightarrow{b} R[u]/I = S^{-1}R$$

where $I = (su-1)$. Thus $S^{-1}M$ is obtained by extension of scalars by a and then by b, i.e., (cf. T.P.,D)

$$S^{-1}M = R[u] \otimes_R M \;/\; I(R[u] \otimes_R M) .$$

Now an element of $R[u] \otimes_R M$ can be written uniquely in the form

$$\sum u^i \otimes m_i \qquad m_i \in M$$

(this is easy to see). Hence if $m \in I(R[u] \otimes_R M)$, we have

$$1 \otimes m = (su - 1) \sum u^i \otimes m_i \text{ , i.e.,}$$

$$1 \otimes m = -1 \otimes m \text{ ;}$$

$$su(u^{i-1} \otimes m_{i-1}) = u^i \otimes sm_{i-1} = u^i \otimes m_i \quad \text{for } i = 1,\ldots,n$$

$$su(u^n \otimes m_n) = u^{n+1} \otimes sm_n = 0 .$$

Thus $$u^{n+1} \otimes s^{n+1}m = 0 ,$$

whence $s^{n+1}m = 0$. This completes the proof.

From the proposition we can deduce the following rule:

(5) $$s_1^{-1} m_1 = s_2^{-1} m_2 \quad \text{in } S^{-1}M$$

iff. there is an $s \in S'$ such that

$$s(s_2m_1 - s_1m_2) = 0 \quad \text{in } M .$$

We leave it as an exercise. This means that we could have <u>defined</u> $S^{-1}M$ as the set of equivalences of "fractions" $s^{-1}m$ for the equivalence relation (5).

B. <u>The sheaf associated to a module.</u>

If $S = \{s\}$, we will use the notation M_s for $S^{-1}M$ (cf.(2.B.4)). The assertion analogous to (2.D.3) is

<u>Proposition 1</u>: Let R be a ring and $S = \{s_i | i \in I\}$ a subset of R . Suppose that the ideal generated by S is the unit ideal R , i.e., that the open sets X_{s_i} cover $X = \operatorname{Spec} R$. Put $M_i = M_{s_i}$, $M_{ij} = M_{s_i s_j}$. There are canonical maps $M \longrightarrow M_i$, $M_i \longrightarrow M_{ij}$, $M_j \longrightarrow M_{ij}$.

(a) If $m, m' \in M$ are elements such that $m = m'$ in M_i for each i , then $m = m'$ in M .

(b) Let $m_i \in M_i$ $(i \in I)$ be elements and suppose that $m_i = m_j$ in M_{ij} for each pair $i,j \in I$. Then there is a (unique) element $m \in M$ such that $m = m_i$ in R_i for each i .

Since the proof is the same as that of (2.D.3), we omit it.

As in (2.E), we can define a <u>sheaf</u> $\tilde{M}$ in Spec $R = X$ associated to M by setting $\tilde{M}(X_s) = M_s$. This definition is extended to arbitrary opens U as follows: Choose a covering $\{X_{s_i}\}$ of U by opens of the form X_s , and let $\tilde{M}(U)$ contain one element for every collection of elements $a_i \in M_{s_i}$ such that $a_i = a_j$ in $M_{s_i s_j}$ for each i, j . It follows from Proposition 1 that this gives a sheaf $\tilde{M}$ on X . We omit the proof.

Note that $\tilde{M}(U)$ has in an obvious way the structure of a module over the ring $\tilde{R}(U)$. This means that $\tilde{M}$ is a sheaf of $\tilde{R}$ -modules in the following sense:

<u>DEFINITION 2</u>: Let X be a topological space and $\mathcal{R}$ a sheaf of rings on X . A sheaf of $\mathcal{R}$ -modules $\mathcal{M}$ is a sheaf of abelian groups together with a law of composition

$$\mathcal{R}(U) \times \mathcal{M}(U) \longrightarrow \mathcal{R}(U)$$

for each open U of X making $\mathcal{M}(U)$ into an $\mathcal{R}(U)$-module, such that if $V \subset U$ the diagram

$$\begin{tikzcd} \mathcal{R}(U) \times \mathcal{M}(U) \arrow[r] \arrow[d] & \mathcal{M}(U) \arrow[d] \\ \mathcal{R}(V) \times \mathcal{M}(V) \arrow[r] & \mathcal{M}(V) \end{tikzcd}$$

commutes, where the vertical arrows are induced by the restriction maps.

<u>Definition 3</u>: A <u>map</u> $f: F \longrightarrow G$ of sheaves of sets on a space X consists of a map

$$f(U): F(U) \longrightarrow G(U)$$

for each open $U \subset X$ compatible with the restriction maps, i.e., such that for $V \subset U$ the diagram

$$\begin{array}{ccc} F(U) & \xrightarrow{f(U)} & G(U) \\ \downarrow & & \downarrow \\ F(V) & \xrightarrow{f(V)} & G(V) \end{array}$$

commutes, where the vertical arrows are the restrictions. If F, G are sheaves of groups (modules over a given sheaf of rings), then f is called a <u>homomorphism</u> if in addition each $f(U)$ is a homomorphism of the structure in question. The set of such homomorphisms is denoted by $\mathrm{Hom}(F,G)$.

<u>Proposition 4</u>: Let M, N be R -modules. There is a natural 1-1 correspondence between R -homomorphisms $f: M \longrightarrow N$ and $\tilde{R}$ -homomorphisms $\phi: \tilde{M} \longrightarrow \tilde{N}$, i.e.,

$$\mathrm{Hom}_R(M,N) \approx \mathrm{Hom}_{\tilde{R}}(\tilde{M},\tilde{N}) .$$

proof: A homomorphism $\phi: \tilde{M} \longrightarrow \tilde{N}$ includes an R-homomorphism $\phi(X): M \longrightarrow N$ since $M = \tilde{M}(X)$ etc. Conversely, since localization of modules is a functor, an R-homomorphism $f: M \longrightarrow N$ induces an R_s -homomorphism $f_s: M_s \longrightarrow N_s$

for each $s \in R$. Clearly the compatibility conditions are satisfied so that one obtains a homomorphism $\tilde{f}: \tilde{M} \longrightarrow \tilde{N}$ pf $\tilde{R}$-modules in this way. It is naturally given on opens X_s, and extends in an obvious way to arbitrary opens. I claim these two correspondences are inverses of each other:

Trivially, the module homomorphism $M \longrightarrow N$ associated to $\tilde{f}$ is again f. What has to be shown is that if $\phi: \tilde{M} \longrightarrow \tilde{N}$ is any $\tilde{R}$-homomorphism, and $f = \phi(X): M \longrightarrow N$, then $\phi = \tilde{f}$, i.e., for every $s \in R$, the two maps $\phi(X_s)$, f_s from M_s to N_s are equal. But the diagrams

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow & & \downarrow \\ M_s & \xrightarrow{\phi(X_s)} & N_s \end{array} \qquad \begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow & & \downarrow \\ M_s & \xrightarrow{f_s} & N_s \end{array}$$

both commute. Hence $\phi(X_s)$ and f_s are equal on the elements of M_s which are images of elements of M. Since these images generate M_s as R_s-module, it follows that $\phi(X_s) = f_s$. This completes the proof.

Definition 5: Let R be a ring and $X = \operatorname{Spec} R$. A sheaf of $\tilde{R}$-modules $\mathcal{M}$ is called quasi-coherent iff. $\mathcal{M}$ is isomorphic to $\tilde{M}$ for some R-module M.

Of course, an isomorphism $\mathcal{M} \xrightarrow{\sim} \tilde{M}$ is an isomorphism $\mathcal{M}(U) \xrightarrow{\sim} \tilde{M}(U)$ for each open $U \subset X$ compatible with the restriction maps (cf. Defn. 3).

An important fact is that the property of being quasi-coherent is determined "locally" on X :

Theorem 6: Let R be a ring, $X = \operatorname{Spec} R$, and $\mathcal{M}$ a sheaf of $\tilde{R}$-modules. Then $\mathcal{M}$ is quasi-coherent iff. there is a set $S = \{s_i \mid i \in I\} \subset R$ which generates the unit ideal, such that the restriction $\mathcal{M}|X_{s_i}$ of $\mathcal{M}$ to X_{s_i} is quasi-coherent for each i.

By restriction $F|U$ of a sheaf F to an open subset U of X, we just mean the obvious sheaf on U, namely if $V \subset U$ is open, then V is open in X, and we take $F(V)$ as sections of $F|U$ on V.

It is clear that if the sheaf $\mathcal{M}$ is quasi-coherent, so is $\mathcal{M}|X_{s_i}$ for each i. In fact, if $\mathcal{M} = \tilde{M}$, then $\mathcal{M}|X_{s_i} = \tilde{M}_{s_i}$ = the sheaf associated to the R_{s_i}-module M_{s_i}. We need to prove the converse.

To begin with, the natural candidate for a module M such that $\tilde{M} \approx \mathcal{M}$ is the R-module $\mathcal{M}(X)$. Denote it by M. For any $t \in R$, the restriction map is a map $M = \mathcal{M}(X) \longrightarrow \mathcal{M}(X_t)$, and it is immediately seen to be a map of R-modules (where the R_t-module $\mathcal{M}(X_t)$ is viewed as an R-module by restriction of scalars). Therefore (T.P.,D.1) there is a unique R_t-homomorphism $M_t \longrightarrow \mathcal{M}(X_t)$ such that the diagram of maps

$$\begin{array}{ccc} M & \longrightarrow & M_t \\ \| & & \downarrow \\ \mathcal{M}(X) & \longrightarrow & \mathcal{M}(X_t) \end{array}$$

commutes. Thus it is clear that $\mathcal{M}$ is quasi-coherent iff. the map $M_t \longrightarrow \mathcal{M}(X_t)$ is an isomorphism for each $t \in R$.

Now suppose that $\mathcal{M}|X_{s_i}$ is quasi-coherent for each i, i.e., that $\mathcal{M}|X_{s_i} = \tilde{M}_i$ where M_i is the R_{s_i}-module $\mathcal{M}(X_{s_i})$. We may suppose $S = \{s_1, \ldots, s_n\}$ finite (1.C.9). We want to show that the map

$$M_t \longrightarrow \mathcal{M}(X_t)$$

is bijective for any $t \in R$.

<u>injectivity</u>: Say $t^{-r} m$ is mapped to zero in $\mathcal{M}(X_t)$. This is equivalent with saying that $m = 0$ in $\mathcal{M}(X_t)$, where $m \in M = \mathcal{M}(X)$. Then

$$m = 0 \quad \text{in } \mathcal{M}(X_{s_i t}) \quad \text{for each } i .$$

Since $X_{s_i t} \subset X_{s_i}$, and $\mathcal{M}|X_{s_i} = \tilde{M}_i$, we have $\mathcal{M}(X_{s_i t}) = (M_i)_t$. Hence (A.4) there is an n such that

$$t^n m = 0 \quad \text{in } M_i .$$

One n will do for all i. Since the X_{s_i} cover X, the sheaf axiom for $\mathcal{M}$ implies

$$t^n m = 0 \quad \text{in } \mathcal{M}(X) = M .$$

Hence (A.4)

$$m = 0 \quad \text{in } M_t ,$$

so

$$t^{-r} m = 0 \quad \text{in } M_t \text{, too.}$$

<u>surjectivity</u>: Let $z \in \mathcal{M}(X_t)$. Consider the image of z in $\mathcal{M}(X_{s_i t}) = (M_i)_t$. We may write it as a "fraction"

$$z = t^{-n} a_i \qquad \text{in} \quad (M_i)_t$$

for some a_i in M_i and for some n (one will work for each i). Then

$$t^n z = a_i = a_j \qquad \text{in} \ \mathcal{M}(X_{s_i s_j t}) ,$$

and

$$\mathcal{M}(X_{s_i s_j t}) = (M_{ij})_t$$

where

$$M_{ij} = (M_i)_{s_j} = (M_j)_{s_i} = \mathcal{M}(X_{s_i s_j}) .$$

Hence

$$t^m a_i = t^m a_j \qquad \text{in} \quad M_{ij}$$

for some m . Replacing a_i by $t^m a_i$, we are reduced to the case that

$$a_i = a_j \qquad \text{in} \quad M_{ij} = \mathcal{M}(X_{s_i s_j}) .$$

Hence the sheaf axiom implies that there exists $a \in M$ such that $a = a_i$ in $\mathcal{M}(X_{s_i}) = M_i$ for each i . Then

$$t^{-n} a = t^{-n} a_i = z \qquad \text{in} \ \mathcal{M}(X_{s_i t})$$

for each i , hence

$$t^{-n} a = z \qquad \text{in} \ \mathcal{M}(X_t) .$$

Since $t^{-n} a \in M_t$, this completes the proof.

C. Gluing of Sheaves.

In defining the structure sheaf $\tilde{R}$ (2,E) and the sheaf $\tilde{M}$ associated to a module M (B), we had to extend the definition which was given naturally for opens of the form X_s to arbitrary opens. The precise assertion justifying this procedure is the following:

Proposition 1: Let X be a topological space and $\mathcal{B}$ a collection of open sets of X which form a base for the topology, and which is closed under finite intersections. Suppose given a set $F(U)$ for each $U \in \mathcal{B}$ and a restriction map $F(U) \longrightarrow F(V)$ for $V \subset U$ in $\mathcal{B}$, satisfying the transitivity of restriction (2.E.1) wherever applicable. Suppose finally that the sheaf axiom (2.E.2) holds when U, $\{V_i\}$ are in $\mathcal{B}$. Then there is a sheaf F on X, unique up to unique isomorphism, whose set of sections on a $U \in \mathcal{B}$ is $F(U)$ and whose restriction maps are the given ones when $V \subset U$ are in $\mathcal{B}$. F will have the structure of a sheaf of groups (or modules over a given sheaf of rings) if the restriction to $\mathcal{B}$ does, in the obvious sense.

The sheaf F is constructed as follows: For U open in X, choose a covering of U by opens $\{V_i\}$ in $\mathcal{B}$, which is possible since $\mathcal{B}$ is a base for the topology, and let $F(U)$ contain one element for each collection of elements $\{a_i \in F(V_i)\}$ which satisfies $a_i = a_j$ in $F(V_i \cap V_j)$ for each i,j (note that $V_i \cap V_j$ is in $\mathcal{B}$).

The reader should now be ready to verify that this depends up to canonical isomorphism only on U, and that one gets a sheaf in this way, thus proving the proposition.

It follows from the proposition that a sheaf can be reconstructed if its restriction to U_i is known for a set $\{U_i\}$ of opens covering X. For, we need only to know its sections on a base closed under intersections, and the set of open sets V which are contained in at least one of the U_i form such a set. Therefore we can also construct a sheaf on X when sheaves F_i are given on U_i, provided we have a method of identifying compatibly the restrictions $F_i|U_{ij}$ and $F_j|U_{ij}$ $(U_{ij} = U_i \cap U_j)$, i.e., an isomorphism $\theta_{ij}\colon F_i|U_{ij} \xrightarrow{\sim} F_j|U_{ij}$. Thus

<u>Proposition 2</u>: Let $\{U_i\}$ be an open cover of X, and call $U_{ij} = U_i \cap U_j$, $U_{ijk} = U_i \cap U_j \cap U_k$. Let F_i be a sheaf of sets (groups, modules) on U_i and let <u>gluing data</u> as follows be given: An isomorphism

(3) $$\theta_{ij}\colon F_i \xrightarrow{\sim} F_j \quad \text{on} \quad U_{ij}$$

between the restrictions of F_i, F_j to U_{ij} for each i,j such that for each triple i,j,k the restrictions of the isomorphisms to U_{ijk} satisfy the <u>compatibility</u>

condition

(4) $$\theta_{ij}\,\theta_{jk} = \theta_{ik} \quad \text{on} \quad U_{ijk} .$$

Then there is a sheaf of sets (groups, modules) F and an isomorphism

(5) $$\phi_i : F \xrightarrow{\sim} F_i \quad \text{on} \quad U_i$$

of its restriction to U_i such that

(6) $$\theta_{ij}\,\phi_i = \phi_j \quad \text{on} \quad U_{ij}$$

for each i,j . The collection $\{F, \phi_i\}$ is determined up to unique isomorphism by the gluing data.

In fact, condition (4) is just designed so that we can identify F_i with F_j on U_{ij} via the isomorphism θ_{ij} without contradictory identifications on the triple intersections.

Corollary 6: In the above proposition, let $X = \operatorname{Spec} R$. If $U_i = X_{s_i}$ for some s_i , and if each F_i is a quasi-coherent sheaf of $\tilde{R}_{s_i}$-modules on X_{s_i}, then F is a quasi-coherent sheaf of $\tilde{R}$ -modules on X .

This follows from (B.6).

D. Locally free modules.

Definition 1: Let R be a ring and M an R-module. M is called locally free of rank n if there is a set S of elements of R which generates the unit ideal, such that M_s is a free R_s-module of rank n for each $s \in S$.

This notion is analogous to that of vector bundle in topology. We want to use the results of the previous sections to classify locally free modules.

Fix a set $S = \{s_1, \ldots, s_n\}$ which generates the unit ideal R, and let M be an R-module such that $M_i = M_{s_i}$ is free of rank n over $R_i = R_{s_i}$ for each i. Denote by F_i the free module over R_i with basis $\{v_1, \ldots, v_n\}$. We use the same symbols $\{v_\nu\}$ for each i.

The assertion that M_i is free of rank n is just that there is an isomorphism of R_i-modules, corresponding to the choice of a basis in M_i,

$$f_i \colon F_i \xrightarrow{\sim} M_i .$$

Denote as usual by $\tilde{}$ the sheaf associated to a module. Since $\tilde{M}_i | X_{s_i s_j} = \tilde{M}_j | X_{s_i s_j}$, the isomorphisms f_i give isomorphisms

$$\tilde{\theta}_{ij} = f_j^{-1} f_i \colon \tilde{F}_i \xrightarrow{\sim} \tilde{F}_j \qquad \underline{\text{on } X_{s_i s_j}} .$$

The $\tilde{\Theta}_{ij}$ satisfy the compatibility condition (C.4) so as to be gluing data for a sheaf, and it is immediately seen that the sheaf obtained by the gluing is canonically isomorphic to the sheaf $\tilde{M}$ associated to the module M.

Now $\tilde{F}_i$ and $\tilde{F}_j$ restricted to U_{ij} are both just the sheaf associated to the free R_{ij}-module F_{ij} with basis $\{v_1, \ldots, v_n\}$. Hence $\tilde{\Theta}_{ij}$ comes from an <u>automorphism</u> Θ_{ij} of F_{ij} (B.4). An endomorphism of a free module is given by an $n \times n$-matrix $(a_{\nu\mu})$, and it is an automorphism iff. the matrix is invertible, i.e., iff. $\det(a_{\nu\mu})$ is a unit in R.

<u>Definition 2</u>: We denote by $Gl_n(R)$ the group of invertible $n \times n$-matrices with entries taken from R, and by Gl_n the <u>sheaf</u> of groups on $X = \operatorname{Spec} R$ whose group of sections $Gl_n(U)$ on an open set $U \subset X$ is the group of invertible $n \times n$-matrices with entries in $\tilde{R}(U)$.

It is immediately seen that Gl_n is a sheaf since $\tilde{R}$ is. We have shown the following:

<u>Corollary 3</u>: With the above notation, an R-module M, together with a choice of a basis of M_i, i.e., an isomorphism $f_i : F_i \xrightarrow{\sim} M_i$, for each i corresponds canonically to a <u>cocycle</u> Θ <u>with values in</u> Gl_n, i.e., to a collection of invertible matrices

$$\Theta_{ij} \in Gl_n(R_{ij})$$

such that

$$\Theta_{ij}\Theta_{jk} = \Theta_{ik} \quad \text{in } Gl_n(R_{ijk}) .$$

This does not yet determine the set of isomorphism classes of modules M such that M_i is a free R_i-module of rank n for each i, because there was an arbitrary choice of basis for each M_i. Let

$$f_i': F_i \xrightarrow{\sim} M_i$$

be the isomorphism corresponding to another choice of basis. Then

$$f_i'^{-1} f_i = g_i$$

is an automorphism of F_i, given by some invertible matrix in $Gl_n(R_i)$ which we denote by the same letter. Call $\theta'_{ij} = f_j'^{-1} f_i'$ the corresponding cocycle. Then

$$(4) \qquad \theta'_{ij} = g_j \theta_{ij} g_i^{-1} \quad \text{in} \quad Gl_n(R_{ij}) .$$

Thus two cocycles θ, θ' with values in Gl_n are obtained from the same module M by different choices of bases for M_i iff. there is a collection $\{g_i \in Gl_n(R_i)\}$ such that (4) holds for each i,j. Clearly two isomorphic modules give rise to the same sets of cocycles, and conversely. Hence

<u>Corollary 5</u>: There is a 1-1 correspondence between isomorphism classes of R-modules M such that M_i is a free R_i-module of rank n for each i and equivalence classes of cocycles with values in Gl_n, where

two cocycles θ , θ' are equivalent iff. there is a collection $\{g_i \in Gl_n(R_i)\}$ of invertible matrices such that (4) holds for each pair i,j .

Remark 6: The above corollary is a special case of a very general principal. Of special interest is the case $n = 1$. The modules are locally free of rank one. An invertible 1×1 -matrix is just a unit of R , and Gl_1 is frequently denoted $\tilde{R}^*$ = sheaf of invertible elements of $\tilde{R}$.

E. H^1 .

Definition 1: Let X be a topological space, $\{U_i\}$ a covering by open sets, and F a sheaf of groups on X . A 1 -cocycle a on U_i with values in F is a collection of elements

$$a_{ij} \in F(U_i \cap U_j)$$

such that for each triple i,j,k

$$a_{ij}\, a_{jk} = a_{ik} \qquad \text{in } F(U_i \cap U_j \cap U_k) \ .$$

Two 1 -cocycles a , a' are called cohomologous is there is a collection of elements

$$b_i \in F(U_i)$$

such that

$$a'_{ij} = b_j\, a_{ij}\, b_i^{-1} \qquad \text{in } F(U_i \cap U_j) \text{ for each } i,j \ .$$

This is clearly an equivalence relation, and the set of equivalence classes is denoted by

$$H^1(\{U_i\},F) ,$$

and is called the <u>1-cohomology of</u> F <u>on the covering</u> U_i.

Thus corollary 5 asserts that isomorphism classes of R-modules M such that M_i is a free R_i-module of rank n are in 1-1 correspondence with elements of $H^1(\{U_i\},Gl_n)$.

If $\{V_\nu\}$ is another covering of X, and if each V_ν is contained in some U_i, i.e., $\{V_\nu\}$ is a <u>refinement</u> of the covering $\{U_i\}$, then there is a natural <u>injective</u> map

(2) $$H^1(\{U_i\},F) \longrightarrow H^1(\{V_\nu\},F)$$

given as follows: Say V_ν is contained in $U_{i(\nu)}$. Let a be a 1-cocycle of $\{U_i\}$ with values in F, and define a 1-cocycle $\bar{a}$ of $\{V_\nu\}$ with values in F by

$$\bar{a}_{\nu\mu} = \text{restr. to } V_\nu \cap V_\mu \text{ of } a_{i(\nu)i(\mu)} \in F(U_{i(\nu)} \cap U_{i(\mu)}) .$$

There is a choice of the element $U_{i(\nu)}$ of U_i containing a given V_ν involved in this description, and an important fact is that the map (2) does <u>not</u> depend on these choices.

Thus we can view $H^1(\{U_i\},F)$ as a <u>subset</u> of $H^1(\{V_\nu\},F)$ in a natural way whenever $\{V_\nu\}$ is a refinement of $\{U_i\}$. The union of these sets, as $\{V_\nu\}$ ranges over coverings of X, is denoted by

$$(3) \qquad H^1(X,F)$$

and is called the <u>1 -cohomology of</u> F <u>on</u> X.

We are not going to prove the injectivity of (2), or its independence of the choice of $U_{i(\nu)}$. These facts can be found in any text treating cohomology of sheaves. Notice however that for the sheaf Gl_n, both assertions are clear. For, the map (2) is just the inclusion of the set $\{$isom. classes of modules M which are free on each $U_i\}$ in the set $\{$isom. classes of modules M which are free on each $V\}$. Since any locally free module of rank n will appear in some such set, we get

<u>Corollary 4</u>: The set of isomorphism classes of locally free R-modules of rank n is in 1-1 correspondence with $H^1(X,Gl_n)$.

<u>Remark 5:</u> If F is a sheaf of <u>abelian</u> groups, $H^1(\{U_i\},F)$ (and therefore also $H^1(X,F)$) can be given the structure of an abelian group. For, the 1 -cocycles then form an abelian group, and the cohomology relation is obtained by dividing this group by the group of <u>1 -coboundaries</u> which

are the 1-cocycles which can be written in the form (multiplicative notation)

$$b_j \, b_i^{-1} \quad \text{in} \quad F(U_i \cap U_j)$$

for some collection $\{b_i \in F(U_i)\}$. We leave the verification, which is essentially immediate, to you.

For instance the set of isom. classes of loc. free sheaves of rank 1 on $X = \text{Spec. } R$ forms an abelian group $H^1(X, \tilde{R}^*)$ (cf. Remark D.6). This group is often called the <u>Picard group</u> of X, and is denoted

(6) $$\text{Pic } X = H^1(X, \tilde{R}^*) .$$

For abelian group sheaves, one can also define higher cohomology groups $H^q(X,F)$ $(q > 1)$. There is however no natural group structure on $H^1(X,F)$ if F is non-abelian, and no definition of higher cohomology is known in that case except for $q = 2$, and that is quite complicated.

STALKS AND EXACT SEQUENCES

A. Direct limits.

Definition 1: A filtering set I is a set together with a partial ordering $\leq$ such that for any two elements $i, i' \in I$ there is a $j \in I$ with $i \leq j$ and $i' \leq j$.

Definition 2: A directed system of sets (or directed set) indexed by a filtering set I consists of

(i) A set S_i for each $i \in I$,

(ii) A map $S_i \longrightarrow S_j$ for each $i \leq j$ in I,

such that if $i \leq j \leq k$ the resulting diagram

$$\begin{tikzcd} S_i \arrow[r] \arrow[dr] & S_j \arrow[d] \\ & S_k \end{tikzcd}$$

commutes.

A directed system of groups (rings) is a directed system of sets together with a group (ring) structure on each S_i such that the maps $S_i \longrightarrow S_j$ are homomorphisms. Given a directed system $\{R_i\}$ of rings, a directed system $\{M_i\}$ of modules over $\{R_i\}$ is a directed system of sets together with an R_i module structure for each M_i such that the maps $M_i \longrightarrow M_j$ are additive group homomorphisms and the induced diagrams

$$\begin{array}{ccc} R_i \times M_i & \longrightarrow & M_i \\ | & & | \\ R_j \times M_j & \longrightarrow & M_j \end{array}$$

commute, when $i \leqq j$.

Definition 3: Let $S = \{S_i\}$ be a directed system of sets. Its direct limit, denoted by

$$\varinjlim_{i \in I} S_i = \underset{\rightarrow}{S}$$

is the set obtained by dividing out in $\bigcup_{i \in I} S_i$ by the following equivalence relation:

Let $a_i \in S_i$, $a_{i'} \in S_{i'}$. Then $a_i \sim a_{i'}$ iff. there is a j with $i \leqq j$ and $i' \leqq j$ such that the images in S_j of A_i and $a_{i'}$ are equal, or, as one says, such that

$$a_i = a_{i'} \quad \text{in } S_j .$$

This relation is clearly symmetric and reflexive. It has to be shown to be transitive: Let $a_i \in S_i$, $a_{i'} \in S_{i'}$, $a_{i''} \in S_{i''}$. Suppose

(*) $$a_i = a_{i'} \quad \text{in } S_j$$

for some j $(i \leqq j$, $i' \leqq j)$ and also

$$a_{i'} = a_{i''} \quad \text{in } S_{j'}$$

for some j' $(i' \leqq j'$, $i'' \leqq j')$. Choose k such that $k \geqq j$, $k \geqq j'$. Then by (*) and the commutativity of (2),

$$a_i = a_{i'} \quad \text{in } S_k .$$

Similarly,

$$a_{i'} = a_{i''} \quad \text{in } S_k ,$$

hence

$$a_i = a_{i''} \quad \text{in } S_k$$

which proves the transitivity.

Remark 4: It is clear from the construction that $\varinjlim S_i$ does not change if the index set I is replaced by any subset J which contains arbitrarily large elements, i.e., such that any $i \in I$ is $\leqq j$ for some $j \in J$. Such a subset is called final (or cofinal).

Proposition 5: If $S = \{S_i\}$ is a directed system of groups (rings, modules over a given ring), then $\varinjlim S_i = \underset{\rightarrow}{S}$ inherits this structure from the S_i.

proof: We will treat the case of a group. Let $\underline{a}, \underline{b} \in \underset{\rightarrow}{S}$, and let $a_i, b_i \in S_i$ represent $\underline{a}, \underline{b}$ respectively. Since any two indices are less than a third, $\underline{a}, \underline{b}$ can be so represented (same i). Try to define $\underline{ab}$ = (class of $a_i b_i$). The whole point is to show that this is independent of the choice of the representatives a_i, b_i. Then since three elements $\underline{a},\underline{b},\underline{c}$ can be represented in one S_i, the associativity of multiplication in $\underrightarrow{S}$ follows from the associativity in the S_i. So does the existence of an identity and of inverses.

Well, suppose $\underline{a},\underline{b}$ are also represented by $a_{i'}, b_{i'}$ in $S_{i'}$. Then $a_i = a_{i'}$ in S_j for some j, and similarly $b_i = b_{i'}$ in S_j for some j. One j will work for both $\underline{a},\underline{b}$. Let a_j, b_j be the common images in S_j. Then since $S_i \longrightarrow S_j$ is a group homomorphism,

$$a_i b_i \sim a_j b_j \sim a_{i'} b_{i'} .$$

Hence $\text{class}(a_i b_i) = \text{class}(a_{i'} b_{i'})$, which completes the proof.

Proposition 6: (universal property) Let $S = \{S_i\}$ be a directed system of sets (groups, rings, modules) and let $\underrightarrow{S} = \varinjlim_i S_i$. There are (obvious) canonical maps $S_i \xrightarrow{\ell_i} \underrightarrow{S}$ such that for $i \leq j$ the diagram

$$\begin{tikzcd} S_i \arrow[rr] \arrow[dr] & & S_j \arrow[dl] \\ & \underrightarrow{S} & \end{tikzcd}$$

commutes, and $\underrightarrow{S}$ is the universal object for such a family of maps, i.e., given a set (group, ring, module) T and a collection of maps $f_i: S_i \longrightarrow T$ such that for

$i \leq j$ the diagram

$$(*) \qquad \begin{tikzcd} S_i \arrow[rr] \arrow[dr, "f_i"'] & & S_j \arrow[dl, "f_j"] \\ & T & \end{tikzcd}$$

commutes, there is a <u>unique</u> map $\underset{\rightarrow}{f}: \underset{\rightarrow}{S} \longrightarrow T$ such that

$$f_i = \underset{\rightarrow}{f}\, \ell_i \qquad \text{for each } i .$$

proof: Of course ℓ_i is given from the inclusion of S_i in $\bigcup_j S_j$. Since the S_i together map onto $\underset{\rightarrow}{S}$, it is clear that a map $\underset{\rightarrow}{f}$ will be uniquely determined by a collection $\{f_i\}$. Let $\{f_i\}$ be given, and define $\underset{\rightarrow}{f}: \underset{\rightarrow}{S} \longrightarrow T$ by

$$\underset{\rightarrow}{f}(\underline{s}) = f_i(s_i)$$

where s_i represents $\underline{s}$. Because of (*) this is independent of the choice, and thus defines a map $\underset{\rightarrow}{f}$.

B. <u>Stalks</u>.

Let X be a topological space, F a sheaf on X, and x a point of X. The set of open neighborhoods of x (opens in X containing x) is clearly filtering when ordered by inclusion, i.e., when $U \leq V$ means (unfortunately) $U \supseteq V$.

The <u>stalk</u> F_x of F at x is the direct limit over this filtering set of the sets of sections $F(U)$:

(1) $$F_x = \varinjlim_{x \in U} F(U) \ .$$

Thus (A.5) F_x is a group (ring, module) if F is a sheaf of groups (rings, modules). The stalk is clearly a functor of F, i.e., a map $f\colon F \longrightarrow G$ of sheaves induces a map $f_x\colon F_x \longrightarrow G_x$ of stalks in an obvious way. We leave it to the reader to make the map explicit.

Note that if U is an open containing x, then we have a canonical map (A.5)

(2) $$F(U) \longrightarrow F_x \ .$$

Hence we can use terminology of the following type: Let $a, a' \in F(U)$ be sections.

(3) $$a = a' \quad \underline{\text{at } x} \quad \text{or} \quad \underline{\text{in } F_x}$$

means that the images in F_x are equal. This means they represent the same element of $F_x = \varinjlim_{x\ U} F(U)$. By the definition of $\varinjlim$, it is clear that

(4) $a = a'$ at x iff. there is a $V \subset U$ containing x such that $a = a'$ in $F(V)$.

Moreover, any element of F_x is represented by an element of $F(V)$ for some neighborhood V of x.

Proposition 5: (i) Let F be a sheaf. Two sections $a, a' \in F(U)$ are equal iff. they represent the same element of the stalk F_x for every point x of U.
(ii) A map $f\colon F \longrightarrow G$ of sheaves is an isomorphism iff. for every $x \in X$ the map of stalks $f_x\colon F_x \longrightarrow G_x$ is bijective.

proof: (i) If $a = a'$ at x, then $a = a'$ on V for some neighborhood V of x. Hence if $a = a'$ at x for each $x \in U$, then $a = a'$ on a set of open sets which covers U. Hence (2.E.2a) $a = a'$.

(ii) Clearly, f an isomorphism implies f_x bijective. Conversely, suppose f_x is bijective for each x. We need (3.B.3) to show that $f(U): F(U) \longrightarrow G(U)$ is bijective for each U. Since f_x is injective, it follows that two sections $a, a' \in F(U)$ whose images in $G(U)$ are equal are equal at x for every $x \in U$, hence are equal, by (i). Thus $f(U)$ is injective.

Let $b \in G(U)$. Then for every $x \in U$, there is an element $\underline{a}_x \in F_x$ whose image in G_x is equal to that of b. Let $a_x \in F(V_x)$ be a representative of $\underline{a}_x$ in some neighborhood V_x of x. The image of a_x in $G(V_x)$ is equal to b <u>at x</u>. Therefore, if we replace V_x by a smaller neighborhood, we may assume $f(a_x) = b$ in $G(V_x)$. (We have written f instead of $f(V_x)$, as a shorthand.) Let V_i be some of the V_x's which cover U, and a_i the corresponding elements. Then

$$f(a_i) = b = f(a_j) \quad \text{in } G(V_i \cap V_j) .$$

Since f is injective,

$$a_i = a_j \quad \text{in } F(V_{ij})$$

hence by the sheaf axiom (2.E.2) there is an element $a \in F(U)$ such that $a = a_i$ in $F(V_i)$ for each i. Then the image of a in $G(U)$ is equal to b on each $G(V_i)$, hence equals b. This shows that $f(U): F(U) \longrightarrow G(U)$ is surjective, and completes the proof.

Proposition 6: Let R be a ring, $x \in X = \operatorname{Spec} R$.
(i) The stalk $\tilde{R}_x$ of $\tilde{R}$ at x is the local ring R_{p_x}, where p_x is the prime ideal corresponding to x.
(ii) Let M be an R-module. The stalk $\tilde{M}_x$ of $\tilde{M}$ at x is the module M_{p_x}.

Here we have extended the notation of (2.C) in the obvious way to modules, i.e., if $S = R-p$, then $S^{-1}M$ is denoted by M_p.

proof: In the limit (1), it suffices (A.4) to take neighborhoods U of x which are of the form X_s (2.B.5), where $s \in S = X - p_x$. By the universal property for rings of fractions, we have a map

$$\tilde{R}(X_s) = R_s \longrightarrow R_{p_x} = S^{-1}R,$$

which is of course the map (2), hence a map

$$\varinjlim R_s = \tilde{R}_x \longrightarrow R_{p_x}.$$

Since every element of R_{p_x} is of the form $s^{-1}r$ for $s \in S$, $r \in R$ (S is a multiplicative system (2.C)), it is clear that this map is surjective. To show injectivity, suppose

$$\underline{z} \in \varinjlim R_s$$

has image zero in R_{p_x}. Represent $\underline{z}$ by an element z in R_s for some s, and write

$$z = s^{-n} r \qquad \text{in } R_s .$$

Then $z = 0$ in R_{p_x} iff. $r = 0$ in R_{p_x} iff. there is a $t \subset S$ such that $tr = 0$ in R (2.A.4). Then

$$z = 0 \qquad \text{in } R_{st} \quad (2.A.4),$$

and since the image of z in R_{st} also represents $\underline{z}$, it follows that $\underline{z} = 0$.

The proof for an R module goes the same way.

C. Exact sequences.

The notion of stalk of a sheaf allows us to define injectivity or surjectivity of maps of sheaves. A map $f: F \longrightarrow G$ is said to be injective (surjective) iff. the induced map of stalks $f_x: F_x \longrightarrow G_x$ is injective (surjective) for each $x \in X$. By (B.5(ii)), a map which is both surjective and injective is an isomorphism. It happens that a map f is injective iff. $F(U) \longrightarrow G(U)$ is injective for each U. This follows from (B.5(i)). The same is not true for surjective maps. A surjective map of sheaves does in general not have the property that $F(U) \longrightarrow G(U)$ is surjective. See however (C.3) below.

Let $A \longrightarrow B \longrightarrow C$ be maps of sheaves of abelian groups. The sequence is said to be <u>exact</u> if for each $x \in X$ the induced sequence of stalks $A_x \longrightarrow B_x \longrightarrow C_x$ is exact, i.e., the image of the first map is equal to the kernel of the second.

<u>Proposition 2</u>: (left exactness of sections) Let $0 \longrightarrow A \longrightarrow B \longrightarrow C$ be an exact sequence of sheaves of abelian groups on X. For every open $U \subset X$ the sequence

$$0 \longrightarrow A(U) \longrightarrow B(U) \longrightarrow C(U)$$

is exact.

proof: Recall that the exactness of $0 \longrightarrow A \longrightarrow B$ just means that the map $A \longrightarrow B$ is injective. It was seen above that then $A(U) \longrightarrow B(U)$ is also injective. We need to show the exactness of the sequence at $B(U)$. Let $b \in B(U)$ have image zero in $C(U)$. For each $x \subset X$, the image $\underline{b}$ of b in B_x (B.2) is mapped to zero in C_x, hence is the image of some $\underline{a} \in A_x$, since the sequence of stalks is exact. Let $a \in A(V)$ represent $\underline{a}$ on some neighborhood V of x. Then the image of a

in $B(V)$ is equal to b in B_x, hence is equal to b in some smaller neighborhood of x, which we may suppose equal to V. This is true for each x, hence there is a covering of U by such neighborhoods, say V_i, with elements $a_i \in A(V_i)$, such that $a_i = b$ in $B(V_i)$. Then $a_i = a_j$ in $B(V_{ij})$, hence $a_i = a_j$ in $A(V_{ij})$ because $A \longrightarrow B$ is injective. Thus there exists an $a \in A(U)$ such that $a = a_i$ on V_i. Then $a = b$ in $B(V_i)$ for each i, hence $a = b$ in $B(U)$, which shows that b is in the image of $A(U)$. The converse is clear, so this completes the proof.

As a substitute for surjectivity of sections, one has an exact cohomology sequence. It is very useful for calculating H^1 (cf. exerc. No. 2,6,7):

Proposition 3: Let $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ be an exact sequence of sheaves of abelian groups on X. There is an exact sequence

$$0 \to A(X) \to B(X) \to C(X) \xrightarrow{\delta} H^1(X,A) \to H^1(X,B) \to H^1(X,C) .$$

Note: The sequence has analogues in the case of non-abelian groups, and for abelian groups it continues with the higher cohomology groups.

We will sketch the proof: The sequence is exact at $A(X)$, $B(X)$, by (C.2). Consider $C(X)$: Let $c \in C(X)$. Since

$B \longrightarrow C$ is surjective, c (or rather, its image) is in the image of B_x in every stalk C_x. Hence there is a neighborhood U of x and a section $b \in B(U)$ whose image is equal to c in C_x. Therefore the image of b is equal to c in $C(V)$ for some neighborhood $V \subset U$ of x. Since x is any point of X, we may cover X by opens V_i such that there is an element $b_i \in B(V_i)$ whose image in $C(V_i)$ is c. Then $b_i - b_j$ (additive notation!) has image zero in $C(V_{ij})$. Hence (identifying $A(V_i)$ with a subset of $B(V_i)$)

$$b_i - b_j = a_{ij} \in A(V_{ij}) .$$

Clearly $\{a_{ij}\}$ is a 1-cocycle of V_i with values in A, hence represents an element of $H^1(\{V_i\}, A)$, hence of $H^1(X,A)$. This element is defined to be the image $\delta(c)$ of c. It has to be shown to be well defined. Then δ is obviously a homomorphism.

Now $\delta(c) = 0$ iff. $\{a_{ij}\}$ is a coboundary (3.E.5). This means that

$$a_{ij} = \alpha_i - \alpha_j \qquad \text{on } V_{ij}$$

for some $\alpha_i \in A(V_i)$. Put $\beta_i = b_i - \alpha_i$. Then the image of β_i in $C(V_i)$ is still c, since α_i has image zero. But

$$\beta_i - \beta_j = 0 \qquad \text{on } V_{ij} .$$

Hence there is a $\beta \in B(X)$ with $\beta = B_i$ on V_i (2.E.2). Since the image of β in $C(X)$ is equal to c on each V_i, it is c. Hence $\delta(c) = 0$ iff. c is in the image of $B(X)$. This proves exactness at $C(X)$.

exactness at $H^1(X,A)$: A 1-cocycle $\{a_{ij}\}$ on V_i with values in A represents zero in $H^1(X,B)$ iff. there are sections $b_i \in B(V_i)$ with $b_i - b_j = a_{ij}$ in $B(V_{ij})$. Let c_i be the image of b_i in $C(V_i)$. Then

$$c_i - c_j = 0 \quad \text{on } V_{ij} .$$

Hence there is a $c \in C(X)$ with $c = c_i$ on V_i. Clearly $\delta(c)$ is the cohomology class represented by $\{a_{ij}\}$. Thus $\{a_{ij}\}$ represents zero in $H^1(X,B)$ iff. its cohomology class is in the image of δ, which is what was to be proved.

We leave the exactness at $H^1(X,B)$ as an exercise.

D. Exactness of sections of quasi-coherent sheaves.

Proposition 1: (right exactness of tensor product)
Let R be a ring, M an R-module, and

$$A \longrightarrow B \longrightarrow C \longrightarrow 0$$

an exact sequence of R-modules. Then the sequence

$$M \otimes_R A \longrightarrow M \otimes_R B \longrightarrow M \otimes_R C \longrightarrow 0$$

is exact.

proof: Recall (TP, C.7) that the map $M \otimes A \longrightarrow M \otimes B$ is the unique one sending a tensor $m \otimes a \rightsquigarrow m \otimes b$ where the image of a in B is b.

exactness at $M \otimes C$: The tensors $m \otimes c$ generate $M \otimes C$ (TP, C.1). Since every x is image of some $b \in B$, the module $M \otimes B$ maps onto a set which generates $M \otimes C$, hence onto $M \otimes C$.

exactness at $M \otimes B$: This is essentially (TP, C.8). Let $K \subset B$ be the image of A in B, which is the kernel of $B \longrightarrow C$. Applying (TP, C.8) with suitable relabeling to the modules

$$0 \subset M, \qquad K \subset B$$

we get

$$M \otimes C = M \otimes B / W$$

where W is the submodule generated by tensors of the form $x \otimes k$, $k \in K$ and $x \in M$. Since K is the image of A in B, the module N is just the image of $M \otimes A$ in $M \otimes B$. This completes the proof.

It is <u>not</u> true in general that if $A \longrightarrow B$ is injective then $M \otimes A \longrightarrow M \otimes B$ is also injective. A module M which has this property (for all injections $A \longrightarrow B$) is called a <u>flat</u> module.

However, if R is a ring, $S \subset R$, then $S^{-1}R$ is flat as R-module:

Proposition 2: (exactness of localization) Let R be a ring and $S \subset R$. Let

$$A \longrightarrow B \longrightarrow C$$

be an exact sequence of R-modules. Then

$$S^{-1}A \longrightarrow S^{-1}B \longrightarrow S^{-1}C$$

is also exact.

proof: First of all, if $A \longrightarrow B$ is injective, so is $S^{-1}A \longrightarrow S^{-1}B$. For, let $z \in S^{-1}A$, say (3.A.3) $z = s^{-1}a$ where $s \in S'$, $a \in A$. Then

$$z \rightsquigarrow 0 \quad \text{in } S^{-1}B$$

iff.

$$a \rightsquigarrow 0 \quad \text{in } S^{-1}B \quad (\text{since } s \text{ is a unit in } S^{-1}B)$$

iff. (3.A.4)

$$s'a \rightsquigarrow 0 \quad \text{in } B \text{ for some } s' \subset S'$$

iff.

$$s'a = 0 \quad \text{in } A$$

iff.

$$z = 0 \quad \text{in } S^{-1}A .$$

Moreover, localization is right exact by (D.1), because $S^{-1}A = S^{-1}R \otimes_R A$, etc. These two facts imply the proposition:

Suppose $A \longrightarrow B \longrightarrow C$ exact. Let $C' = \operatorname{im}(B \longrightarrow C)$. Then $C' \longrightarrow C$ is injective, hence

$$S^{-1}C' \longrightarrow S^{-1}C \quad \text{is injective.}$$

Also, $A \longrightarrow B \longrightarrow C' \longrightarrow 0$ is exact, hence (D.1)

$$S^{-1}A \longrightarrow S^{-1}B \longrightarrow S^{-1}C' \longrightarrow 0$$

is exact. Therefore,

$$\operatorname{im}(S^{-1}A \longrightarrow S^{-1}B) = \ker(S^{-1}B \longrightarrow S^{-1}C')$$

$$= \ker(S^{-1}B \longrightarrow S^{-1}C)$$

which is what was to be proved.

<u>Proposition 3</u>: Let R be a ring and $X = \operatorname{Spec} R$. A sequence

$$\tilde{A} \longrightarrow \tilde{B} \longrightarrow \tilde{C}$$

of quasi-coherent sheaves on X is exact iff. the associated sequence (3.B.4) of R-modules

$$A \longrightarrow B \longrightarrow C$$

is exact.

proof: Suppose $A \longrightarrow B \longrightarrow C$ is exact. Then since (B.6) for $x \in X$ the stalk A_x is the localized module A_{p_x}, etc. it follows from Proposition 2 that $A_x \longrightarrow B_x \longrightarrow C_x$ is exact for each x, hence that $\tilde{A} \longrightarrow \tilde{B} \longrightarrow \tilde{C}$ is exact.

Conversely, suppose that $\tilde{A} \longrightarrow \tilde{B} \longrightarrow \tilde{C}$ is exact, and consider the associated sequence $A \longrightarrow B \longrightarrow C$. Let $a \in A$. The image of a in C is zero in C_x for each x (since $A_x \longrightarrow C_x$ is zero). Hence (B.5(i)) the image of a in C is zero. Therefore

$$\operatorname{im}(A \longrightarrow B) = I \subset K = \ker(B \longrightarrow C) .$$

Because of Proposition 2, one sees immediately that

$$K_x = \ker(B_x \longrightarrow C_x) \quad \text{and} \quad I_x = \operatorname{im}(A_x \longrightarrow B_x) .$$

Hence since $A_x \longrightarrow B_x \longrightarrow C_x$ is exact, we have

$$I_x = K_x$$

for each $x \subset X$, and we want to show that $I = K$. But the exact sequence

$$0 \longrightarrow I \longrightarrow K \longrightarrow K/I \longrightarrow 0$$

yields exact sequences of stalks for each $x \in X$ by (D.2). Since $I_x = K_x$, the stalk of K/I at x is zero, thus K/I has all stalks zero, and hence is zero by (B.5(ii)), i.e., $I = K$.

Remark: The above fact is also reflected in the vanishing of $H^1(X,\tilde{A})$ for a quasi-coherent sheaf $\tilde{A}$ (cf. C.3 and problem 4 of exerc. 2).

Corollary 4: Let R be a ring and $S = \{s_i\}$ a set of elements of R which generates the unit ideal. A sequence of modules

$$A \longrightarrow B \longrightarrow C$$

is exact iff. for each i the sequence

$$A_{s_i} \longrightarrow B_{s_i} \longrightarrow C_{s_i}$$

is exact.

PROJECTIVE MODULES

A. The serpent diagram.

With every map $f: M \to N$ of R-modules is associated its kernel and cokernel $(=M/\text{im } f)$. This association is functorial in the following sense: If $f': M' \to N'$ is another map, and if f, f' are embedded in a commutative square

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow & & \downarrow \\ M' & \xrightarrow{f'} & N' \end{array}$$

(which should be called a "morphism of maps"), then there are canonically induced maps

$$\ker f \longrightarrow \ker f'$$
$$\operatorname{coker} f \longrightarrow \operatorname{coker} f' .$$

In fact, $\ker f$ is a submodule of M and its image in M' is obviously in $\ker f'$. This gives the map of kernels. For the cokernels, we have a map $N \longrightarrow N'$, hence a map $N \longrightarrow (N'/\text{im } f') = (\operatorname{coker} f')$. To factor this map through $N \longrightarrow (N/\text{im } f)$, it is enough by the universal mapping property of quotient modules to show that the image of $(\text{im } f)$ in $(\operatorname{coker} f')$ is zero. This just means that M is mapped to zero in $(N/\text{im } f)$, which is clear, since its image is in $(\text{im } f')$. Note that the induced maps are such that the diagram

$$\begin{array}{ccccccc} K & \longrightarrow & M & \xrightarrow{f} & N & \longrightarrow & C \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ K' & \longrightarrow & M' & \xrightarrow{f'} & N' & \longrightarrow & C' \end{array}$$

commutes, where the K's and C's are kernels and cokernels, and this property characterizes the induced maps uniquely.

<u>Proposition 1:</u> (left exactness of kernel) Let

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] \arrow[d, "f'"] & M \arrow[r] \arrow[d, "f"] & M'' \arrow[d, "f''"] \\ 0 \arrow[r] & N' \arrow[r] & N \arrow[r] & N'' \end{tikzcd}$$

be a commutative diagram with <u>exact rows</u>. Then the induced sequence

$$0 \longrightarrow \ker f' \longrightarrow \ker f \longrightarrow \ker f''$$

is exact.

<u>Proposition 2:</u> (right exactness of cokernel) Let

$$\begin{tikzcd} M' \arrow[r] \arrow[d, "f'"] & M \arrow[r] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\ N' \arrow[r] & N \arrow[r] & N'' \arrow[r] & 0 \end{tikzcd}$$

be a commutative diagram with <u>exact rows</u>. Then the induced sequence

$$\operatorname{coker} f' \longrightarrow \operatorname{coker} f \longrightarrow \operatorname{coker} f'' \longrightarrow 0$$

is exact.

<u>Proposition 3:</u> (serpent diagram) Let

$$\begin{tikzcd} & M' \arrow[r] \arrow[d, "f'"] & M \arrow[r] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\ 0 \arrow[r] & N' \arrow[r] & N \arrow[r] & N'' & \end{tikzcd}$$

be a commutative diagram with <u>exact</u> <u>rows</u>. There is a canonical map $\ker f'' \xrightarrow{\delta} \operatorname{coker} f'$ such that the induced sequence

$$\ker f' \longrightarrow \ker f \longrightarrow \ker f'' \xrightarrow{\delta} \operatorname{cok} f' \longrightarrow \operatorname{cok} f \longrightarrow \operatorname{cok} f''$$

is exact.

Note that by propositions 1, 2, we can add zeros to the appropriate end of the sequence if $M' \longrightarrow M$ is injective, or if $N \longrightarrow N''$ is surjective.

We omit the proofs of these propositions.

B. <u>Finiteness conditions on modules.</u>

<u>Definition 1:</u> An R-module M is said to be of <u>finite type</u>, or to be <u>finitely generated</u> if there is a finite subset of M, say $\{m_1, \ldots, m_n\}$, such that every element of M can be written as a linear combination of the elements m_i, i.e., in the form

$$\sum_i r_i m_i$$

for suitable $r_i \in R$. This is the same as saying that if F_0 is the free module on the set $\{x_1, \ldots, x_n\}$ then the map $F_0 \longrightarrow M$ sending $x_i \rightsquigarrow m_i$ is <u>surjective</u>. Hence we can say that M is of finite type if there is a free module of finite rank F_0 and an exact sequence

$$(2) \qquad F_0 \longrightarrow M \longrightarrow 0 .$$

Let $\mathcal{R} \subset F_0$ be the kernel of this map, so that

$$(3) \qquad 0 \longrightarrow \mathcal{R} \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

is exact. In the above notation, $\mathcal{R}$ is called the <u>module of relations</u> among the $\{m_i\}$. This expresses the fact that $\mathcal{R}$ consists of those linear combinations

$$\Sigma\, r_i x_i \qquad\qquad r_i \in R$$

such that

$$\Sigma\, r_i m_i = 0 .$$

If $\mathcal{R}$ is again a module of finite type, then M is said to be of <u>finite presentation</u>. This means that there is a free module of finite rank F_1 and a surjective map $F_1 \longrightarrow \mathcal{R}$. Hence M is of finite presentation if there is an exact sequence

$$(4) \qquad F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0 ,$$

where F_1 , F_0 are free modules of finite rank. Such an exact sequence is called <u>finite presentation</u> of M . The generators of F_1 map to certain relations in F_0 , and any other relation is a linear combination of these.

One could define higher order notions by introducing the module $\mathcal{R}_1 = \ker(F_1 \longrightarrow F_0)$ of "relations among the relations", etc...

In order to justify our terminology, we should really show that the question of whether or not $\mathcal{R}$ is of finite type doesn't depend on the choice of (2) . This is done in (iv) of the following proposition:

Proposition 5: (i) Let M be of finite type. Then any set $\{m_\alpha\}$ which generates M contains a finite subset which already generates M .

(ii) Let $A \longrightarrow B \longrightarrow C \longrightarrow 0$ be an exact sequence of modules. If B is of finite type, so is C . If A and C are of finite type, so is B .

(iii) Let $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ be an exact sequence. If C has a finite presentation and B is of finite type, then A is of finite type.

(iv) If M has a finite presentation $F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$ and if $F_0' \longrightarrow M \longrightarrow 0$ is a map corresponding to another finite set of generators for M , then the module of relations $\mathcal{R}' = \ker(F_0' \longrightarrow M)$ is finitely generated.

Proof: (i). Let say $\{u_1,\ldots,u_n\}$ be any finite set of generators of M . Write each $\{u_i\}$ as a finite linear combination of some m_α's , say

$$u_i = \sum_i a_i \, m_{\alpha_i} \; .$$

Then with only a finitely many m_α , we can express all the $\{u_i\}$, hence since $\{u_i\}$ generates M , so does this finite set.

(ii). Clearly, if $\{b_i\}$ is a set of generators for B, then the images of the elements b_i in C generate C. Hence if B is of finite type, so is C.

Suppose that A, C are of finite type. Let $\{\bar{a}_1,\ldots,\bar{a}_n\}$ be the images in B of a set $\{a_i\}$ of generators for A, and let $b_1,\ldots,b_s$ be representatives on B of a set $\{c_1,\ldots,c_s\}$ of generators of C. Then I claim that the set $\{\bar{a}_i, b_j\}$ generates B. In fact, if $x \in B$ is arbitrary, then its image $\bar{x} \in C$ is a linear combination,

$$\bar{x} = \Sigma\, r_j c_j \,.$$

Hence the element

$$x - \Sigma\, r_j b_j$$

of B has image zero in C, i.e., is in $\ker(B \to C)$, hence in $\operatorname{im}(A \to B)$. Say it is the image of $\Sigma\, r_i' a_i$. Then

$$x = \Sigma\, r_i' \bar{a}_i + \Sigma\, r_j b_j$$

is a linear combination of the elements $\{\bar{a}_i, b_j\}$, which is what was to be shown.

(iii). Let $0 \to \mathcal{R} \to F_0 \to C \to 0$ be a finite presentation of C. Since F_0 is free, a map of this module to any module is given by assigning the image of a basis. Hence it is clear that there is a map $F_0 \to B$ making the triangle

$$\begin{tikzcd} F_0 \arrow[rr] \arrow[dr] & & B \arrow[dl] \\ & C & \end{tikzcd}$$

commute. Replace it by the square

$$\begin{array}{ccc} F_0 & \longrightarrow & C \\ \downarrow & & \| \\ B & \longrightarrow & C \end{array} .$$

There is an induced map of kernels $\mathcal{R} \longrightarrow A$ (cf. A), hence a diagram

$$\begin{array}{ccccccccc} & & K' & & K & & 0 & & \\ 0 & \longrightarrow & \mathcal{R} & \longrightarrow & F_0 & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & D' & & D & & 0 & & \end{array}$$

where we have placed the kernels and cokernels around the periphery. Applying the serpent diagram, we get an exact sequence

$$0 \longrightarrow K' \longrightarrow K \longrightarrow 0 \longrightarrow D' \longrightarrow D \longrightarrow 0 .$$

Hence $D' \approx D$. Since F_0 is of finite type, so is C, hence D' (by (i)). By assumption, $\mathcal{R}$ is of finite type too. Therefore (i) and the exact sequence

$$\mathcal{R} \longrightarrow A \longrightarrow D' \longrightarrow 0$$

imply that A is of finite type.

(iv). Apply (iii).

<u>Proposition 6:</u> If $R \longrightarrow R'$ is a homomorphism and M is an R-module of finite type (resp. of finite presentation), then $R' \otimes_R M$ is again of finite type (resp. of finite

presentation).

Proof: By (4.D.1) the functor $R' \otimes_R \cdot$ is right exact. Therefore, an exact sequence $F_0 \longrightarrow M \longrightarrow 0$ yields an exact sequence $R' \otimes_R F_0 \longrightarrow R' \otimes_R M \longrightarrow 0$, showing that if M is of finite type, so is $R' \otimes_R M$. The case of finite presentation is similar.

Proposition 7: A module M is of finite type (resp. finite presentation) if and only if there is a set $\{s_i\}$ of elements of R which generates the unit ideal, such that M_{s_i} is of finite type (resp. finite presentation) as R_{s_i}-module for each i.

Proof: The fact that if M is of finite type (resp.) then M_{s_i} is too, follows from Prop. 6, and the fact (3.A) that localization is a tensor product. Conversely, suppose that M_{s_i} is of finite type for each i. We may assume $\{s_i\}$ a finite set. Let $\{m_{ij}\}_j \subset M_{s_i}$ be a finite set of elements which generate the module. Each m_{ij} is of the form $s_i^{-n} m'_{ij}$ for suitable $m'_{ij} \in R$. Since s_i is a unit in R_{s_i}, the elements $\{m'_{ij}\}_j$ for the various modules are all in R. Then I claim that the set $\{m'_{ij}\}_{ij}$ generates N. This means that the map from the free module F on the set $\{x_{ij}\}_{ij}$ to M sending $x_{ij} \rightsquigarrow m_{ij}$ is surjective. To check this, it suffices (4.D.3) to do so locally, hence to do so for each M_{s_i}. But the elements $\{m'_{ij}\}$ clearly generate M_{s_i}, and so we are done.

If M_{s_i} is of finite presentation for each i, then we already know that M is finitely generated, hence that there is an exact sequence $F_0 \longrightarrow M \longrightarrow 0$ with F_0 free and of finite rank. We want to show that the module $\mathcal{R}$ of relations is of finite type. But to show this it suffices to show that the module $\mathcal{R}_{s_i}$ is of finite type for each i, which follows immediately from the fact that M_{s_i} is finitely presented, and from (5(iii)).

C. Localization of homomorphisms.

Let $R \longrightarrow R'$ be a ring homomorphism, and M, N R-modules. If $f: M \longrightarrow N$ is a homomorphism, then since $R' \otimes .$ is a functor, there is induced a homomorphism

(1) $$R' \otimes f = f': R' \otimes M \longrightarrow R' \otimes N .$$

It is given by the formula

$$f'(r' \otimes m) = r' \otimes f(m) .$$

Remember that $\mathrm{Hom}_R(M,N)$ is an R-module under addition and scalar multiplication of homomorphisms. It is easy to see that the map (given by (1))

(2) $$\mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_{R'}(R' \otimes M, R' \otimes N)$$

is R-linear, i.e., a homomorphism of modules, where the term on the right, which is naturally an R'-module, is viewed as an R-module by restriction of scalars. By the characteristic property (TP. D.1) of $\otimes$, (2) induces a map

(3) $$R' \otimes_R (\mathrm{Hom}_R(M,N)) \longrightarrow \mathrm{Hom}_{R'}(R' \otimes M,\ R' \otimes N)\ .$$

It sends a tensor $r' \otimes f$ to the homomorphism

(4) $$[r' \otimes f] : R' \otimes M \longrightarrow R' \otimes N$$

given by

(4) $$[r' \otimes f](t' \otimes m) = (r't') \otimes f(m)\ .$$

Suppose now that $R' = S^{-1}R$ for some subset S of R. Then following our notation (2.D.2) , we can write an element of $S^{-1}(\mathrm{Hom}_R(M,N))$ in the form $s^{-1}f$. The map (4)

(5) $$[s^{-1}f] : S^{-1}M \longrightarrow S^{-1}N$$

of localized modules is just given by

(5) $$[s^{-1}f](t^{-1}m) = (st)^{-1}(f(m))\ .$$

In general, (3) is neither injective nor surjective, but we have the following:

<u>Proposition 7:</u> Let R be a ring and $S \subset R$. Let M, N be R-modules, and suppose that M is finitely presented. Then the map (3)

$$S^{-1}(\mathrm{Hom}_R(M,N)) \longrightarrow \mathrm{Hom}_{S^{-1}R}(S^{-1}M,\ S^{-1}N)$$

is an isomorphism.

Proof: <u>injectivity</u>. Suppose that for some element $s^{-1}f \in S^{-1}(\mathrm{Hom}_R(M,N))$ the associated homomorphism $[s^{-1}f]$ is zero. This means (5)

$$[s^{-1}f](m) = s^{-1}(f(m)) = 0 \quad \text{in } S^{-1}N$$

for each $m \in M$. Hence (2.A.4)

$$(8) \qquad s'f(m) = 0 \qquad \underline{\text{in } N}$$

for some $s' \in S'$. Since M is of <u>finite type</u>, one s' will do in (8) for each of a finite set of generators of M, hence for every element of M. Thus there is an $s' \in S'$ such that (8) holds for each element of M. This means

$$s'f = 0 \qquad \text{in } \mathrm{Hom}_R(M,N) \quad ,$$

whence

$$f = 0 \quad \text{in } S^{-1}(\mathrm{Hom}_R(M,N)) \ .$$

Hence also $s^{-1}f = 0$, which proves the injectivity.

<u>surjectivity</u>. Let

$$\phi\colon S^{-1}M \longrightarrow S^{-1}N$$

be an $S^{-1}R$-homomorphism. It suffices to show that there is some element $s \in S'$ such that the map $s\phi$ comes from a homomorphism $f\colon M \longrightarrow N$. Choose a set of generators m_i for M, so as to get an exact sequence

$$0 \longrightarrow \mathcal{R} \longrightarrow F_0 \longrightarrow M \longrightarrow 0 \ .$$

Multiplying ϕ through by some $s \in S'$ to clear denominators, we may assume that $\phi(m_i) = n_i$ in $S^{-1}N$ for some elements $n_i \in N$. Then we can define a map

$$\psi \colon F_0 \longrightarrow N$$

be sending the basis $x_i \rightsquigarrow m_i$. We would like to extend this map to a diagram

(9)
$$\begin{tikzcd} F_0 \arrow[r] \arrow[dr, "\psi"'] & M \arrow[d, "f"] \\ & N \end{tikzcd}$$

If this is done, we will have $f(m_i) = n_i$ and it then will follow easily that $[f] = \phi$.

Now by the universal mapping property for the quotient module $M \approx F_0/\mathcal{R}$, the map f exists iff. the image of $\mathcal{R}$ in N under ϕ is zero. But we have a diagram

$$\begin{tikzcd} S^{-1}F_0 \arrow[r] \arrow[dr, "{[\psi]}"'] & S^{-1}M \arrow[d, "\phi"] \\ & S^{-1}N \end{tikzcd}.$$

Hence the image of $S^{-1}\mathcal{R}$ in $S^{-1}N$ is zero, at any rate, and this means that for any $z \in \mathcal{R}$,

$$\psi(z) = 0 \quad \text{in } S^{-1}N .$$

Hence

$$s\psi(z) = 0 \text{ in } N$$

for some $s \in S'$. Since M is <u>finitely presented,</u> $\mathcal{R}$ is of finite type, and so one s will do for all $z \in \mathcal{R}$ (since one will kill $\psi(z)$ for z any one of a finite set of generators).

Now we can still multiply the map ϕ by s, and then if we also replace by $s\psi$, we do get $\psi(\mathcal{R}) = 0$, and hence f exists. This completes the proof.

D. The sheaf Hom.

Let F, G be sheaves of abelian groups, or of modules over a given sheaf of rings on a topological space X. Put $H(U) = \mathrm{Hom}(F|U, G|U)$ (nb. this means maps (3,B.3) of the sheaf $F|U$ to $G|U$, and is not to be confused with $\mathrm{Hom}(F(U), G(U))$ = maps from the group of sections $F(U)$ to $G(U)$!). Given a map $F|U \longrightarrow G|U$, we can restrict it to a smaller open set $V \subset U$. Hence H thus defined is a pre-sheaf. It is actually a sheaf. This is because, to give a map $F \longrightarrow G$, it suffices to do so locally, i.e., on each open set U_i of a covering of X, with compatibility on U_{ij}. This is clear from the discussion of (3.C).

We will denote this sheaf by $\underline{\mathrm{Hom}}(F,G)$

$$(1) \qquad \underline{\mathrm{Hom}}(F,G)[U] = \mathrm{Hom}(F|U, G|U) .$$

If M, N are R-modules and $X = \mathrm{Spec}\, R$, we will write (1) as

$$\underline{\mathrm{Hom}}_{\tilde{R}}(\tilde{M},\tilde{N}) .$$

As a consequence of (C.7), we get

Corollary 2: Let M, N be R-modules, and let $\underline{Hom}_R(M,N)$ denote the sheaf associated to the R-module $Hom_R(M,N)$. There is a natural map

$$Hom_R(M,N) \longrightarrow \underline{Hom}_{\tilde{R}}(\tilde{M},\tilde{N})$$

and if M is finitely presented, it is an isomorphism.

Translating the map above for an open set of the form X_s, it reads

$$(Hom_R(M,N))_s \longrightarrow Hom(\tilde{M}|X_s,\ \tilde{N}|X_s) .$$

By (3.B.4), the term on the right is $Hom_{R_s}(M_s,N_s)$. Thus the map is the one given by (C.3). It extends to arbitrary opens as usual (3.C.1), and the bijectivity if M is finitely presented is the assertion of (C.7).

E. Projective modules.

Definition 1: An R-module P is projective if, given a diagram

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow & & \\ B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

, the row exact, there is a map $P \longrightarrow B$ such that the triangle

$$\begin{tikzcd} & P \arrow[dl] \arrow[d] \\ B \arrow[r] & C \end{tikzcd}$$

commutes.

This can also be stated as follows: If

$$B \longrightarrow C$$

is surjective, so is the induced map

$$\mathrm{Hom}_R(P,B) \longrightarrow \mathrm{Hom}_R(P,C) \quad .$$

To appreciate the meaning of this, note

<u>Proposition 2:</u> (left exactness of Hom in the second variable)

Let $0 \to A \to B \to C$ be an exact sequence, and M any R-module. The induced sequence

$$0 \longrightarrow \mathrm{Hom}_R(M,A) \longrightarrow \mathrm{Hom}_R(M,B) \longrightarrow \mathrm{Hom}_R(M,C)$$

is exact.

We leave the proof as an exercise.

Therefore, we can express the fact that P is projective by saying that

$$\mathrm{Hom}_R(P,\cdot)$$

is an <u>exact</u> <u>functor</u>. For, (left exactness) + (preserves surjections) $\Longrightarrow$ (exactness) .

An analogous discussion could be made by reversing all arrows (Hom is right exact in the first variable). The resulting notion is that of <u>injective</u> module.

<u>Elementary</u> <u>facts.</u>

(3) R is projective as a module over itself.

For, $\mathrm{Hom}_R(R,M) \approx M$, i.e., $\mathrm{Hom}_R(R,\cdot)$ is the identity functor, hence certainly exact.

(4) A direct sum of projectives is projective.

For, to map a direct sum to B , it suffices to map each summand to B , hence the condition of the definition is trivially satisfied for the direct sum if it is for each summand.

(5) A free module is projective.

Combine (3) and (4) .

(6) Let $0 \to A \to B \to C \to 0$ be exact.

If C is projective, the sequence <u>splits</u>, i.e., $B \approx A \oplus C$.

More precisely, there is a map $C \to B$ (necessarily injective) which, when composed with the map $B \to C$ above gives the identity on C . We just put $P = B$ in definition 1. Then if we denote by C also its image in B , we have clearly $A \cap C = (0)$, and $A + C = B$, hence $B = A \oplus C$. Note, however, that the splitting $B \approx A + C$ is <u>not</u> canonical. It depends on the choice of the map $C \to B$.

(7) Let P be a projective module. If P is of finite type, it is also of finite presentation.

For, we get (B.3) an exact sequence

$$0 \to \mathcal{R} \to F_0 \to P \to 0$$

with F_0 of finite type, and we have to show that $\mathcal{R}$ is of finite type. But by (6) , $F_0 \approx \mathcal{R} \oplus P$, hence $\mathcal{R}$ is a <u>quotient</u> of the finitely generated module F_0 , hence itself finitely generated (B.5(i)).

(8) Let P be a projective R-module. Then $S^{-1}P$ is a projective $S^{-1}R$ -module for any $S \subset R$.

For, let

$$\begin{array}{ccc} & S^{-1}P & \\ & \downarrow & \\ B' \longrightarrow & C' \longrightarrow & 0 \end{array}$$

be a diagram of $S^{-1}R$ -modules to test projectivity. Combining with the canonical map $P \longrightarrow S^{-1}P$, we get an R-linear map $P \longrightarrow C'$, hence an R-linear map $P \longrightarrow B'$ making a commutative triangle, since P is projective. Hence by the characteristic property (TP.D.1) , there is a $S^{-1}R$ -linear map $S^{-1}P \longrightarrow B'$ induced by this map, and one sees immediately that it has the required property.

<u>Proposition 9:</u> (projective is a local notion)

Let P be a module of finite presentation. Then P is projective iff. there is a subset $S \subset R$ which generates the unit ideal such that P_s is a projective R_s-module for each $s \in S$.

Proof: This follows from (D.2) . To show as in the definition that

$$\mathrm{Hom}_R(P,B) \longrightarrow \mathrm{Hom}_R(P,C)$$

is surjective, it suffices by (3.B.4) , (4.D.3) , (D.2) to show that the map of <u>quasi-coherent sheaves</u>

$$\underline{\mathrm{Hom}}_{\tilde{R}}(\tilde{P},\tilde{B}) \longrightarrow \underline{\mathrm{Hom}}_{\tilde{R}}(\tilde{P},\tilde{C})$$

is surjective, and this is a local question. Note the elegance of this method of proof (due to Serre, I believe), in which results about modules are applied to the module Hom . The converse is contained in (8) .

Corollary 10: A locally free module of finite rank is projective.

For, it is finitely presented by (B.7) since it is locally free. Now apply (5) , and the above proposition.

F. Nakayama Lemma.

This is a very important tool:

Theorem (1): (Nakayama Lemma) Let R be a ring, and $\mathfrak{a}$ an ideal contained in every maximal ideal of R (for instance, R local and $\mathfrak{m}$ its maximal ideal). Let M be an R-module of finite type. If $\mathfrak{a} M = M$, i.e. (cf. TP.D.2) if $(R/\mathfrak{a}) \otimes_R M = M/\mathfrak{a} M = (0)$, then $M = (0)$.

Proof: Let $\{m_1, \ldots, m_n\}$ generate M . Since $\mathfrak{a} M = M$, we can write m_1 as contained in $\mathfrak{a} M$, i.e., in the form

$$m_1 = \sum_i a_i m_i \qquad a_i \in \mathfrak{a}.$$

Solving for m_1 ,

$$(1 - a_1)m_1 = \sum_{i=2}^{n} a_i m_i .$$

But since $\mathfrak{a}$ is in every maximal ideal, $1 - a_1$ is in no maximal ideal, hence in no prime ideal, and therefore is a unit, because of (1.A) . Thus we can express m_1 as a linear combination of the other m_i's, and so m_1 is not needed to generate M. By induction, nothing is needed to generate M, hence $M = (0)$.

Remark: The assumption that M is of finite type is essential.

Here are some variations on this theme:

Corollary 2: Let R, $\mathfrak{a}$ be as above, and $A \longrightarrow B$ a map of R-modules, with B of finite type. If $A/\mathfrak{a}A \longrightarrow B/\mathfrak{a}B$ is surjective, so is $A \longrightarrow B$.

Let C be the cokernel of $A \longrightarrow B$, so that the sequence $A \to B \to C \to 0$ is exact. By right exactness of tensor product (4.D.1),
$A/\mathfrak{a}A \longrightarrow B/\mathfrak{a}B \longrightarrow C/\mathfrak{a}C \longrightarrow 0$ is again exact. Thus if $A/\mathfrak{a}A \longrightarrow B/\mathfrak{a}B$ is surjective, then $C/\mathfrak{a}C = (0)$. Since B is of finite type, so is C (B.5(ii)), hence $C = (0)$ by the Nakayama lemma.

Corollary 3: If B is a module of finite type, and if $b_1, \ldots, b_n$ are elements of B whose residues (modulo $\mathfrak{a}B$) generate $B/\mathfrak{a}B$, then $b_1, \ldots, b_n$ generate B.

For, we want to show that the map $F \longrightarrow B$ of the free module F on a set $x_1, \ldots, x_n$ sending $x_i \rightsquigarrow b_i$ is surjective, and the assumption implies that $F/\mathfrak{a}F \longrightarrow B/\mathfrak{a}B$ is surjective, hence we may apply (2).

We remark that also in this corollary, it is essential to know beforehand that B is of finite type.

As a corollary, we obtain the fact that finitely generated projectives over a local ring are free:

Proposition 4: Let R be a local ring, and P a finitely generated projective module over R. Then P is a free module.

Proof. Denote by $\overline{R}$ the field $R/\mathfrak{m}$ ($\mathfrak{m}$ is the maximal ideal), and by $\overline{P}$ the $\overline{R}$-vector space $P/\mathfrak{m}P$. Let $x_1,\ldots,x_n$ be elements of P such that their residues $\overline{x}_1,\ldots,\overline{x}_n$ in $\overline{P}$ form a basis for that vector space. I claim that $x_1,\ldots,x_n$ is a basis for P: By corollary 3, the elements $\{x_i\}$ generate P, at any rate. Hence we get an exact sequence (B.3)

$$0 \to \mathcal{R} \to F_0 \to P \to 0 \quad ,$$

and we need to show that $\mathcal{R} = (0)$. But $\mathcal{R}$ is of finite type. Thus it suffices (1) to show that $\overline{\mathcal{R}} = \mathcal{R}/\mathfrak{m}\mathcal{R} = (-0)$. We know that $\overline{F}_0 \hookrightarrow \overline{P}$, since that elements $\overline{x}_i$ are a basis. Now because tensor product is only right exact, we can't yet conclude that $\overline{\mathcal{R}} = (0)$! We need to use the projectivity of P. Using that, the sequence above splits (E.6), and since tensor product does commute with direct sums (TP.C.4), we get

$$\overline{F}_0 \approx \overline{\mathcal{R}} \oplus \overline{P} = \overline{\mathcal{R} \oplus P} \quad .$$

Since $\overline{F}_0 \hookrightarrow \overline{P}$, this shows that $\overline{\mathcal{R}} = (0)$, and completes the proof.

G. Characterization of projectives of finite type.

The result is the following:

Theorem 1: Let R be a ring and M an R-module. The following are equivalent:

(i) M is a projective of finite type.

(ii) M is locally free of finite rank.

(iii) M is finitely presented and for every $p \in \operatorname{Spec} R$, M_p is a free R_p-module.

Proof: (ii) $\Rightarrow$ (i) and (i) $\Longrightarrow$ (iii) are done ((E.10) and (E.8) + (F.4)). We need only show (iii) $\Longrightarrow$ (ii). This is an example of a standard kind of reasoning: What we need to show is the following:

Lemma 2: If M is an R-module which is finitely presented, and such that M_p is a free R_p-module for some prime p of R, then there is an $s \in R-p$ such that M_s is a free R_s-module.

For, applying this to every $p \in \operatorname{Spec} R$, we find that M is locally free.

To show lemma 2, choose elements $x_1, \ldots, x_n$ which form a basis for M_p. Clearing denominators, we may assume $x_i \in M$. Then we get a corresponding map

$$F \longrightarrow M$$

of a free module to M, and we know $F_p \xrightarrow{\sim} M_p$. Hence we are reduced to the following lemma:

Lemma 3: Let $f: M \longrightarrow N$ be a map of R-modules, and assume M is of finite type and N is of finite presentation. Suppose that $f_p: M_p \longrightarrow N_p$ is an isomorphism for some $p \in \operatorname{Spec} R$. Then there is an $s \in R-p$ such that $f_s: M_s \longrightarrow N_s$ is an isomorphism.

We first settle the special case $N = (0)$:

Lemma 4: Let M be an R-module of finite type. If $M_p = (0)$ for some $p \in \operatorname{Spec} R$, then there is an element $s \in R-p$ such that $M_s = (0)$.

Proof of (4): Let $\{m_1, \ldots, m_n\}$ generate M. Since each m_i is zero in M_p, there is an $s \in R-p$ such that

$$sm_i = 0 .$$

One s will do for all m_i. Then also $sx = 0$ for any $x \in M$, hence $M_s = (0)$.

Proof of lemma (3): Let C be the cokernel of f. C is of finite type (B.5(ii)), and $C_p = (0)$. Hence $C_s = (0)$ for some s, by lemma 4. Localizing everything with respect to this s, we may assume that the map $f: M \longrightarrow N$ is already surjective. The finiteness conditions on M, N are preserved (B.6). Then $\ker f = K$ is of finite type (B.5(iii)), and $K_p = (0)$, hence $K_s = (0)$ for some $s \in R-p$, again by lemma 4. This completes the proof of Lemma 3, and of theorem 1.

CLASSICAL IDEAL THEORY

The main discussion starts in section C. In the first two sections, we introduce some notions which will be needed, and which we will study in more detail later.

A. Noetherian rings and modules.

Definition 1: A module M is noetherian if every submodule of M is of finite type (5.B.1). (In particular, M itself is of finite type, but this is in general not sufficient.) A ring R is noetherian if it is noetherian as a module over itself, which means that every ideal has a finite set of generators.

Equivalent conditions:

(2) Every increasing sequence of submodules

$$N_1 \subseteq N_2 \subseteq N_3 \quad \ldots$$

of M becomes constant, eventually.

(3) Every set $S \neq \emptyset$ of submodules of M contains a maximal element.

For a ring, you just replace the word submodule by the word ideal.

To prove the equivalence of (1), (2), (3) is an easy exercise: If M is noetherian, then the union $N = \bigcup N_i$

of an increasing sequence of submodules (which is again a submodule) is generated by finitely many elements, and these are therefore in some N_i and so $N_i = N$. Thus the sequence is constant after that point. This shows that (1) $\Longrightarrow$ (2). If (2) holds and S is a non-empty set of submodules, choose any one, and call it N_1. If it is maximal, (3) is proved. If not, there is a larger submodule in S, call it N_2, etc.. By (2), the process stops, showing that S contains a maximal element, i.e., that (3) holds. Finally, suppose that (3) holds. Let N be any submodule, and let S be the set of finitely generated submodules of N, which is non-empty because it contains (0). Clearly, the only possible maximal element of S is N itself, since we could always add a generator to any smaller module, and the result would again be finitely generated. Thus N must be in S, which proves (1).

Elementary properties:

(4) A submodule or a quotient module of a noetherian module is again noetherian.

For submodules, this is trivial from the definition. For a quotient module M/N, where M is noetherian, recall that submodules of M/N are in one-one correspondence with submodules of M which contain N. Now condition (2) implies that M/N is noetherian.

(5) Let $A \longrightarrow B \longrightarrow C$ be an exact sequence. If A and C are noetherian, so is B.

This is essentially the converse of (4). We may by (4) replace A by its image in B and C by the image of $B \longrightarrow C$, so as to get an exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 .$$

Let N be a submodule of B. Then the sequence

$$0 \longrightarrow A \cap N \longrightarrow N \longrightarrow N/A \cap N \longrightarrow 0$$

is exact (n-th isom. thm.), and we want to show that N is finitely generated. Now $A \cap N \subset A$ and $N/A\cap N \subset C$, hence these two are finitely generated, and so we are through by (5.B.5(ii)).

(6) A finite direct sum of noetherian modules is noetherian.

(7) Let R be a noetherian ring, and I an ideal of R. Then $\overline{R} = R/I$ is noetherian.

To see this, note that any ideal of $\overline{R}$ may be viewed as an R-submodule of $\overline{R}$ by letting R act through the map $R \longrightarrow \overline{R}$. By (4), $\overline{R}$ is a noetherian R-module, from which the result follows immediately.

(8) Let R be a noetherian ring. Then the following conditions on an R-module M are equivalent:

(i) M is noetherian.

(ii) M is of finite type.

(iii) M is finitely presented.

By (6), a free module of finite rank is noetherian. Hence by (4), an exact sequence $0 \longrightarrow \mathcal{R} \longrightarrow F_0 \longrightarrow M \longrightarrow 0$ with F_0 free and of finite rank implies M and $\mathcal{R}$ noetherian, and so $\mathcal{R}$ of finite type, hence M finitely presented. This shows that (ii) implies (i) and (iii). (iii) $\Longrightarrow$ (ii) and (i) $\Longrightarrow$ (ii) are trivial.

(9) Let M be a noetherian R-module. Then $S^{-1}M$ is a noetherian $S^{-1}R$-module for any $S \subset R$. In particular, $S^{-1}R$ is noetherian if R is.

Let N' be any submodule of $S^{-1}M$, and denote by $\phi\colon M \longrightarrow S^{-1}M$ the map. Then (this is similar to 2.B.1) the submodule of $S^{-1}M$ generated by $\phi(\phi^{-1}(N'))$ is again N'. For, it is clearly in N', and if $x \in N'$ is any element, then $x = s^{-1}m$ for some $s \in S'$, $m \in M$, hence $sx = m$ is in $\phi(\phi^{-1}(N'))$. But s is a unit, and so the submodule generated by sx contains x. Now $\phi^{-1}(N')$ is a submodule of M, hence is finitely generated. The images of these generators generate N', which shows N' finitely generated.

The geometry of the spectrum of a noetherian ring has the following agreeable properties:

Proposition 10: Let R be noetherian, and $X = \operatorname{Spec} R$.

(i) Every descending chain $Y_1 \supseteq Y_2 \supseteq \dots$ of closed subsets of X becomes constant, eventually.

(ii) Every non-empty set S of closed subsets of X has a minimal element.

(iii) Every closed set Y is a finite union of irreducible closed sets (cf. (1.F)).

Assertions (i), (ii) are just immediate consequences of (2), (3) applied to the ideals $\mathcal{I}(Y)$ (cf. 1.D). To prove (iii), let S be the set of closed subsets for which the assertion is false. If S were not empty, it would contain a minimal element Y, by (ii). Y cannot be irreducible, hence is a union of two proper closed subsets. Since Y is minimal, each of these subsets is a finite union of irreducible subsets, hence Y is too; a contradiction. Thus S is empty.

B. Integral ring extensions.

Definition 1: Let $R \longrightarrow A$ be a ring homomorphism, so that A is a (commutative) R-algebra. An element $\alpha \in A$ is said to be integral over R if it is a root of an equation of the form

$$(2) \qquad x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_o = 0$$

with $a_i \in R$.

The important thing is that the equation is monic. Note that when we substitute α in (2), we (naturally) replace the coefficients a_i by their images in A, i.e., we view them as scalars for the structure of R-algebra on A.

Theorem 3: Let $R \longrightarrow A$ be as above, and $\alpha \in A$. The following are equivalent:

(i) α satisfies an equation (2).

(ii) The subalgebra $R[\alpha]$ of A generated by α is of finite type as an R-module.

(iii) There is an $R[\alpha]$-module M which is faithful, and which is of finite type as an R-module (by restr. of scalars).

A module M' over a ring R' is called faithful if no element of R' other than zero annihilates all of M'. For instance, R' itself is faithful.

proof: Suppose (i) holds. Now $R[\alpha]$ is generated as a module by the powers $1, \alpha, \alpha^2, \ldots$ of α, in any case. But when the equation

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_o = 0$$

holds, we can use it repeatedly to express any power as a linear combination of the powers $1, \alpha, \ldots, \alpha^{n-1}$. Thus $R[\alpha]$ is generated by these powers, and hence is of finite type.

If (ii) holds, then we can take for M the module

$R[\alpha]$ in (iii), hence (iii) holds.

Suppose that (iii) holds. We are to prove (i): Let $m_1, \dots, m_n$ generate M as R-module (hence as $R[\alpha]$-module). Since M is an $R[\alpha]$-module, we can express the element αm_i as linear combinations of m_j with coefficients in R. Say

$$\alpha m_i = \sum_j a_{ij} m_j \qquad a_{ij} \in R .$$

In matrix notation, we get by bringing everything to one side of the equation

$$(4) \qquad (\alpha I - (a_{ij})) \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} ,$$

where I denotes the identity matrix. (You have to read the matrix $(\alpha I - (a_{ij}))$ as in A, replacing the elements a_{ij} by their images!) Put $(b_{ij}) = (\alpha I - (a_{ij}))$ and let (B_{ij}) be the adjoint matrix of (b_{ij}), so that

$$(B_{ij})(b_{ij}) = \det(b_{ij})\ I .$$

Multiplying (4) on the left by (B_{ij}), we get

$$\det(b_{ij}) \cdot I \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} ,$$

i.e., $\det(b_{ij})\, m_i = 0$ for each i. Thus $\det(b_{ij})\, M = (0)$, hence since M is a faithful $R[\alpha]$-module, $\det(b_{ij}) = 0$.

But by definition of (b_{ij}), this just expresses the fact that α is a root of the characteristic polynomial of the matrix (a_{ij}), which is a monic equation of the form (2) having coefficients in R. This completes the proof.

Definition 5: A commutative R-algebra A is called integral over R if every element of A is integral.

Corollary 6: Let $R \longrightarrow A \longrightarrow B$ be ring homomorphisms. If A is integral over R and B is integral over A, then B is integral over R.

For, let $\beta \in B$, and let

$$\beta^n + \alpha_{n-1}\beta^{n-1} + \ldots + \alpha_1\beta + \alpha_0 = 0$$

be a monic equation for β over A $(\alpha_i \in A)$. Since each α_i is integral over R, it is easily seen that the subalgebra $R[\alpha_i,\beta]$ of B generated by $\{\beta,\alpha_i\}$ (strictly speaking, replace the α_i by their images in B) is a finite type R-module. I leave the verification to you. But $R[\alpha_i,\beta]$ is an $R[\beta]$-module, and is clearly faithful as such, since it contains $R[\beta]$. Hence β is integral over R by (3(iii)).

Corollary 7: Let $R \longrightarrow A$ be a ring homomorphism. The set of elements of A which are integral over R forms a subring.

For, if α,β are integral over R, then the subalgebra $R[\alpha,\beta]$ of A these elements generate is a finite R-module.

It is faithful as an $R[u]$ -module, since it contains this ring, where u is any polynomial in α,β with coefficients in R. Thus u is integral by (3(iii)).

Suppose now that R is an integral domain, and let K be its field of fractions. It may happen that K contains elements integral over R, but not in R:

Example 8: Let $R = k[x,y]/(y^2-x^3)$. Then the element $t = y/x$ satisfies the monic equation $t^2 - x = 0$, but $t \notin R$.

Similarly, let $R = \mathbb{Z}[x]/(x^2 - 8)$. The element $x/2 = t$ satisfies the equation $t^2 - 2 = 0$, but is not in the ring.

Definition 9: Let R be an integral domain with field of fractions K. The set $\bar{R}$ of elements of K which are integral over R is called the integral closure of R in K. It is a ring because of (7). R is said to be integrally closed, or normal, if $R = \bar{R}$.

In the above example, the integral closure of R is actually $k[t]$ (resp. $\mathbb{Z}[t]/(t^2-2)$).

Proposition 10: Let R be an integral domain. Then if R is integrally closed, so is $S^{-1}R$ for any $S \in R-\{0\}$. Conversely, if for each prime p of R the local ring R_p is integrally closed, so is R.

proof: If R is integrally closed, let α be an element of the field of fractions K which is integral over $S^{-1}R$, say

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_o = 0 , \quad a_i \in S^{-1}R .$$

Write (2.A.3) $a_i = s^{-1}b_i$ (one denominator s for all i). Then $\beta = \alpha s$ is integral over R since it satisfies the equation

$$\beta^n + b_{n-1}\beta^{n-1} + \ldots + s^{n-2}b_1\beta + s^{n-1}b_o = 0$$

with coefficients in R. Thus β is in R, whence $\alpha = s^{-1}\beta$ is in $S^{-1}R$.

Now drop the assumption that R is integrally Let $\overline{R}$ be its integral closure, which is an R-module, and we have an inclusion map $R \subset \overline{R}$. By (4.D.3) it is an isomorphism iff the associated map of sheaves $\tilde{R} \longrightarrow \tilde{\overline{R}}$ is one. This is a question of their stalks. But if the stalk R_p is integrally closed, then it must be isomorphic to $\overline{R}_p$, since this latter is obviously an integral extension. This proves the second assertion.

C. Discrete valuation rings.

Let R be an integral domain with maximal ideal $\mathfrak{m} \neq 0$, and suppose that $\mathfrak{m}$, (0) are the only two points of

Spec R . Thus R is a local ring, and Spec R has one closed point and one "general point". An example is $R = k[[t]]$ (1.E.4). Suppose also that the ideal is finitely generated, say $\mathfrak{m} = (m_1, \ldots, m_n)$.

If $\mathfrak{a}$ is any proper ideal of R (i.e., one different from (0), R), its radical rad $\mathfrak{a}$ (1.D) has no choice but to be $\mathfrak{m}$. Thus for each i ,

$$m_i^s \in \mathfrak{a}$$

for some integer s . Because there are only finitely many m_i's , it follows that any monomial in the m_i of sufficiently large degree is in $\mathfrak{a}$, and so

(1) $\mathfrak{m}^N \subset \mathfrak{a}$ for sufficiently large N .

If we apply this fact to the ideal (x) generated by a non-zero element $x \in \mathfrak{m}$, we find

(2) $\mathfrak{m}^N \subset (x)$ for sufficiently large N .

Proposition 3: Under the above hypotheses, the intersection of the powers $\mathfrak{m}^n$ of the maximal ideals is (0) :

$$\bigcap_n \mathfrak{m}^n = (0) .$$

Remark: This is actually true for any noetherian local ring. It is an important theorem of Krull. One can show that in our situation, R is in fact noetherian.

proof: Suppose $x \neq 0$ is in every $\mathfrak{M}^n$. Then it follows from (2) that $\mathfrak{M}^N \subset (x) \subset \mathfrak{M}^N$, i.e.,

$$(x) = \mathfrak{M}^N \qquad \text{if } N \text{ is large.}$$

The same is true if x is replaced by the element x^2. Thus x is a multiple of x^2:

$$x = r\,x^2 \qquad\qquad r \in R\,.$$

Cancelling x,

$$1 = rx$$

i.e., x is a unit, a contradiction.

Theorem 5: Let R be an integrally closed (B.9) domain in which there is only one prime ideal $\mathfrak{M} \neq (0)$, and suppose $\mathfrak{M}$ finitely denerated. Then $\mathfrak{M}$ is generated by a single element.

This is not a trivial fact. It is the key result of "classical ideal theory". The assumption that $\mathfrak{M}$ be finitely generated is essential.

proof: Let K be the field of fractions of R, and let $z = y/x$ be an element of K not in R. Such an element exists since $\mathfrak{M} \neq (0)$. We have $x \in \mathfrak{M}$. By (2), any element of $\mathfrak{M}^N$ is divisible by x if N is sufficiently large, i.e., any monomial w in a set $\{m_i\}$ of generators of $\mathfrak{M}$ of sufficiently large degree is divisible by x, and so $wz \in R$ for such a monomial. Now if we replace z by mz for a cautiously chosen monomial m in $\{m_i\}$, we can get into the situation where

$$(6) \qquad m_i z \in R \qquad i = 1,\ldots,n$$

but $z \notin R$, i.e.,

$$\mathfrak{M} z \subset R ,$$

where $\mathfrak{M} z = \{mz \mid m \subset \mathfrak{M}\}$ Now it is immediately seen that $\mathfrak{M} z$ is an ideal of R.

<u>case 1:</u> $\mathfrak{M} z = R$. Then $mz = 1$ for some $m \in \mathfrak{M}$, i.e., $z = 1/m$. Because of (6), m divides each m_i and hence $\mathfrak{M}$ is generated by the single element m.

<u>case 2:</u> $\mathfrak{M} z \subseteq \mathfrak{M}$. Let R' be the ring $R[z]$. The assumption implies that $\mathfrak{M}$ is closed under multiplication by all powers of z, hence by all elements of R', i.e., $\mathfrak{M}$ is an R'-module. It is of finite type as an R-module and faithful as R'-module (easy to see). Therefore R' is integral over R by (B.3(iii)). This is a contradiction, since R was assumed integrally closed.

<u>Definition 7:</u> A ring R satisfying the hypotheses of (5) is called a <u>discrete valuation ring</u>.

Thus a discrete valuation ring is a local integral domain, and it has the following properties (by 5 and 3):

(8) (i) The maximal ideal $\mathfrak{M}$ of R is generated by one element x.

(ii) $\bigcap_n \mathfrak{M}^n = (0)$.

Note that by (i) any non-unit $a \in R$ is divisible by some power of x. By (ii), a is not divisible by arbitrarily large powers of x, unless $a = 0$. Hence we may write any non-zero element $a \in R$ in the form

$$a = ux^e \tag{9}$$

for some unit $u \in R$ and some integer $e \geq 0$.

If a is any non-zero element of the field of fractions K of R, then $a = r/s$ for some $r,s \in R$. Using the fact that r,s can be written in the form (9), one finds that also

$$a = u\,x^e \tag{10}$$

for some unit $u \in R$ and some integer e, which may now however be negative.

It is easily seen that the exponent e is uniquely determined by a. The unit u is also uniquely determined, once the generator x of $\mathfrak{M}$ is chosen. e is called the <u>order of zero</u> of a (or, $-e$ is called the <u>order of pole</u> of a). The "valuation" of the discrete valuation ring is the rule assigning to each $a \in K$ the exponent e. There is an obvious exact sequence

$$(11) \qquad 0 \longrightarrow R^* \longrightarrow K^* \longrightarrow \mathbb{Z} \longrightarrow 0$$

where R^* is the groups of units of R, K^* is the multiplicative groups of non-zero elements of K, and the additive group of integers $\mathbb{Z}$ represents the order of zero of the elements of K^*.

<u>Corollary 12:</u> The only ideals of R other than (0) are the powers $\mathfrak{m}^n = (x^n)$ of $\mathfrak{m}$.

For, any non-zero ideal $\mathfrak{a}$ contains a power of x because of (9), and the smallest such power clearly generates $\mathfrak{a}$.

Since this discussion was based only on properties 8,(i),(ii), we see also that

<u>Corollary 13:</u> Any local integral domain having properties (8)(i),(ii) is a discrete valuation ring.

For, the only prime ideals are (x), (0), by (12). We need furthermore to check that such a ring is integrally closed. This is clear from (10): If we write an integral dependence relation for an element $a \in K$ over R in the form

$$a^n + b = 0$$

where b is a polynomial in a of lower degree than n, we obtain from (10)

$$u^n x^{en} + v\, x^f \;=\; 0$$

where $b = v\, x^f$. Hence $en = f$. But since b has lower degree in a , this is not possible unless $e \geqq 0$.

D. Dedekind domains.

Definition 1: A noetherian integral domain R is called a dedekind domain if it satisfies one of the following equivalent conditions:

(i) for every prime ideal $p \neq (0)$, the local ring R_p is a discrete valuation ring.

(ii) R is integrally closed, and every prime ideal $p \neq (0)$ is maximal.

Examples: $\mathbb{Z}$ is a dedekind domain. A discrete valuation ring is a dedekind domain.

Let us verify the equivalence of (i) and (ii): If (ii) holds, then it is clear that the local rings R_p have only two prime ideals. By (B.10), they are integrally closed, hence by (C.5) are discrete valuation rings. Conversely, if (i) holds, then every prime $p \neq (0)$ is maximal. For, if $(0) \subsetneqq p \subsetneqq q$, then the ring R_q must contain three prime ideals (2.C), contradicting the assumption that it is a discrete valuation ring. Again, R is integrally closed by (B.10).

Notice that because of (i) and (A.9), $S^{-1}R$ is a dedekind domain if R is.

Let $\mathfrak{a} \neq (0)$ be an ideal of R. Then $\mathfrak{a}$ is contained in only finitely many prime ideals of R. For, suppose the contrary. Let $\mathfrak{a}$ be a maximal element among the ideals contained in infinitely many prime ideals, and let $\mathfrak{P}$ be the set of prime ideals containing $\mathfrak{a}$. I claim $\mathfrak{a}$ is prime, which will contradict (1.(ii)), since $(0) \subsetneqq \mathfrak{a} \subsetneqq p$ for some $p \in \mathfrak{P}$: If $ab \in \mathfrak{a}$ then $ab \in p$ for each $p \in \mathfrak{P}$. Since $\mathfrak{P}$ is infinite, either a or b is in infinitely many members of $\mathfrak{P}$, say a is. Then the ideal $\mathfrak{a} + (a)$ is in infinitely many primes, hence is equal to $\mathfrak{a}$ since $\mathfrak{a}$ was maximal. Thus a is in $\mathfrak{a}$ which is therefore a prime ideal. This completes the proof of our assertion.

For each prime $p \neq (0)$ of R, we can express a non-zero element a of R in the form (C.9) in the local ring R_p. More generally, if a is any non-zero element of the field of fractions K of R, we can express a in the form (C.10) in R_p. The exponent e is called the <u>order of zero of</u> a <u>at</u> p (or, $-e$ is called the <u>order of pole of</u> a <u>at</u> p).

Because an element $a \neq 0$ of R is in only finitely many prime ideals (by the above reasoning, with $\mathfrak{a} = (a)$), it follows that a has only finitely many zeros. Since any $a \in K$ is a fraction $a = r/s$ of such elements, it is also true that a non-zero element $a \in K$ has only finitely many zeros and poles.

The main theorem of classical ideal theory is

Theorem 2: (unique factorization of ideals) Let R be a dedekind domain. Any non-zero ideal $\mathfrak{a}$ of R is (uniquely) expressible as a finite product of prime ideals

$$\mathfrak{a} = \prod_i p_i^{e_i} = p_1^{e_1} \cdots p_n^{e_n} . \quad (e_i > 0) .$$

proof: The term on the right is meant as the usual product of ideals. Now $\mathfrak{a}$ is contained in only finitely many prime ideals $p_1, \ldots, p_n$ $(p_i \neq (0))$. For each i, let e_i be the minimal order of zero of a at p_i among all elements $a \in \mathfrak{a}$. Then

$$\mathfrak{a} \subset p_i^{e_i} .$$

Hence we have the inclusions

$$\mathfrak{a} \subset \bigcap_i p_i^{e_i} \supset \prod_i p_i^{e_i}$$

among the three ideals, and I claim these inclusions are equalities:

This is of course a question which can be expressed in terms of exact sequences (an inclusion $A \subset B$ is an equality iff. the sequence $A \to B \to 0$ is exact).
Hence we may apply the theory of (4.D). Proposition 3 of (4.D) says that it suffices to show the inclusion maps among the <u>associated</u> <u>sheaves</u> are equalities, and this is a question of their stalks (4.B.5(ii) and 4.C). By (4.B.6), the stalk of $\tilde{M}$ at a prime ideal q is the localized module M_q, and when you localize an ideal $I \subset R$, you get the ideal I_q of R_q generated by the image of I. Thus we have to show that for each q the ideals in R_q generated by the three ideals in question are equal. This is really easy from (C.11), and we leave the verification to the reader.

<u>Corollary 3:</u> Every non-zero ideal $\mathfrak{a}$ of R is a locally free R-module of rank 1.

Apply (5.G.1) to reduce to the case of a discrete valuation ring (or the field K). For such a ring, it is clear from (C.12), since a non-zero principal ideal in an integral domain is free of rank 1. In fact, it is clear that an ideal $\mathfrak{a}$ of a ring R is a free R-module of rank 1 iff. $\mathfrak{a}$ can be generated by one element a which is not a zero divisor in R.

E. Fractional ideals.

Definition 1: Let R be an integral domain with field of fractions K. A fractional ideal $\mathfrak{a}$ of R is an R-submodule of K which is of finite type as an R-module, i.e., an additive subgroup of K closed under multiplication by elements of R and finitely generated.

In particular, an ideal of R is a fractional ideal. In general however, a fractional ideal will not be a subset of R. Any element $a \in K$ generates a fractional ideal $(a) = \{ra \mid r \in R\}$.

Given two fractional ideals $\mathfrak{a}, \mathfrak{b}$ we can define their product

$$\mathfrak{a} \cdot \mathfrak{b} = \{x \in K \mid x = \sum a_i b_i \text{ for some } a_i \in \mathfrak{a}, b \in \mathfrak{b}\} .$$

It is again a fractional ideal.

Let R be a dedekind domain, and $p \neq (0)$ a prime ideal. Define a fractional ideal

$$p^{-1} = \{a \in K \mid ax \in R, \text{ all } x \in p\} .$$

This is clearly an R-module. To show it is of finite type is a local problem (5.B.7). Therefore we may assume p generated by one element x in R (D.3). Then $a \in p^{-1}$ iff. $a = b/x$ for some $b \in R$, hence p^{-1} is generated by $1/x$.

It is clear how to define fractional ideals p^{-n} and hence, setting $p^0 = R$, all powers of p are defined. They satisfy the usual rules of multiplication, which are trivially verified since the problem is always local and is obvious when $p = (x)$ is generated by one element.

More generally, we have products of powers

$$\prod_i p_i^{e_i} \qquad e_i \text{ integers.}$$

An element $a \neq 0$ of K is in $\prod p_i^{e_i}$ iff the order of zero of a at p_i is at least e_i (or order of pole is at least $-e_i$), and if the order of zero at q is ≥ 0 for all other non-zero primes q, i.e., $a \in R_q$ for all other q. This assertion is verified locally as for (D,2).

Theorem 2: Every non-zero fractional ideal $\mathfrak{a}$ is uniquely expressible as a product of prime powers

$$\mathfrak{a} = \prod_i p_i^{e_i} = p_1^{e_1} \cdots p_n^{e_n}, \qquad e_i \neq 0 .$$

proof: Let $a_1, \ldots, a_m \in K$ be generators for $\mathfrak{a}$ and for each non-zero prime p of R define an integer

$$e = \min_\nu \{\text{order of zero of } a_\nu \text{ at } p\} .$$

Since each a_i has only finitely many zeros and poles, $e = 0$ for all but a finite number of p, say $p_1, \ldots, p_n$.

Then I claim

$$\mathfrak{a} = \prod_i p_i^{e_i}$$

and the verification is the same as that of (D.2).

<u>Corollary 3:</u> The non-zero fractional ideals form a group D under multiplication, and the group is isomorphic to the direct sum of copies of the add. group $\mathbb{Z}$ of integers, one copy for each non-zero prime $p \in \operatorname{Spec} R$:

$$D \approx \bigoplus_{p \in \operatorname{Spec} R} \mathbb{Z} \qquad (p \neq (0)) .$$

The isomorphism is of course the one which associates to $\mathfrak{a}$ the exponent e_i in the p_i-th copy of $\mathbb{Z}$, in the above situation. Sometimes an element D is written multiplicatively, as above, in (2), and sometimes additively as $\Sigma\, e_i p_i$ = a linear combination of primes with integer coefficients. D is also sometimes called the group of <u>divisors</u> (whence the D).

F. The ideal class group.

As in (D.3), we see that any non-zero fractional ideal $\mathfrak{a}$ of a dedekind domain R is a locally free R-module of rank 1. Indeed, this is reduced by (5.B.7) to a statement about the fractional ideal of a local ring R_p, which is a discrete valuation ring (or the field K), and it is clear from (C.10) that every non-zero fractional ideal of a discrete valuation ring is principal, and generated by some power x^e (possibly negative) of the generator for the maximal ideal, hence is free of rank 1.

The ideal $\mathfrak{a}$ is a free module iff. it is principal, i.e., generated by one element $a \in K$. Now, we can associate with an element $a \neq 0$ of K the fractional ideal (a) it generates (cf. E.1) and hence get a map

(1) $$K^* \longrightarrow D$$

where $K^* = K - \{0\}$ and D is the group of non-zero fractional ideals (cf. E.3). If we write $(a) = \prod p_i^{e_i}$ by (E.2), then it is clear from the discussion of (E) that e_i is just the order of zero of a at p_i. Therefore, (1) is a homomorphism of the multiplicative group K^* to D. Its kernel is the group of elements $a \in K^*$ which have no zeros or poles, i.e., the group of units R^* of R (why is this so?). Thus we have an exact sequence

(2) $$0 \longrightarrow R^* \longrightarrow K^* \longrightarrow D$$

(compare with (C.11)). The image of K^* in D is the subgroup of principal ideals, i.e., those which are free modules. The cokernel of $K^* \longrightarrow D$ is called the ideal class group:

(3) (ideal class group) = (fract. ideals)/(principal ones) .

Proposition 4: The ideal class group is naturally isomorphic to the group $H^1(X,\tilde{R}^*)$ of all locally free rank 1 modules (3.E.6), in particular, every such module is isomorphic to a fractional ideal. More precisely, (2) can be completed to an exact sequence

$$0 \longrightarrow R^* \longrightarrow K^* \longrightarrow D \longrightarrow H^1(X,\tilde{R}^*) \longrightarrow 0 .$$

proof: The exact sequence is just an exact cohomology sequence obtained from the following exact sequence of sheaves: Let $\tilde{R}^*$ be defined as in (3.D.6). Define $\tilde{K}^*$ to be the "constant sheaf" whose value on any non-empty $U \subset X$ is $\tilde{K}^*(U) = K^*$. This is clearly a sheaf. Finally, define a sheaf $\tilde{D}$ by

$$D(U) = \bigoplus_{p \in U} \mathbb{Z}$$

where p runs over non-zero primes contained in U . When $V \subset U$ one gets the homomorphism $\tilde{D}(U) \longrightarrow \tilde{D}(V)$ by dropping the summands $\mathbb{Z}$ corresponding to those primes p in U

but not in V. I leave to you the easy verification that this is a sheaf. Now we have a natural inclusion $\tilde{R}^*(U) \subset \tilde{K}^*(U) = K^*$ for each $U \neq \emptyset$, hence a map $\tilde{R}^* \longrightarrow \tilde{K}^*$. Also, for any $a \in \tilde{K}^*(U) = K^*$, we can associate to a its orders of zero at those primes p in U, and thus get a map $\tilde{K}^*(U) \longrightarrow \tilde{D}(U)$. I claim that the sequence

$$(5) \qquad 0 \longrightarrow \tilde{R}^* \longrightarrow \tilde{K}^* \longrightarrow \tilde{D} \longrightarrow 0$$

is exact. To check this, note that the stalks at $p \in X$ $(p \neq (0))$ are

$$(\tilde{R}^*)_p = R^*_p \ ; \quad (\tilde{K}^*)_p = K \ ; \quad (\tilde{D})_p = \mathbb{Z}$$

where $\mathbb{Z}$ represents that copy corresponding to the prime p in the various neighborhoods U of p. Thus the exactness is just (C.11). For the stalk at the point (0), we get

$$(\tilde{R}^*)_{(0)} = K^* = (\tilde{K}^*)_{(0)} \ ; \quad (\tilde{D})_{(0)} = 0 \ .$$

Having the exact sequence (5), the proposition will follow from the exact cohomology sequence (4.C.3) once we verify that

$$(6) \qquad H^1(X,\tilde{K}^*) = 0 \ ,$$

which is a consequence of the fact that $\tilde{K}^*$ is a constant sheaf. It is an easy and dull verification with cocycles, which we omit.

STRUCTURE THEORY FOR MODULES OVER NOETHERIAN RINGS

A. Support of a module.

Let R be a ring and $X = \operatorname{Spec} R$.

Definition 1: Let M be an R -module. The support of M , written $\operatorname{supp} M$, is the set of points $p \in X$ such that the localized module $M_p \neq 0$, i.e., such that the stalk of the sheaf $\tilde{M}$ at p is not zero.

Thus the support answers the crudest possible question about $\tilde{M}$. It is not without interest, however. One often uses locutions of the type "M is zero outside of Y" if Y is a subset of X containing $\operatorname{supp} M$. Note that $M = 0$ iff. $\operatorname{supp} M = \emptyset$. Also, the support of a localized module $S^{-1}M$ is obviously $(\operatorname{supp} M) \cap (\operatorname{Spec} S^{-1}R)$ (cf. 2.B).

Suppose that M is generated by one element m , and let $\mathfrak{a} = (\text{annihilator of } M) = \{ r \in R \mid rm = 0 \}$. Then $M \quad R/\mathfrak{a}$ as an R -module (via the map sending $r \rightsquigarrow rm$), and I claim

(2) $$\operatorname{supp}(R/\mathfrak{a}) = V(\mathfrak{a}) ,$$

(in particular, $\operatorname{supp} R = \operatorname{Spec} R$). In fact, $V(\mathfrak{a})$ identifies naturally with the spectrum of the ring $R/\mathfrak{a}$. (1.C.13), and one sees immediately that the stalk $(R/\mathfrak{a})_p$ is just the local ring of $R/\mathfrak{a}$ at the prime $(p/\mathfrak{a}\,p)$ of $R/\mathfrak{a}$ if $\mathfrak{a} \subset p$, and is zero otherwise.

One can also look at it this way: Suppose $\{m_i\}$ generates M. Then the images of the m_i in M_p generate this R_p-module. This is clear. Thus $M_p \neq 0$ iff some m_i is not zero at p. This last is true iff (3.A.4) $sm_i \neq 0$ for all $s \in R-p$, i.e., iff $\operatorname{ann}(m_i) \subset p$. Thus

$$\text{(3)} \qquad \operatorname{supp} M = \bigcup_i V(\mathfrak{a}_i) ,$$

where $\mathfrak{a}_i$ = (annihilator of m_i).

Corollary 4: If M is of finite type, then $\operatorname{supp} M$ is a closed subset of $\operatorname{Spec} R$.

Proposition 5: (i) If $\{N_i\} \subset M$ is a family of submodules and $\Sigma N_i = M$, then $\operatorname{supp} M = \bigcup \operatorname{supp} N_i$.

(ii) If $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is exact, then

$$(\operatorname{supp} B) = (\operatorname{supp} A) \cup (\operatorname{supp} C) .$$

Both assertions are clear.

Example 6: Let A be a finite abelian group, i.e., a finite $\mathbb{Z}$-module. The support of A is the set of primes p which divide the order of A. You should verify this. Supp A is therefore a finite set of closed points of $\operatorname{Spec} \mathbb{Z}$.

The first structure theorem for finite abelian groups asserts that an abelian group is isomorphic to a direct product of its p-sylow subgroups, each having support at only one point. There is an analogous result for modules over an arbitrary ring R, but because the geometry of $\operatorname{Spec} R$ is usually more complicated that that of $\operatorname{Spec} \mathbb{Z}$, the result is less powerful. It is closely related to (1.E.1).

Theorem 7: Let M be an R-module. Suppose $C_1, \ldots, C_n \subset X = \operatorname{Spec} R$ are disjoint closed subsets and that

$$\operatorname{supp} M \subset \bigcup_i C_i .$$

Then M is canonically isomorphic to a product

$$M = \prod_i M_i$$

of modules M_i with $\operatorname{supp} M_i \subset C_i$.

proof: Clearly, it suffices to treat the case of two closed subsets C_1, C_2. Construct the sheaf $\mathcal{M}_1$ associated to the module M_1, first locally, as follows: Let $p \in X$ be any point.

case 1: $p \notin C_1$. Then $p \in X - C_1$. Choose an open neighborhood of p of the form X_s $(s \in R)$ contained in $X - C_1$. This exists by (2.B.5). Let the sheaf $\mathcal{M}_1 | X_s$ be the zero sheaf.

<u>Case 2:</u> $p \in C_1$. Then $p \in X-C_2$. Choose an open neighborhood of p of the form X_s contained in $X-C_2$, and let $\mathcal{M}_1|X_s$ be the sheaf $\tilde{M}_s$ associated to the module M_s . Thus $\mathcal{M}_1|X_s = \tilde{M}|X_s$ in this case.

I claim that if p,q are any two points, and the chosen neighborhoods are X_s, X_t resp., then the above definitions give canonically isomorphic sheaves when restricted to $X_{st} = X_s \cap X_t$: If both $p,q \notin C_1$, then the sheaves defined are both zero. If both $p,q \in C_1$, they are $\tilde{M}|X_{st} = \tilde{M}_{st}$. Finally, if say $p \notin C_1$ and $q \in C_1$, then the first sheaf is zero, and so we need to show the second is zero too. Note that by construction we have $X_{st} \subset X-(C_1 \cup C_2)$. Thus we are reduced to the following

<u>Lemma 8:</u> If X_u $(u \in R)$ is an affine open which does not meet $C_1 \cup C_2$, then $M_u = 0$.

But $(\operatorname{supp} M_u) = (\operatorname{supp} M) \cap X_u = \emptyset$, so $M_u = 0$ as desired.

It is clear that the above isomorphisms satisfy the compatibility conditions (3.C) so as to give gluing data for a sheaf $\mathcal{M}_1$. The sheaf so constructed is locally quasi-coherent, hence quasi-coherent (3.B.6), and so $\mathcal{M}_1 = \tilde{M}_1$ where $M_1 = \mathcal{M}_1(X)$. The module M_2 is obtained similarly.

To give a map $\tilde{M} \longrightarrow \tilde{M}_i$, it suffices to do so locally (subject to the usual compatibility). Locally, a map is evidently given by the above construction. Hence we obtain a map

$$M \longrightarrow M_1 \times M_2 .$$

To show that it is an isomorphism, is again a local problem, and is also clear from the construction - locally, one of $\tilde{M}_i$ will be zero, and the other will be isomorphic to $\tilde{M}$.

B. Associated primes.

If one wants to get more detailed information about R -modules M , it is reasonable to regard modules of the form R/p (p a prime ideal) as known". They are just free rank one modules, but "over a different ring", which is in fact an integral domain. A good question to ask about a module M is for which p the module contains a sub-module isomorphic to R/p . (It is not very informative to know that M contains a quotient module isomorphic to R/p.)

<u>Definition 1:</u> A prime $p \in \operatorname{Spec} R$ is an <u>associated prime</u> of M if M contains a submodule isomorphic to R/p .

This is clearly the case iff there is an element $m \in M$ whose annihilator is the ideal p (m corresponds to the residue of 1 in the submodule R/p .)

The set of all associated primes is denoted by

$$\text{ass } M .$$

Here is a result which shows that the notion is a good one:

<u>Proposition 2:</u> Let R be a noetherian ring. If a module M is not zero, then $\text{ass } M \neq \emptyset$.

proof: Let S be the set of ideals different from R which are annihilators of elements of M , and let $\mathfrak{a}$ be a maximal element of S (6.A.3). I claim $\mathfrak{a}$ is prime, which will prove the proposition. Say $\mathfrak{a} =$ (annihilator of m) . If $ab \in \mathfrak{a}$ but $b \in \mathfrak{a}$, then $bm \neq 0$. Clearly any element of $\mathfrak{a}$ annihilates bm . Hence (annihilator of bm) $\supset \mathfrak{a}$, thus is equal to $\mathfrak{a}$ because was a maximal element of S and 1 (annihilator of bm). But a annihilates bm . Therefore $a \in \mathfrak{a}$, which completes the proof.

<u>Elementary properties:</u>

(3) The annihilator of any non-zero element of R/p is p , whence any non-zero submodule $M \subset R/p$ has p as its only associated prime.

(4) If $N \subset M$, then $(\text{ass } N) \subset (\text{ass } M)$.

(5) If $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is exact, then

$$(\text{ass } B) \subset (\text{ass } A) \cup (\text{ass } C)$$

(equality does not usually hold). For, let $M \subset B$ be a submodule isomorphic to R/p. If $M \cap A = 0$, then M is isomorphic to its image in $C = B/A$. If $M \cap A \neq 0$, then A contains a non-zero submodule of M, which has p as associated prime by (3).

(6) $$\text{ass}(A \oplus C) = (\text{ass } A) \cup (\text{ass } C) .$$

Apply (5) and (6).

The following result may be considered the second structure theorem for modules over noetherian rings:

Proposition 7: Let R be a noetherian ring and M an R-module of finite type. There exists a chain of submodules

$$0=M_0 \subset M_1 \subset \ldots \subset M_n=M$$

such that for each i, the module M_i/M_{i-1} is isomorphic to R/p_i for a suitable prime p_i of R.

This proposition is reminiscent of the Jordan-Hölder theorem, for groups, but unfortunately there is no possibility of asserting uniqueness of the factors M_i/M_{i-1}. For instance, the abelian group $\mathbb{Z}$ has the decomposition given by the submodules $0 \subset \mathbb{Z}$, which yields one factor $\mathbb{Z}$, and also has the decomposition given by the submodules $0 \subset qp^2\mathbb{Z} \subset qp\,\mathbb{Z} \subset p\,\mathbb{Z} \subset \mathbb{Z}$, which has factors isomorphic respectively to $\mathbb{Z}$, $\mathbb{Z}/p$, $\mathbb{Z}/q$, $\mathbb{Z}/p$.

The proof is a standard noetherian argument: Consider the family S of submodules of M for which the theorem is true, and let N be a maximal one (6.A.3), so that we have a chain of submodules

$$0=N_0 \subset N_1 \subset \ldots \subset N_r=N \text{ , etc...}$$

If $N \neq M$, then M/N has an associated prime by (2), hence a submodule $\overline{N}'$ isomorphic to R/p for some p. This submodule corresponds to a submodule N' of M containing N, and $N'/N \approx R/p$. Hence the sequence of submodules

$$0=N_0 \subset N_1 \subset \ldots \subset N_r \subset N'$$

shows that the theorem is true for N', which contradicts the maximality of N. Thus $N = M$.

<u>Corollary 8:</u> If R is noetherian and M is of finite type, then $\operatorname{ass} M$ is a finite set of primes.

This follows from (6) by induction on the length of the chain $M_0 \subset \ldots \subset M_n$. For, we have the exact sequence

$$0 \longrightarrow M_{n-1} \longrightarrow M_n \longrightarrow R/p_n \longrightarrow 0 ;$$

and $\operatorname{ass}(R/p_n) = \{p_n\}$.

C. Relation with the support.

We suppose throughout this section that R is a noetherian ring.

By (A.2) and (A.5(ii)), it is clear that every associated prime of M is in the support of M (this doesn't depend on the noetherian hypothesis):

$$\text{(1)} \qquad \text{ass } M \subset \text{supp} M .$$

However, they are not usually the same. If M is of finite type, then supp M is closed. Hence (1.F) if $p \in$ supp M, and q is any prime containing p, also $q \in$ supp M. Therefore supp M will in general have to be infinite, while by (B.8), ass M is finite. However, the closure of ass M is all of supp M :

Proposition 2: The minimal primes of ass M and of supp M are the same.

By a minimal prime of a subset $S \subset X = \text{Spec } R$, we mean of course a prime which contains no other primes of S. Recall (1.F) that the closure of a prime p in X is the irreducible closed set consisting of all primes q which contain p. Thus if S is a closed set, then the minimal primes of S are the generic points of the irreducible components of S (which are finite in number by

(6.A.10); in particular, a non-empty closed S contains some minimal primes:

$$(\text{minimal primes}) \longleftrightarrow (\text{largest closure}) .$$

Hence proposition 2 is just the assertion that the closure of ass M is supp M, when M is of finite type.

Proof of (2): It is a slight refinement of the proof of (B.2): Let q be in supp M, so that $M_q \neq 0$. What we need to do is to find an associated prime p which is contained in q. Let S be the set of annihilators $\mathfrak{a}$ of elements m such that $\mathfrak{a} \subset q$. This is the same as saying that $m \neq 0$ in M_q, by (3.A.4). Since $M_q \neq 0$, the set is non-empty. Let $\mathfrak{a} =$ (annih. of m) be maximal in S. It suffices to show that $\mathfrak{a}$ is prime:

Say $ab \in \mathfrak{a}$. If $bm \neq 0$ in M_q, the (annih. of bm) contains $\mathfrak{a}$ and a, hence is equal to $\mathfrak{a}$ since $\mathfrak{a}$ was maximal. Thus $a \in \mathfrak{a}$. If on the other hand $bm = 0$ in M_q, then (3.A.4) there is an element $c \notin q$ such that $cbm = 0$ in M. But c is a unit in M_q, hence $cm \neq 0$ in M_q. Since (annih. of cm) contains $\mathfrak{a}$ and b, and $\mathfrak{a}$ was maximal, $b \in \mathfrak{a}$. This completes the proof.

Proposition 3: Let M be an R-module.

(i) An element $r \in R$ is in no associated prime iff. r annihilates no non-zero element $m \in M$.

(ii) An element $r \in R$ is in every associated prime iff it is in every prime of $\operatorname{supp} M$ iff every $m \in M$ is annihilated by some power of r.

Proof: (i). Clearly, r cannot be in an associated prime of M unless $rm = 0$ for some $m \neq 0$. Conversely, if $rm = 0$, then r annihilates every element of the submodule Rm of M generated by m, hence is in any associated prime of Rm.

(ii) It follows from (2) that r is in every associated prime iff. r is in every prime of $\operatorname{supp} M$. Moreover, if a prime $p =$ (annih. of m), and if some power of r annihilates m, then $r \in p$. Hence r is in every associated prime if every element of M is annihilated by a power of r. Conversely, suppose r is in every prime of $\operatorname{supp} M$, and let $m \in M$. We want to show that $r^n m = 0$ for some n, and by (A.5(ii)), we may replace M by the submodule Rm generated by m, which is isomorphic to $R/\mathfrak{a}$. ($\mathfrak{a}$ = (annih. of m)). Then R operates through the quotient ring $R/\mathfrak{a}$, and one reduces easily, using (1.C.13), to the case that $R = R/\mathfrak{a}$, i.e., that M is the ring R itself, viewed as an R-module. Now $\operatorname{supp} R = \operatorname{Spec} R$ (A.2). Thus the assertion is that if r is in every prime ideal then $r^n \cdot 1 = 0$ for some n, i.e., r is nilpotent. This is (1.D.2).

Corollary 4: An R-module M has p as its only associated prime iff.

(i) For $r \notin p$, no non-zero $m \in M$ is annihilated by r, and

(ii) For $r \in p$, every $m \in M$ is annihilated by some power of r.

D. Primary decomposition.

The ring R is assumed noetherian throughout.

Definition 1: A module M is p-coprimary (p a prime of R) iff

$$\text{ass } M = \{p\} .$$

A submodule $Q \subset M$ is p-primary iff M/Q is p-coprimary.

When dealing with p-coprimary modules, we can use the result (C.4). Note that by (B.3)

(2) a non-zero submodule of a coprimary module is coprimary.

Remark: In this context, the notion of coprimary module seems the more natural one. Historically, the concept of primary ideal (= primary submodule of R) was first developed. An ideal $I \subset R$ is p-primary if R/I is p-coprimary. This means that

(3) An ideal I is p-primary iff.

(i) $rx \in I$ and $r \notin p \Rightarrow x \in I$, and

(ii) the radical (rad I) of I is p.

This is just a restatement of (C.4), applied to the module R/I.

An ideal I is p-primary for some prime ideal p iff

(4) $ab \in I$ and $a \notin I \Rightarrow b^n \in I$ for some n.

In fact, if (4) holds, then (rad I) $= p$ is a prime ideal since

$$ab \in p \Rightarrow a^m b^m \in I \text{ for some } m,$$

hence by (4), $a^m \in I$ or $b^{mn} \in I$ for some n, i.e., a or b is in p. Moreover, (4) is clearly equivalent to (3)(i). Each asserts

$$ab \in I \Rightarrow a \in I \text{ or } b \in p.$$

Here is the main result on coprimary modules:

Theorem 5: A finitely generated module M is isomorphic to a submodule of a finite product of coprimary modules, i.e., there is an injective map

$$M \longrightarrow \prod_i N_i \qquad \text{with each } N_i \text{ coprimary}$$

<u>Example 7:</u> A finitely generated coprimary abelian group is either

(a) a torsion free abelian group ((0)-coprimary)

or

(b) a finite group of p-power order ((p)-coprimary) .

Thus any finitely generated abelian group A is isomorphic to a direct product of coprimary ones, and the structure theory continues, to classify these as direct sums of cyclic groups. For finite groups, (6) is just a weak version of (A.7).

It is not true, however, that a module is isomorphic to a direct sum of coprimary ones when the geometry of Spec R is more complicated. The simplest type of problem which arises is caused by an intersection of irreducible closed sets corresponding to two associated primes:

Let $R = k[x,y]$ (cf. 1.G.6), and $M = R/(xy)$. The support of M is the union of the two loci $V(x) \cup V(y)$ (the y and x axes). One has an injection

$$M \hookrightarrow (R/(x))\times(R/(y))$$

which is not surjective. The elements of M satisfy an extra condition at the point $(0,0)$ (cf. Ex. 1, No. 5).

<u>Variants:</u> Stated in terms of primary submodules of M , (6) reads

(8) Every finitely generated module M contains a finite set $Q_1,\dots,Q_n$ of primary submodules with

$$\bigcap_i Q_i = 0 \quad .$$

For, if (8) holds, put $N_i = M/Q_i$. Then $M \longrightarrow \prod N_i$ is injective because the intersection of the Q_i is zero. Conversely, if $M \longrightarrow \prod N_i$ is injective, let Q_i be the kernel of the map $M \longrightarrow N_i$. We may omit those factors N_i for which $Q_i = M$ (i.e., $M \longrightarrow N_i$ is the zero map). Then M/Q_i is a submodule of N_i, hence is coprimary (2).

Let R be a ring and I an ideal of R . Then (8) applied to R/I asserts

(9) Every proper ideal I of R is an intersection of finitely many primary ideals.

That is the classical assertion.

<u>proof of 6:</u> The argument is a particularly elegant example of the use of noetherian induction: For varying submodules, $M' \subset M$, we try to prove (6) for the quotient module M/M' . We will be interested in the case $M' = 0$. Let S be the set of submodules M' such that (5) is false for M/M' . We want to show S empty. Suppose not. Then there is a maximal element, M' . Thus (5) is false for M/M' but is true for M/N if N is larger than M' . We may replace

M by M/M' and M' by 0, i.e., we are reduced to the case that (5) is false for M, but true for M/N whenever $N \neq 0$. In the form of assertion (8), this says that there exists no finite set of primary submodules Q_i of M with intersection 0, but for any submodule $N \neq 0$, there exists a set with intersection N. To show the impossibility of this, it clearly suffices to find <u>any two non-zero submodules</u> A,B <u>of</u> M <u>such that</u> $A \cap B = 0$. Now M is not itself coprimary, or we are done. Hence M has at least two associated primes p, q. Let A,B be submodules isomorphic to R/p, R/q respectively. Then $A \cap B = 0$. For, if $m \neq 0$ is in $A \cap B$, then (annih. of m) $= p = q$ by (B.3), a contradiction. This completes the proof.

Notice how the proof makes use of the existence of <u>submodules</u> isomorphic to R/p to conclude the existence of certain quotient modules.

E. Questions of uniqueness.

We assume R noetherian and M of finite type.

Let $M \hookrightarrow \prod N_i$ be a submodule of a product of coprimary modules N_i $(i = 1,\ldots,n)$ as in (D.6), and let p_i be the prime ideal associated to N_i. We may be able to simplify the expression slightly: First of all, if $p_i = p_j$ for two indices, then $N_i \times N_j$ is again p_i-coprimary (B.6). Therefore we can shorten the product. Also, we can replace N_j by the image of the map $M \longrightarrow N_j$ if that is smaller, and we can eliminate any N_j if the image is zero.

For the primary submodules Q_i as in (D.8), this amounts to replacing Q_i, Q_j by $Q_i \cap Q_j$ if both are primary for the same p, and leaving out a Q_j if $\bigcap_{i \neq j} Q_i = 0$.

When this is done, the primary decomposition is said to be <u>reduced</u>.

<u>Proposition 1:</u> The set of primes $\{p_i\}$ associated to the members $\{Q_i\}$ of a reduced primary decomposition is ass M.

proof: It is clear from (B.4) that ass $M \subset \{p_i\}$, because $\{p_i\} = \mathrm{ass}(\prod M/Q_i)$ by (B.6). Conversely, to show p_1, say, is an associated prime, consider the submodule $N = \bigcap_{i>1} Q_i$. We have $N \neq 0$ since the decomposition is reduced. Clearly N is isomorphic to a non-zero submodule of M/Q_1, hence (B.3) ass $N = \{p_1\} \subset$ ass M.

Proposition 1 shows that the primes associated to a reduced primary decomposition are uniquely determined; it is unfortunately not true that the submodules Q_i (resp. the quotients M/Q_i) are unique:

Example 2: Let M be the abelian group $\mathbb{Z} \oplus \mathbb{Z}/2$. Put

$$Q_1' = (2\,\mathbb{Z})\oplus(0)\ ,\quad Q_2' = (0)\oplus\mathbb{Z}/2\ .$$

Then $Q_1' \cap Q_2' = 0$. But the natural choice is

$$Q_1 = \mathbb{Z} \oplus (0)\ ,\qquad Q_2 = (0) \oplus \mathbb{Z}/2\ .$$

However, the minimal primes of ass M correspond to uniquely determined primary submodules Q_i . It is only for the non-minimal ones that a problem may arise. Let C_i be the irreducible closed subset of $X = \operatorname{Spec} R$ corresponding to p_i , then for a prime p_i which is not minimal, C_i is contained in some other C_j . Such a C_i is called an embedded component of supp M , and it is these that give the trouble.

Proposition 3: Let p_1 be a minimal prime of ass M . Then the submodule Q_1 associated to p_1 in a reduced primary decomposition is uniquely determined.

proof: Since p_1 is a minimal prime, it contains no other p_i , hence $p_1 \not\supset \bigcap_{i>1} p_i$ (1.C.8). Thus there is an element a which is in p_i for $i > 1$ but not in p_1 ; put

$$K_n = \{m \in M \mid a^n m = 0\}\ .$$

Then K_n is an increasing sequence of submodules of M , which becomes constant for large n . Let K be this constant value. I claim $K = Q_1$. This will show that Q_1 is unique.

Now the map

$$Q_1 \longrightarrow \prod_{i>1} M/q_i$$

is injective, since

$$(Q_1 \cap Q_2) \cap \ldots \cap (Q_1 \cap Q_n) = 0 .$$

Therefore ass $Q_1 \subset \{p_2, \ldots, p_n\}$. Since a is in each of these primes, and Q_1 is finitely generated (6.A.1), some power a^n of a annihilates Q_1 (C.3(ii)). Consider the diagram

$$\begin{array}{ccccccccc}
 & & K' & & K & & K'' & & \\
 & & \cap & & \cap & & \cap & & \\
0 & \to & Q_1 & \longrightarrow & M & \longrightarrow & M/Q_1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & Q_1 & \longrightarrow & M & \longrightarrow & M/Q_1 & \longrightarrow & 0
\end{array}$$

where the vertical arrows are multiplication by a^n, (i.e., $x \rightsquigarrow a^n x$). Since $a \in p_1$, multiplication by a is injective in M/Q_1 (C.3(i)), whence the kernel K'' is zero. By assumption, the map $Q_1 \longrightarrow Q_1$ is zero, hence $K' = Q_1$. By left exactness of kernel, the sequence

$$0 \longrightarrow Q_1 \longrightarrow K \longrightarrow 0$$

is exact, which proves the assertion.

THEORY OF POLYNOMIAL RINGS

In this part, we study finitely generated rings R over a field k, i.e., ones which are generated as a k-algebra by finitely many elements, or, equivalently, are quotients of a polynomial ring in finitely many variables over k.

The notation $k[x_1,\ldots,x_n]$ will stand for an algebra which is generated by some elements $x_1,\ldots,x_n$ over k. We do not assume, unless we so state, that the x_i's are "independent", i.e., that the ring is the polynomial ring in variables $x_1,\ldots,x_n$. In general, it will be a quotient of the polynomial ring.

A. The Hilbert basis theorem.

It is

Theorem 1: A finitely generated (commutative) algebra A over a noetherian ring R is noetherian. In other words, if A is a quotient of a polynomial ring $R[x_1,\ldots,x_n]$ over R, and if R is noetherian, then A is, too.

Proof: By (6.A.7), a quotient of a noetherian ring is noetherian. Hence it suffices to treat the case of a polynomial ring. Since $R[x_1,\ldots,x_n] = R[x_1,\ldots,x_{n-1}][x_n]$, it suffices by induction to treat the case $n = 1$, i.e., $A = R[x]$.

Let I be an ideal of $R[x]$, and consider the leading coefficients of polynomials of I. (a_i is the leading coefficient of

$$f(x) = a_i x^i + \ldots + a_1 x + a_0 \qquad a_\nu \in R\ .)$$

Let $\mathfrak{a}_i$ be the set of leading coefficients a_i of polynomials of I <u>of degree</u> i . It is immediately seen that $\mathfrak{a}_i$ is an ideal in R , and that

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \ldots .$$

Since R is noetherian, this sequence of ideals becomes constant, say $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots$.

Let $\{a_{ij}\}_j$ be a finite set of generators for $\mathfrak{a}_i$, $i \leqq n$, and let f_{ij} be a polynomial in I of degree i with leading coefficient a_{ij} . Then I claim that I is generated by the set $\{f_{ij}\}_{ij}$:

Let $g \in I$, say

$$g(x) = b_m x^m + \ldots + b_1 x + b_0\ .$$

<u>Case 1:</u> $m > n$. Since $\mathfrak{a}_n = \mathfrak{a}_m$, the leading coefficient b_n is in $\mathfrak{a}_n$, hence

$$b_m = \sum_j r_j a_{nj} \qquad r_j \in R\ .$$

Then

$$h = x^{m-n}\left(\sum_j r_j f_{nj}\right)$$

is of degree m and has leading coefficient b_m . Hence $g-h$ has lower degree.

Case 2: $m \leqq n$. Then b_m is in $\mathfrak{a}_m$, hence

$$b_m = \sum_j r_j a_{mj} \qquad r_j \in R ,$$

and so

$$h = \sum_j r_j f_{mj}$$

is of degree m and has leading coefficient b_m . Again $g-h$ has lower degree.

Proceed by induction.

B. Cohen-Seidenberg.

This theorem is an important application of the Nakayama Lemma (5.F.1):

Theorem 1: Let R be a ring and let $R \subset A$ be a finitely generated integral ring extension. Then the map Spec $A \longrightarrow$ Spec R is surjective.

(Note that we assume the map $f: R \longrightarrow A$ injective.)

Proof: Recall (1.C.10) that the map Spec $A \longrightarrow$ Spec R carries a prime ideal P of A to $f^{-1}(P)$, which in this case is just $P \cap R$. Thus the assertion of the theorem is:

(2) Let p be a prime of R . There is a prime P of A such that $P \cap R = p$.

Consider first the case that R is a local ring and that $p = \mathfrak{m}$ is its maximal ideal. Since A is finitely generated and integral, it is an R-module of finite type

(6.B.3). Thus we may apply the Nakayama lemma (5.F.1), and we conclude that

$$\mathfrak{m} A \neq A .$$

In this situation, $\mathfrak{m} A = \left\{ \Sigma m_i a_i \,\middle|\, m_i \in \mathfrak{m} \text{ and } a_i \in A \right\}$ is just the <u>ideal</u> of A generated by $\mathfrak{m}$. Therefore this ideal is contained in a maximal ideal M, and we have

$$\mathfrak{m} \subset M \cap R \subset R .$$

Since $1 \notin M$, it follows that $M \cap R \neq R$. Hence $\mathfrak{m} = M \cap R$, which is what was to be proved.

Now to treat the general case, consider the diagram of rings

$$\begin{array}{ccc} R & \longrightarrow & R_p \\ \downarrow & & \downarrow \\ A & \longrightarrow & A_p \end{array}$$

where A_p is the ring obtained by localizing A with respect to $R-p$ (it is the stalk of the sheaf of $\tilde{R}$-modules $\tilde{A}$ at p). Clearly, A_p is a finite integral extension of R_p. Thus if we let $\mathfrak{m} = p R_p$ be the maximal ideal of R_p, we can apply the above reasoning to conclude that there is a maximal ideal M of A_p such that $M \cap R_p = \mathfrak{m}$. Let P be its inverse image in A. Then $P \cap R =$ (inv. im. of M in R) $=$ (inv. im. of $\mathfrak{m}$ in R) $= p$ (by (2.B.2), for instance). Thus P is the required prime of A.

To understand the geometric nature of integral extensions one should combine (1) with the following observation:

<u>Proposition 2:</u> Let $f: R \longrightarrow A$ be a finitely generated <u>integral</u> extension. Then the map $\operatorname{Spec} A \longrightarrow \operatorname{Spec} R$ is finite-to-one.

Proof: Let $p \in \operatorname{Spec} R$, and let $\{P_i\}$ be the set of primes of A whose image $f^{-1}(P_i)$ in $\operatorname{Spec} R$ is p. Then no image in A of an element $s \in R-p$ lies in any P_i. Hence (2.B.2) the P_i generate distinct prime ideals in A_p, and they lie over the maximal ideal of R_p. Thus it suffices to treat the case R local and $p = \mathfrak{m}$ its maximal ideal. Now for any prime P of A such that $P \cap R = \mathfrak{m}$, we have $\mathfrak{m} A \subset P$. Hence (1.C.13) P corresponds to a prime ideal of $A/\mathfrak{m} A$, which is a finite dimensional vector space over $k = R/\mathfrak{m}$, and thus has only finitely many prime ideals.

For reference, we also include the following two propositions:

<u>Proposition 4:</u> Let R be an integral domain with field of fractions K and let α be an element of an extension field L/K which is algebraic over K.

(i) There is a non-zero element $r \in R$ such that $r\alpha$ is integral over R.

(ii) If R is integrally closed, and if α is integral over R, then the irreducible monic equation for α over K has its coefficients in R.

Proof: (i) Let

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 = 0 \qquad c_i \in K$$

be the irreducible monic equation for α over K. Clearing denominators, we get an equation for α of the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \qquad a_i \in R .$$

The element $a_n\alpha$ therefore satisfies the equation

$$x^n + (a_{n-1}a_n)x^{n-1} + \cdots + (a_1 a_n{}^{n-1})x + (a_0 a_n{}^n) = 0 ,$$

and hence is integral over R.

(ii) Each of the conjugates $\alpha_1,\ldots,\alpha_n$ of α in a splitting field is also integral, since it satisfies the same equation. By (7), the symmetric functions in α_i are also integral, and they are in K, hence in R. Since the coefficients of the irreducible equation for α over K are symmetric functions, this equation has coefficients in R.

<u>Proposition 5:</u> A unique factorization domain is integrally closed.

Proof: Let $z \in K$ be an element which is integral over R, and write $z = x/y$ where $x,y \in R$ are elements with greatest common divisor 1. Write the monic equation

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1x + a_0 = 0 , \qquad a_i \in R$$

in the form

$$(x/y)^n = b/y^{n-1} \qquad b \in R$$

by putting the terms of degree $< n$ in z on the other side. We get

$$x^n/y = b \in R ,$$

hence y divides x^n. Since $\gcd(x,y) = 1$, it follows that y is a unit, i.e., $z \in R$.

C. <u>The Noether normalization theorem.</u>

When combined with (B.1), this is a powerful tool:

<u>Theorem 1:</u> Let R be a finitely generated integral domain over a field k, and suppose that the transcendence degree of R/k (= tr. deg. K/k, if K is the field of fractions of P) is s. There is a set of elements $\{y_1,\ldots,y_s\} \subset R$ (necessarily algebraically independent over k) such that R is a finite integral extension of the subring $k[y_1,\ldots,y_s]$.

Proof: (Nagata). Say R is generated by $\{x_1,\ldots,x_n\}$, i.e., $R = k[x_1,\ldots,x_n]$. If the elements x_i are algebraically independent, there is nothing to prove. Suppose not. Then there is a non-trivial relation among them, of the form

$$(2) \quad \Sigma\, a_{(j)}x^{(j)} = \Sigma\, a_{j_1\cdots j_n}\, x_1^{\,j_1} \cdots x_n^{\,j_n} = 0$$

with coefficients $a_{(j)}$ in k . Put

$$y_i = x_i - x_1^{m_i}$$

$$(3) \qquad x_i = y_i + x_1^{m_i} , \qquad i = 2,\ldots,n .$$

Then $R = k[x_1,\ldots,x_n] = k[y_1,y_2,\ldots,y_n]$. Substituting (3) into (2) . The result is

$$(4) \qquad \Sigma\, a_{(j)}\, x_1^{y_1} (y_2 + x_1^{m_2})^{j_2} \cdots (y_n + x_n^{m_n})^{j_n} = 0 .$$

One sees by expanding a term of this out, that the highest power of x_1 occuring is of the type

$$a_{(j)}\, x_1^{(j_1+m_2j_2+\cdots+m_nj_n)} .$$

Therefore, if $m_2,\ldots,m_n$ are carefully chosen (so that the coefficients $a_{(j)}$ don't cancel out), then (4) is a polynomial in x_1 with coefficients in $k[y_2,\ldots,y_n]$ whose highest coefficient is constant, whence x_1 is integral over $k[y_2,\ldots,y_n]$. Since integral dependence is transitive (6.B.6) , we are reduced to proving the theorem for $k[y_2,\ldots,y_n]$, hence are through by induction on n .

D. The Hilbert Nullstellensatz.

We will state various closely related forms of this fundamental result:

<u>Theorem 1:</u> (Zariski's form). If a finitely generated extension $k[x_1,\ldots,x_n]$ is a field K, then all the x_i are algebraic over k.

Of course, the converse is also true, and is elementary.

<u>Example 2:</u> The field of rational functions $k(x)$ in one variable over k is not finitely generated as a k-algebra. You need to adjoin to $k[x]$ the infinitely many inverses $1/p(x)$, $p(x)$ an irreducible polynomial.

Proof of (1): A polynomial ring in at least one variable is not a field (convince yourself as you like). Thus it contains a prime ideal other than (0), and so by (B.1), an integral extension has more than one prime ideal, and so is not a field. Thus it follows from the Noether normalization theorem that if $k[x_1,\ldots,x_n]$ is a field K, then tr. deg. $K/k = 0$, which is what was to be proved.

<u>Theorem 2:</u> Let $R = k[x_1,\ldots,x_n]$ be a non-zero finitely generated algebra over k. There is a k-homomorphism

$$f\colon R \longrightarrow \overline{k}$$

where $\overline{k}$ is the algebraic closure of k.

Proof: Let $\mathfrak{M}$ be a maximal ideal of R. The map $R \longrightarrow R/\mathfrak{M}$ is a k-homomorphism, if $R/\mathfrak{M}$ is given the obvious structure of k-algebra, and $R/\mathfrak{M}$ is generated by the residues of $x_1,\ldots,x_n$, hence is finitely generated. Thus it suffices to prove the theorem for the field $R/\mathfrak{M}$, i.e., in the case R is a field. Then by (1) , R is an algebraic extension of k , which can indeed be embedded in $\bar{k}$.

<u>Theorem 3:</u> Let $X = \operatorname{Spec} R$, where R is a finitely generated algebra over k , and let $C \subset X$ be a closed set. Then the closed points of C are dense in C .

Proof: Let $\bar{R} = R/\mathscr{I}(C)$. Then $C = \operatorname{Spec} \bar{R}$ (1.C.13) . Since $\bar{R}$ is again finitely generated, we may as well assume $C = X$.

Suppose the points are not dense, and let $Y \subsetneq X$ be their closure. Since $Y = V(\mathscr{I}(Y))$ (1.D.3) , it is immediately seen that there is an element $s \in R$ such that

$$X \supsetneq V(a) \supset Y .$$

Then $\operatorname{Spec} R_s = X - V(s) \neq \emptyset$, hence $R_s = R[1/s] \neq 0$, and so R_s has a maximal ideal $\mathfrak{M}$. <u>But</u> the ring R_s is again finitely generated over k , and so $R_s/\mathfrak{M}$ is a finite algebraic extension of k , by (1) . Therefore, the image of R is $R_s/\mathfrak{M}$ is a field (being an integral domain and a finite k-module), which implies that the prime ideal $\mathfrak{M} \cap R$ of R is a maximal ideal of R corresponding to a closed point of $X-V(s) \subset X-Y$, a contradiction.

<u>Theorem 4:</u> (the classical form). Let $\mathfrak{A}$ be an ideal of the polynomial ring $k[x_1,\ldots,x_n]$, and let $f \in k[x_1,\ldots,x_n]$. If $V(f)$ contains every <u>closed</u> point of $V(\mathfrak{A})$, i.e., if

$f \in \mathfrak{M}$ for every maximal ideal $\mathfrak{M}$ containing $\mathfrak{A}$, then

$$f^n \in \mathfrak{A} \quad \text{for some } n .$$

Proof: Since $V(f)$ is closed, and the closed points of $V(\mathfrak{A})$ are dense by (3) , we have $V(f) \supset V(\mathfrak{A})$. Hence by (1.D.3) , rad $(f) \subset$ rad $(\mathfrak{A})$, i.e., $f^n \in \mathfrak{A}$ for some n .

E. Geometric points.

Fix a field k . Let R be an algebra generated over k by elements $x_1,\ldots,x_n$, and let $\mathfrak{M}$ be a maximal ideal of R . Since $R/\mathfrak{M} = K$ is a finitely generated field over k , (D.1) asserts that it is algebraic, i.e., a finite field extension of k . Thus it can be embedded in an algebraic closure $\bar{k}$ of k , which, as we saw (D.2) , yields a k-homomorphism $f: R \longrightarrow \bar{k}$.

Choose such an embedding of K in $\bar{k}$, and let $a_1,\ldots,a_n$ be the images of the generators x_i . These images determine f since the x_i generate R . Conversely, any choice of elements $a_1,\ldots,a_n \in \bar{k}$ gives rise to a homomorphism $f: R \longrightarrow \bar{k}$ by substitution of a_i for x_i , if $R = k[x_1,\ldots,x_n]$ is the polynomial ring.

Now in general, $R = k[x_1,\ldots,x_n]/I$ where I is some finitely generated (8.A.1) ideal, say

(1) $$f_1,\ldots,f_r \in k[x_1,\ldots,x_n]$$

generate I , so that (1.C.13) Spec R identifies with the variety $V(I) = V(f_1) \cap \ldots \cap V(f_r)$ in "affine space" Spec $k[x_1,\ldots,x_n]$. Then it is clear from the universal property of quotient rings that the substitutions $\{x_i = a_i\}$ give a homomorphism $R \longrightarrow \bar{k}$ <u>if and only if</u>

$$(2) \qquad f_i(a_1,\ldots,a_n) = 0 \qquad i=1,\ldots,r ,$$

i.e., if and only if $(a_1,\ldots,a_n)$ is a solution of the equations $f_1 = \cdots = f_r = 0$.

Such a homomorphism $f\colon R \longrightarrow \bar{k}$ (equivalently, such an n-tuple $(a_1,\ldots,a_n)$) will be called a <u>geometric point</u> of Spec R , or a <u>point with values in</u> $\bar{k}$. This last phrase expresses the fact that the n-tuple $(a_1,\ldots,a_n)$ is what we think of as an ordinary point of n-space, but it has coordinates in the field $\bar{k}$. One introduces similarly the notion of point with values in any field extension L/k , meaning an n-tuple $(a_1,\ldots,a_n)$ with $a_i \in L$, and satisfying (2) .

If $(a_1,\ldots,a_n)$ has coordinates $a_i \in k$, then it is clear that the homomorphism $f\colon R \longrightarrow k$ is obtained by dividing R by the ideal generated by the elements

$$(3) \qquad x_1-a_1 ,\ldots, x_n-a_n \qquad a_i \in k$$

of R . Thus the elements (3) generate $\mathfrak{M}$, in the above situation, and the residue field is $K = k$. It is called a <u>rational point</u> = point with values in k . These points are the familiar ones. If for instance k is algebraically closed, so that $k = K = \bar{k}$, then every geometric point is rational, hence

(4) If k is algebraically closed, every maximal ideal of R is of the familiar type, i.e., generated by some linear functions (3) . The maximal ideals and the geometric points are thus in one-to-one correspondence in this case.

However, when k is not algebraically cosed, there is not a one-one correspondence between geometric points of Spec R and maximal ideals, i.e., closed points of Spec R . Of course, a geometric point $f: R \longrightarrow \bar{k}$ gives a maximal ideal; it is the image of Spec $\bar{k} \longrightarrow R$, i.e., the kernel of f . But to obtain the map $f: R \longrightarrow \bar{k}$ from a maximal ideal $\mathfrak{M}$, we have to embed $R/\mathfrak{M} = K$ in the algebraic closure $\bar{k}$, and the number of ways this can be done is the separable degree of K over k :

(5) Given a maximal ideal $\mathfrak{M}$ of R , there are $[K:k]_s$ distinct geometric points whose image is $\mathfrak{M} \in$ Spec R , where $K = R/\mathfrak{M}$.

This is somewhat confusing at first, and you should think it through.

Example 6: Let $k = \mathbb{R}$ be the field of real numbers, and $R = k[x]$. The two geometric points $x = i$, $x = -i$ (= points with values in $\mathbb{C}$) form a "pair of conjugate points". They correspond to the same maximal ideal of $\mathbb{R}[x]$, namely to the kernel of the map $f\colon R[x] \longrightarrow \mathbb{C}$ sending $x \rightsquigarrow i$ (resp. $x \rightsquigarrow -i$) . The kernel is generated by the polynomial $x^2 + 1$.

F. Dimension theory.

There are two reasonable definitions of dimension for a finitely generated algebra over a field k , and it turns out that they are equivalent.

Definition 1: Let X be a topological space. Its Krull dimension is the length n of the longest chain

$$(\emptyset \neq) \qquad C_0 \subsetneq C_1 \subsetneq \cdots \subsetneq C_n \qquad (\subseteq X)$$

of irreducible closed subsets (1.F) of X , or is ∞ if there is no maximal length. Note that the chain starts with C_0 . Similarly, the Krull dimenson of a ring R is the length n of the longest chain

$$(R \neq) \qquad p_0 \supsetneq p_1 \supsetneq \cdots \supsetneq p_n \qquad (\supseteq (0))$$

of prime ideals of R , or is ∞ if there is no maximal length.

Thus by (1.5.2) , Krull dim(R) = Krull dim(Spec R) .

This notion of dimension is reasonable only for the kind of topological spaces which arise as spectra. It has no connection with the usual notion of dimension of a "nice" space.

Examples 2: A field, or more generally a ring with dcc, has Krull dimension zero. Thus in (1.G), examples 2, 3 have Krull dimension zero. Numbers 4, 5, 7 have Krull dimension 1. We shall see that 6 has Krull dimension 2. By (ex. 1, No. 4), the ring $k[x,y]/(y^2-x^3)$ has also dimension 1.

A restatement of (6.D.1(ii)) is

Corollary 3: A dedekind domain is an integrally closed noetherian domain of Krull dimension 1.

Recall (6.A.10(iii)) that any closed subset $Y \subset X = \operatorname{Spec} R$ (R noetherian) is a finite union of irreducible closed subsets $Y = C_1 \cup \ldots \cup C_n$. If we leave out those C_i which are contained in some other C_j, then it is easily seen that the remaining C's are uniquely determined. They are called the irreducible components of Y. Let p_i be the prime ideal corresponding to C_i (1.F.2). Then the p_i are just the minimal primes containing $\mathcal{J}(Y)$, i.e., (1.D.2),

$$\mathcal{J}(Y) = \cap\, p_i .$$

When $Y = X$, the components are the irreducible components of Spec R, and they correspond to the (finite set of) minimal prime ideals of R. Clearly, the Krull dimension of Spec R is the maximum of the Krull dimensions of the irreducible components of Spec R.

For finitely generated algebras R over a field k, there is another candidate for dimension: If R is an integral domain, we can take its transcedence degree over k (= tr. deg. K/k, K the field of fractions of R). The Nullstellensatz (D.1) says that this agrees with the Krull dimension when either of the two is zero. More generally, for any R finitely generated over k, we can take the maximum value of tr. deg. (R/p) over k for the minimal primes p of R (which correspond by the above discussion to the irreducible components of Spec R). Let us call this number

(4) $$\mathrm{td}(R) .$$

To begin with, note that td is not a very sensitive notion:

<u>Proposition 5:</u> Let R be a finitely generated algebra over k.

(i) $\mathrm{td}(R) = \mathrm{td}(R/N)$, where N is the nilradical (1.D) of R, i.e., the intersection of the minimal primes of R.

(ii) $\mathrm{td}(R) \geq \mathrm{td}(R/I)$ for any ideal I of R.

(iii) If $I_1,\ldots,I_s$ are ideals of R with intersection zero, then

$$\mathrm{td}(R) = \max_{\nu} \{\mathrm{td}(R/I_\nu)\} .$$

(iv) $\mathrm{td}(R) = \mathrm{td}(R_s)$ if s is an element of R which is not in any minimal prime ideal.

(v) $td(R) = td(R')$ if $R \subset R'$ is a finite integral extension.

Proof: (i) is trivial.

(ii). If $\bar{q}$ is a minimal prime of R/I, then the corresponding prime q of R is contained in some minimal one p. One sees immediately that therefore it is enough to prove the inequality when R, R/I are replaced by R/p, R/q respectively. Thus we may assume both are integral domains. Now if $x_1,\ldots,x_n \in R/p$ have algebraically independent residues in R/q, then they are certainly themselves algebraically independent. We can find algebraically independent elements $\bar{x}_1,\ldots,\bar{x}_n \in R/I$, where $n = td(R/I)$ (you just choose them in the fraction field and clear denominators), and they have representatives in R. Hence $td(R) \geq td(R/I)$.

(iii). For, any minimal prime p of R contains one of the I (1.B.7) and thus corresponds to a minimal prime of R/I. Hence $td(R) \leq \max\{td(R/I_\nu)\}$. The other inequality follows from (ii).

(iv). By (2.B.2), each minimal prime p generates a prime ideal of R_S, and clearly $(R/p)_{\bar{S}} = R_S/pR_S$, if $\bar{s}$ is the residue of s (mod p) (cf. proof of (2.B.2)). Thus we are reduced by the definition to the case $R = R/p$, i.e., R an integral domain, and $s \neq 0$. But in this case, the definition depends only on the field of fractions hence we are done.

(v). By (i), we may replace R by R/N and R' by R'/N' (N' = nilradical of R'). It is immediately seen that the map $R \longrightarrow R'$ remains injective. Let $p_1', \ldots, p_r'$ be the minimal primes of R', and $p_i = p_i' \cap R$. Then since R' has no nilradical, $\cap p_i' = (0)$ (1.D), and so also $\cap p_i = (0)$. Applying (iii), we see that it suffices to show that $td(R/p_i) = td(R'/p_i')$ for each i. Thus we are reduced to the case that R and R' are integral domains. In this case, the field of fractions K' is algebraic over the field of fractions K of R, hence tr. deg. K'/k = tr. deg. K/k as desired.

The main result is the following, obviously fundamental, fact:

<u>Theorem 6:</u> Let R be a finitely generated integral domain over k, with $td(R) = n$. Let $f \neq 0$ be a non-unit of R. Then $td(R/(f)) = n-1$. More precisely, for every minimal prime $\bar{p}$ of $\bar{R} = R/(f)$, $td(\bar{R}/\bar{p}) = n-1$.

Proof: This arrangement is taken from Lang's <u>Intr. to Alg. Geom.</u>, and is due to Tate:

We treat first the essentially obvious case $R = k[y_1, \ldots, y_n]$ of a polynomial ring. Any prime ideal p containing f contains an irreducible factor of f. Since R is a UFD, the irreducible factors generate prime ideals, and so these are the minimal primes containing f, and correspond to the minimal primes of $R/(f)$. Thus the assertion of the theorem is just that if f is an irreducible polynomial, then $td(R/(f)) = n-1$.

Write

$$(7) \qquad f = \Sigma\, a_{(j)}\, y^{(j)} = 0 \qquad \text{in } R/(f)$$

and say it involves the variable y_n . Then gf also involves y_n for any $g \neq 0$. Thus there is no polynomial in $y_1,\ldots,y_{n-1}$ congruent zero (mod f) , and so the residues of $y_1,\ldots,y_{n-1}$ if $R/(f)$ are algebraically independent. Since the residue of y_n is algebraic over $k(y_1,\ldots,y_{n-1})$ by (7) , this shows that $td(R/(f)) = n-1$.

In the general case, we may assume that Spec $R/(f)$ has only one minimal prime. For, let $p_1,\ldots,p_r$ be the minimal primes containing f . Choose an element $s \notin p_1$ which is in each of the p_i $(i>1)$. Since $p_1 \not\subset p_i$, also $p_1 \not\subset \bigcap_{i>1} p_i$ (1.C.7) and so this is possible. Then if $\bar{s}$ is the residue of s (mod p_1) , we have

$$(R/p_1)_{\bar{s}} = (R_s/p_1R_s) \ ,$$

and by (4 (iv)), $td(R/p_1) = td(R_s/p_1R_s)$. But since $s \in p_i$ $(i>1)$. The ring R_s has only the one minimal prime p_1R_s containing f (2.B.2) . This proves our assertion.

We want to use the Noether normalization theorem (C.1) and (5 (v)) to complete the proof: Let $k[y_1,\ldots,y_n] \subset R$ be a subring over which R is integral, and let $\mathfrak{a}$ be the kernel of the map

$$k[y_1,\ldots,y_n] \longrightarrow R/(f) .$$

Then $R/(f)$ is an integral extension of its subring $k[y]/\mathfrak{a}$. Hence by (5 (v)) , it suffices to show that $td(k[y]/\mathfrak{a}) = n-1$.

Recall the notion of norm in a finite field extension L/K . For $x \in L$, its norm $N(x) \in K$ is defined as follows: Let $\phi_i : L \longrightarrow \overline{K}$ $(i=1,\ldots,s)$ be the distinct embeddings of L into an algebraic closure $\overline{K}$ of $\overline{K}$, and let $p^e = [L:K]_i$ be the inseparable degree. Put

$$N(x) = \prod_{i=1}^{s} \phi_i(x)^{p^e} .$$

Then $N(x)$ is a function from L to K satisfying

$$N(xy) = N(x)N(y) .$$

The element $N(x)$ is just a certain power of the coefficient of the irreducible monic equation for x over K (proofs may be found in any book on field theory).

Now let L be the field of fractions of R , and $K = k(y_1,\ldots,y_n)$. Put

$$F = N(f) .$$

By (B.4(ii),5) , F is in $k[y_1,\ldots,y_n]$ since f is integral over this ring, and since the norm is a power of a coefficient of the irreducible equation.

I claim that the varieties of F and $\mathfrak{a}$ in Spec $k[y_1,\ldots,y_n]$ are equal, i.e., $V(F) = V(\mathfrak{a})$, i.e. (1.D.4) that $\operatorname{rad} F = \operatorname{rad} \mathfrak{a}$. Since we have settled the case of one equation in Spec $k[y]$, and since one sees immediately that F is not zero or a unit (because it banishes where f does) this will complete the proof.

It is clear that $F \in \mathfrak{a}$. For, F is a power of the constant term a_0 of an irreducible monic equation

$$f^N + \cdots + a_1 f + a_0 = 0$$

(which has coefficients in R (B.4(ii)), hence F is divisible by f in R. Conversely, let $g \in \mathfrak{a}$. Then f divides g in R:

$$g = fh ,$$

whence

$$N(g) = N(f)N(h) .$$

The three terms in this expression are in $k[y]$, again by (B.4(ii)). But since $g \in k[y]$, $N(g)$ is just a certain power of g. Thus

$$F \mid g^m$$

for some m, which completes the proof.

<u>Theorem 8:</u> Let R be a finitely generated algebra over k. Then

$$\text{Krull dim } R = \operatorname{td}(R) .$$

If R is an integral domain, then any chain of prime ideals $p_0 \supset \cdots \supset p_r$ can be extended to a maximal chain having length $td(R)$.

Proof: Induction on $n = td(R)$. It is true if $n=0$. Since both numbers are obtained by maximizing over R/p for the various minimal primes p of R , we may assume R to be an integral domain, and that $td(R) = n$. Let

$$(9) \qquad p_0 \supset \cdots \supset p_{r-1} \supset p_r = (0)$$

be a chain of primes of R . Put $q = p_{r-1}$ then q contains some non-zero element f . By (6) , $td(R/(f)) = n-1$, hence $td(R/q) \leqq n-1$. Since primes of R/q correspond to primes of R containing q , it follows by induction that the length r of the chain (9) is at most n . Moreover, if (9) can not be extended, i.e., if no prime can be inserted in this chain, then clearly q is a minimal prime containing (f) , hence $td(R/q) = n-1$ by (6) , and so by induction, $r=n$.

Example 10: Let $R = k[x,y]$ be the polynomial ring in two variables. Any maximal chain of prime ideals has length 2 , i.e., is of the form

$$\mathcal{M} \supset p \supset (0)$$

where $\mathcal{M}$ is a maximal ideal. We have seen in (E) how these look. The ideal p contains a non-zero polynomial, hence an irreducible one $f(x,y)$ which generates a prime ideal since R is a UFD . Thus $p . (f)$ is a principal prime ideal. Spec $R/p = V(f)$ has dimension 1 . It is an (irred.) "plane curve".

For $R = k[x,y,z]$, the maximal length is 3:

$$\mathfrak{M} \supset q \supset p \supset (0) .$$

$\mathfrak{M}$ is maximal, and p is principal as above. Spec R/p is of dimension 2 -- a "surface". Spec R/q is of dimension 1 , -- a "space curve". etc...

Remark 11: If p is a prime of R , its height h is the length of the longest chain of prime ideals

$$p = p_0 \supset \cdots \supset p_h \quad (\supseteq (0))$$

beginning with p . It is clear from (8) that (6) implies the following assertion:

Let $f \neq 0$ be a non-unit of R . Then the height of a minimal prime p containing f is 1 .

This says that the locus of zeros of a single $f \in R$ can not be too small. A rather delicate fact is that this is true for any noetherian integral domain R . It is known as Krull's principal ideal theorem, and is the basic result of dimension theory in general noetherian rings.

G. The plane curve $y^2 = x^3 + ax + b$.

As an example, we are going to examine in some detail the ideal class group (6.F) $H^1(X,\tilde{R}^*)$ of a certain cubic curve, i.e., of the ring

(1) $$R = k[x,y]/(f)$$

where

(2) $$f = y^2 - (x^3 + ax + b) \qquad a,b \in k .$$

We will not carry out all details of proof.

We assume the field k to be algebraically closed.

Lemma 3: Let f, g be polynomials in two variables in $k[x,y]$ which vanish at the origin $(0,0)$. Write

$$f = ax + by + (\text{higher terms})$$

$$g = cx + dy + (\text{higher terms}) .$$

Suppose that $ad-bc \neq 0$. Then in the local ring A of $k[x,y]$ at the origin, the maximal ideal $\mathfrak{m}$ is generated by f and g.

Proof: View $\mathfrak{m}$ as an A-module. $\mathfrak{m}$ is finitely generated, since it is clear that x, y generate $\mathfrak{m}$. Thus we can apply the Nakayama lemma (5.F.3)! It suffices to show that the residues $\bar{f}$, $\bar{g}$ of f and g modulo $\mathfrak{m}\cdot\mathfrak{m} = \mathfrak{m}^2$ generate $\mathfrak{m}/\mathfrak{m}^2$. But one sees easily that $\mathfrak{m}/\mathfrak{m}^2$ is a vector space over $A/\mathfrak{m} = k$ of dimension 2, and that the condition $ad-bc \neq 0$ is just that $\bar{f}$, $\bar{g}$ form a basis for this space.

Corollary 4: Let $f \in k[x,y]$ be a polynomial vanishing at the point (α,β). If $\frac{df}{dx}(\alpha,\beta)$, $\frac{df}{dy}(\alpha,\beta)$ are not both zero, then the local ring R_p of $R = k[x,y]/(f)$ at the prime p: $x = \alpha$, $y = \alpha$ is a discrete valuation ring.

Such a point is called a <u>simple point</u>, or a <u>smooth point</u> of the curve $f = 0$.

Proof: By making a substitution $x = x' + \alpha$, $y = y' + \beta$, one reduces to the case that $(\alpha,\beta) = (0,0)$. Writing

$$f = ax + by + (\text{higher terms}),$$

we have

$$\frac{df}{dx}(0,0) = a, \qquad \frac{df}{dy}(0,0) = b.$$

Hence if, say, a is not zero, then by (3) the elements f and y generate the maximal ideal in the local ring A. Hence the maximal ideal of R_p, which is just $A/(f)$, is generated by the residue of y. Since R (hence R_p) has Krull dimension 1 by (G.10), this completes the proof.

<u>Corollary 5:</u> Let $f \in k[x,y]$ be an irreducible polynomial, and suppose not all of the polynomials f, $\frac{df}{dx}$, $\frac{df}{dy}$ vanish at any point (α,β). Then $R = k[x,y]/(f)$ is a dedekind domain.

Proof: By (E.4), every maximal ideal of $k[x,y]$ comes from a point (α,β) since k is algebraically closed. Thus for every closed point p of $V(f) = \operatorname{Spec} R$, the ring R_p is a discrete valuation ring by (2). Since Krull dim $(R) = 1$

by (F.10), we are done (F.3).

From now on, we let f be the irreducible polynomial (2), and we assume that the hypotheses of (5) hold for f, so that R is a dedekind domain. It is not hard to see that this implies that the field k is of characteristic different from 2. You may think of k as the field of complex numbers, if you like.

This is a picture of $X = \operatorname{Spec} R$, and some lines, in the plane (the real locus of the cubic often has two parts):

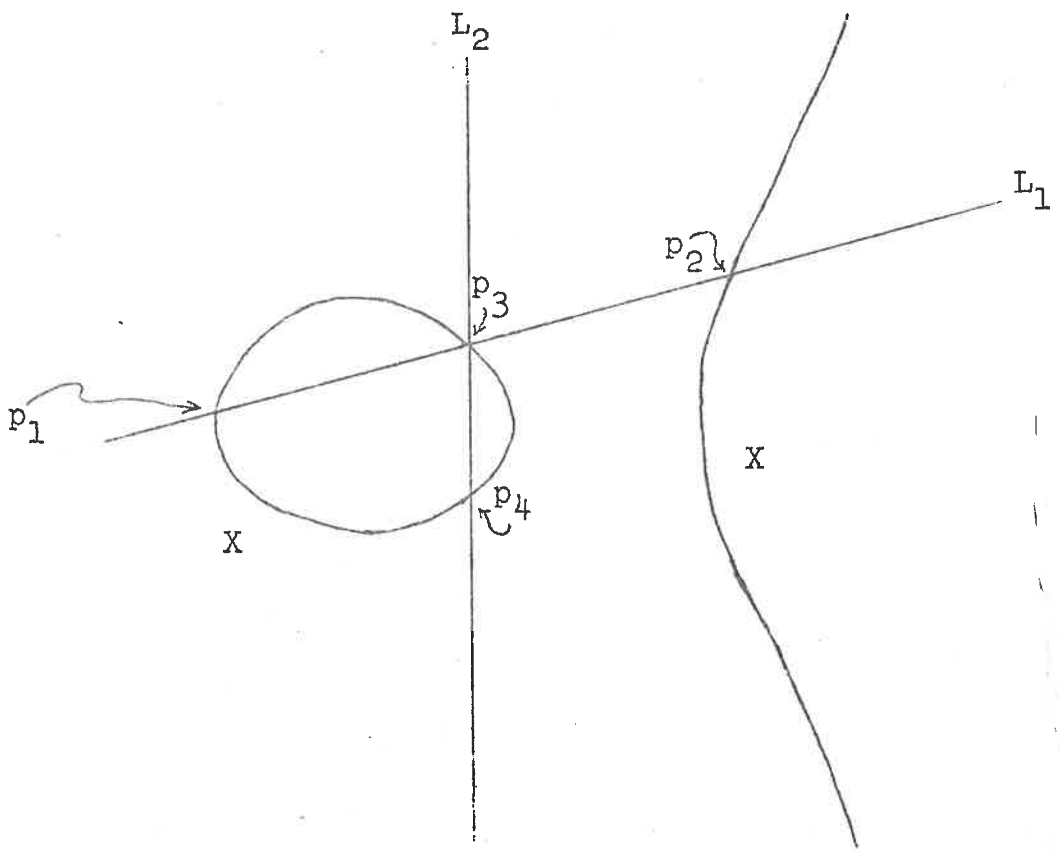


Figure 6

The line L_1 is given by some <u>linear equation</u>

$$g_1(x,y) = 0 .$$

It meets X in at most 3 points. (For, if we change coordinates in the plane, so that L_1 becomes the x-axis ($y=0$), then the equation f (still a cubic) gives an equation of degree ≤ 3 when y is set equal to 0, and the solutions of that equation are the intersection points of X and L_1.) If p is an intersection point, and if the intersection at p is transversal, then the residue $\bar{g}_1$ of g_1 in R generates the maximal ideal in R_p (The phrase "transversal intersection" is expressed in an obvious way in terms of the values of the partial derivatives of f and g_1 at p, and our assertion follows immediately from Lemma 1 after a change of coordinates to move p to the origin.). If X, L_1 have a simple tangency at p, then the residue $\bar{g}_1$ generates the square of the maximal ideal in R_p, etc... (The proof of any such assertion can be carried out in a way similar to that of (1).)

Now R is a dedekind domain (5), hence every non-zero fractional ideal is a product of prime powers. From the above discussion, it is clear that if L_1 meets X in 3 points p_1, p_2, p_3 (necessarily transversally if there are three intersections), then the ideal of R generated by the residue $\bar{g}_1$ is just

$$(\bar{g}_1) = p_1 p_2 p_3$$

(if there is a tangency at one point, then the ideal becomes of the form p^2q , etc.).

Now note that a <u>vertical</u> line L_2 meets X in just two points transversally, of one point with a simple tangency. This follows from the form of the equation (2) . Thus if $g_2 = 0$ is a linear equation for the line L_2 situated as in the figure (6) , the ideal generated by the residue of $g_2^{-1}\ g_1$ is

$$(\bar{g}_2^{-1}\ \bar{g}_1) = p_1 p_2 p_4^{-1}$$

provided L_1, L_2 both meet transversally at p_3 .

If we multiply any non-zero fractional ideal $\mathfrak{a}$ of R by this principal ideal, the effect is to change the exponent e of the primes p_1, p_2, p_4 by 1,1 , -1 respectively. It follows easily that if we start with any ideal

$$\mathfrak{a} = p_1^{e_1} \cdots p_n^{e_n} ,$$

we can change it, by multiplying by a sequence of principal ideals of the above form, into a <u>prime ideal</u>.

Thus the map from the closed points of X to the ideal class group

(7) $$p \rightsquigarrow \text{(its ideal class)}$$

<u>maps onto every non-zero class</u>.

Now it can be shown that the rule

$$(p_1, p_2) \rightsquigarrow p_4$$

(notation as in figure (6)) makes the set of closed points of X into a group except that 0 is missing (it is the point at ∞ of the curve). There are some extreme cases to be described, e.g. if $p_1 = p_2$, which I leave to you. Hence one could expect that the map (7) above is actually one-one as well, and a group homomorphism (taking into account the 0). This is indeed the case, but we are not in a position to prove it so easily here. You have to show that no prime p by itself can be a principal ideal in R.

Here is an outline of a method of proof which can be pushed through for the case $k = \mathbb{C}$: If p were principal, $p = (u)$, then the element $u \in R$ would have only one zero and one pole (at ∞). This would imply that the map $X \longrightarrow \operatorname{Spec} \mathbb{C}[u]$ given by the element $u \in R$ would have to be one-one everywhere, not just at the points p, ∞. But it is easily seen that the variety X, viewed as a closed subspace of complex 2-space with the usual topology, is a torus (minus the point at ∞). In fact, this follows from the fact that the equation (2) represents X as a double covering of the complex x-plane branched at three points (the three roots of $x^2 + ax + b$) plus ∞. This contradicts the existence of a one-one continuous map to the u-plane.

One final remark: Notice that we were able to reduce an arbitrary fractional ideal to a nice form by using only <u>linear functions</u> from the plane. This was very lucky, and the method does not work for higher degree curves. One needs more subtle techniques to treat them; they are provided by what is known as the Riemann-Roch theorem for curves, which assures the existence of elements of the ring having zeros at prescribed points.

FLATNESS

A. Flat modules.

Definition 1: An R-module M is called flat if the functor $M \otimes \cdot$ is exact, i.e., if for every exact sequence

$$A \longrightarrow B \longrightarrow C$$

of R-modules, the sequence

$$M \otimes A \longrightarrow M \otimes B \longrightarrow M \otimes C$$

is again exact.

Since $M \otimes \cdot$ is always right exact (4.D.1), this is equivalent with the assertion that

(2) If $A \subset B$, then $M \otimes A \hookrightarrow M \otimes B$.

Elementary properties:

(3) A direct sum of flat modules is flat.

This follows immediately from (2) and the distributivity of tensor product (T.P.C.4).

(4) A free module is flat.

(5) M and N flat $\Rightarrow M \otimes N$ flat.

This follows from the associativity of tensor product: $(M \otimes N) \otimes A \approx M \otimes (N \otimes A)$.

(6) If M is a flat R-module and $R \longrightarrow R'$ is a ring homomorphism, then $M' = M \otimes_R R'$ is a flat R'-module.

For, recall that there is a canonical isomorphism, for any R'-module A',

(7) $M \otimes_R A' \approx (M \otimes_R R') \otimes_{R'} A' = M' \otimes_{R'} A'$

where A' is viewed as an R-module for the tensor product on the left side by restriction of scalars. Both sides are R'-modules (multiply on the right), and this is an isomorphism of R'-modules.

Now if $0 \longrightarrow A' \longrightarrow B'$ is an exact sequence of R'-modules, (7) clearly implies that $0 \longrightarrow M' \otimes_{R'} A' \longrightarrow M' \otimes_{R'} B'$ is exact.

(8) Flatness is a local notion, i.e., M is flat iff. there is a set S of elements of R which generates the unit ideal such that M_s is flat over R_s for each $s \in S$.

To see this, first note that from (7) it follows that for any two R-modules M, N there are canonical isomorphisms

(9) $M \otimes_R N' \approx M' \otimes_{R'} N' \approx M' \otimes_R N \approx R' \otimes_R (M \otimes_R N)$

where $N' = R' \otimes_R N$ etc.. Since localization is a tensor product, one has canonical isomorphisms (second $\approx$ fourth above)

(10) $$(M \otimes_R N)_s \approx M_s \otimes_{R_s} N_s$$

This just says that the sheaf associated to the tensor product modules is what we would expect:

$$(10) \qquad \widetilde{M\otimes_R N} \approx \tilde{M}\otimes_{\tilde{R}}\tilde{N}$$

where the sheaf on the right is defined to be the one whose sections on an open X_s are $M_s \otimes_{R_s} N_s$. Now (8) is trivial, since the condition for a sequence to be exact is expressed by the associated sheaves (4.D.3) .

Proposition 11: A module of finite presentation is flat iff. it is locally free iff. it is projective.

Proof: By (5.G.1) the last two statements are equivalent. Moreover, a locally free module is flat because of (4) , (8). Thus it remains to show that if M is finitely presented and flat, then it is locally free. Moreover, it suffices by (6) and (5.G.1) to treat the case of a local ring R , and to show that then M is free. Let $\bar{R}$ be the field $R/\mathfrak{m}$, and let $m_1,\dots,m_n$ be elements of M whose residues form a basis of the module $\bar{M} = M/\mathfrak{m}M$. By the Nakayama lemma (5.F.3) , the set $\{m_i\}$ generates M , so that we get an exact sequence (5.B.3)

$$0 \longrightarrow \mathcal{R} \longrightarrow F \longrightarrow M \longrightarrow 0 ,$$

where F is the free module on the set. We want to show that $\mathcal{R}$ is zero, and by the Nakayama lemma, it suffices to show that $\bar{\mathcal{R}} = \mathcal{R}/\mathfrak{m}\mathcal{R}$ is zero (because $\mathcal{R}$ is of finite type since M is finitely presented). If we tensor the above sequence with the exact sequence

$$0 \longrightarrow \mathfrak{m} \longrightarrow R \longrightarrow \overline{R} \longrightarrow 0 \, ,$$

we get a diagram (using (4.D.1))

$$\begin{array}{ccccccccc}
 & & & & 0 & & & & \\
 & & & & \downarrow & & & & \\
 & & \mathfrak{m} \otimes \mathcal{R} & \longrightarrow & \mathcal{R} & \longrightarrow & \overline{\mathcal{R}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathfrak{m} \otimes F & \longrightarrow & F & \longrightarrow & \overline{F} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathfrak{m} \otimes M & \longrightarrow & M & \longrightarrow & \overline{M} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where the bottom row is exact because M is flat. If we apply the serpent diagram (5.A.3) to the left hand pair of columns, we get an exact sequence of kernels and cokernels

$$0 \longrightarrow \overline{\mathcal{R}} \longrightarrow \overline{F} \longrightarrow \overline{M} \longrightarrow 0 \, .$$

Since $\overline{F} \approx \overline{M}$, this shows that $\overline{\mathcal{R}} = 0$, and completes the proof.

<u>Definition 12:</u> An R-module M is <u>faithfully flat</u> if the following condition holds:

A sequence

(*) $$A \longrightarrow B \longrightarrow C$$

is exact iff. the induced sequence

(**) $$M \otimes A \longrightarrow M \otimes B \longrightarrow M \otimes C$$

is exact.

This is equivalent with saying that

(13) M is flat, and for any R-module A, $M \otimes A = 0$ implies $A = 0$.

For, note that $A = 0$ means $0 \longrightarrow A \longrightarrow 0$ is exact. Thus $(12) \Longrightarrow (13)$. Conversely, suppose that (13) holds: Since M is flat, (*) exact implies (**) exact. Suppose (**) exact. Because M is flat, it is immediately seen that $M \otimes \mathrm{im}(A \longrightarrow C) = \mathrm{im}(M \otimes A \longrightarrow M \otimes C)$. Hence $A \longrightarrow C$ is the zero map, i.e., $\ker(B \longrightarrow C) \supset \mathrm{im}(A \longrightarrow B)$. To say these two are equal means that the cokernel ε of the exact sequence

$$0 \longrightarrow \mathrm{im}(A \longrightarrow B) \longrightarrow \ker(B \longrightarrow C) \longrightarrow \varepsilon \longrightarrow 0$$

is zero. Now using the flatness of M, one finds that $M \otimes \varepsilon$ is the cokernel of the corresponding map obtained from (**), hence is zero, whence by (13), $\varepsilon = 0$.

Note that clearly

(14) If M is faithfully flat over R and if $f\colon R \longrightarrow R'$ is arbitrary, then $M' = R' \otimes_R M$ is faithfully flat over R'.

For, M' is flat by (6). Suppose $M' \otimes_{R'} A' = 0$. Then since (7) $M' \otimes_{R'} A' = M \otimes_R A'$, it follows from (13) that $A' = 0$, which shows that M' is faithfully flat.

B. Flat ring extensions.

Definition 1: An R-algebra A is <u>flat</u> (or <u>faithfully flat</u>)

if it is flat (f. flat) as an R-module.

For example, for any $S \subset R$, $S^{-1}R$ is flat, by (4.D.2).

Let A be a flat R-algebra, and I an ideal of R. Put $\bar{R} = R/I$. Then $\bar{R} \otimes A = A/IA$ (TP.D.2). But since A is flat,

$$0 \longrightarrow I \otimes A \longrightarrow A \longrightarrow \bar{A} \longrightarrow 0$$

is exact. Therefore the natural map

(2) $$\begin{aligned} I \otimes A &\longrightarrow IA \\ x \otimes a &\rightsquigarrow xa \end{aligned}$$ is <u>bijective</u>.

For a general ring extension, it would only be surjective.

For any R-module M, there is a natural map

(3) $$\begin{aligned} M &\longrightarrow A \otimes M \\ m &\rightsquigarrow 1 \otimes m \end{aligned},$$

and if A is a faithfully flat R-algebra, this map is <u>injective</u>. For, to prove this, it suffices to show that the map obtained from (3) by tensoring with A is injective, and this map is

$$\begin{aligned} A \otimes M &\longrightarrow A \otimes A \otimes M \\ a \otimes m &\rightsquigarrow a \otimes 1 \otimes m \end{aligned}.$$

There is a map backwards, sending

$$ab \otimes m \leftsquigarrow a \otimes b \otimes m ,$$

and the composition of the two is the identity on $A \otimes M$, hence the first map is injective, as was to be proved. In particular, setting $M = R$ in (3), we obtain

(4) $\quad R \longrightarrow A \quad$ is <u>injective</u>,

if A is faithfully flat over R.

<u>Proposition 5:</u> If $f: R \longrightarrow A$ is a faithfully flat R-algebra, then for every ideal I of R,

$$I = f^{-1}(IA) \quad .$$

If we identify R with a subring of A via (4), this just reads

$$I = R \cap IA \; .$$

proof: Consider the map (3) applied to the exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow \bar{R} \longrightarrow 0 \qquad (\bar{R} = R/I) \; .$$

We get by (2)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I & \longrightarrow & R & \longrightarrow & \bar{R} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & IA & \longrightarrow & A & \longrightarrow & A/IA & \longrightarrow & 0 \end{array} ,$$

and by (3) the last vertical arrow is injective. Therefore an element $x \in R$ which is mapped to zero in A/IA is already zero in $\bar{R}$, i.e., I is the kernel of the map $R \longrightarrow A/IA$, which proves what we want.

<u>Proposition 6:</u> An R-algebra A is faithfully flat if and only if it is flat and the induced map

$$\operatorname{Spec} A \longrightarrow \operatorname{Spec} R$$

is surjective.

proof: Suppose A faithfully flat, and let p Spec R. The algebra A_p is faithfully flat over R_p (A.6). Let $\mathfrak{m} = pR_p$ be the maximal ideal. Then $R_p \cap \mathfrak{m} A_p = \mathfrak{m}$ by (5), hence $\mathfrak{m} A_p$ is not the unit ideal. Thus $\mathfrak{m} A_p$ is contained in a maximal ideal M of A_p, and clearly $M \cap R_p = \mathfrak{m}$. As in the proof of (8.B.1), one sees that if P is the inverse image of M in A, then $P \cap R = p$. Thus Spec $A \longrightarrow$ Spec R is surjective.

Conversely, suppose Spec $A \longrightarrow$ Spec R surjective, and A flat. We need to show that if M is a non-zero R-module, then $M \otimes A \neq 0$. Each finitely generated non-zero submodule $M_0 \subset M$ has the property that $M_0 \otimes A \subset M \quad A$, since A is flat. Therefore it suffices to show $M_0 \otimes A \neq 0$, whence we are reduced to that case M of finite type.

Since $M \neq 0$, there is a $p \in$ Spec R such that $M_p \neq 0$. Since Spec $A \longrightarrow$ Spec R is surjective, the ring $\overline{A} = A_p/\mathfrak{m} A_p$ is not the zero ring
(notation as above). For, it contains a prime ideal. By the Nakayama lemma, $\overline{M} = M_p/\mathfrak{m} M_p$ is a non-zero vector space over the field $\overline{R} = R_p/\mathfrak{m}$, hence is free. Therefore it is clear that $\overline{M} \otimes_{\overline{R}} \overline{A}$ is also non-zero. But we have a commutative diagram of rings

$$\begin{array}{ccc} A & \longrightarrow & \overline{A} \\ \uparrow & & \uparrow \\ R & \longrightarrow & \overline{R} \end{array}$$

and $\overline{M} = M \otimes_R \overline{R}$. Hence $\overline{M} \otimes_{\overline{R}} \overline{A} = M \otimes_R A \otimes_A \overline{A}$, and so $M \otimes_R A$ is also non-zero.

Proposition 7: Let $f: R \longrightarrow R'$ be a faithfully flat ring extension; M an R-module, and $M' = R' \otimes_R M$. Then M is of finite type, or finitely presented, or flat if and only if M' is.

proof: The only if part has been proved (5.B.6), (A.6). Suppose M' of finite type. Since it is clearly generated by the images $1 \otimes m$ of the elements m of M , a finite number $\{1 \otimes m_i\}$ generate M' (5.B.5) . Consider the map $F \longrightarrow M$ of the free module F on x_i , sending $x_i \rightsquigarrow m_i$. We have $F' \to M' \to 0$ exact. Hence $F \to M \to 0$ is exact, i.e., M is of finite type.

If M' is finitely presented, we already know that M is of finite type, and we have to show that a certain module of relations $\mathcal{R}$ (5.B.3) is of finite type. But since R' is flat, one sees immediately that $\mathcal{R}' = R' \otimes_R \mathcal{R}$ is the corresponding module of relations for M' , hence is of finite type. Therefore $\mathcal{R}$ is of finite type, too.

Suppose M' flat. If

$$A \longrightarrow R \longrightarrow C$$

is an exact sequence of R-modules, we have

$$M' \otimes_R A \longrightarrow M' \otimes_R B \longrightarrow M' \otimes_R C$$

exact. But

$$M' \otimes_R A \approx R' \otimes_R (M \otimes_R A) \text{ , etc..}$$

Hence

$$M \otimes_R A \longrightarrow M \otimes_R B \longrightarrow M \otimes_R C$$

is exact since $R \longrightarrow R'$ is faithfully flat. This completes the proof.

FLAT DESCENT

The theory of descent which we treat here is due to Grothendieck, although special cases were known before (cf. Sem. Bourb. #190, and SGA '60, Exposé VIII).

A. Descent.

Let R be a ring, and $f: R \longrightarrow A$ an R-algebra. We assume throughout the discussion that A is faithfully flat (9.B.1) over R. When no indication is made, a tensor product is meant to be taken over R.

We are going to study the following question:

Given an A-module M, when does there exist an R-module N such that $M \approx A \otimes N$? More precisely, what additional structure on the module M will insure the existence and uniqueness of N?

For instance, if M were free over A, with a given basis, we would know how to construct N canonically -- namely as the free R-module with the same basis.

Note that the restriction of scalars is not what we are looking for, since $M \not\approx A \otimes M$ in general.

It is a good idea for the reader to keep the example of localization (cf. 3), which is given in the next section, in mind throughout the discussion.

Among the various tensor products of A with itself there are many maps. In particular, we have the maps

$$(1) \quad A \underset{\xleftarrow{s_0}}{\overset{d_0}{\underset{d_1}{\rightrightarrows}}} A\otimes A \quad \overset{d_0,\ d_1,\ d_2}{\Rrightarrow} \quad A\otimes A\otimes A \cdots\cdots$$

$$A\otimes A \underset{s_1}{\overset{s_0}{\leftleftarrows}}$$

where d_i is the "face" operator which inserts 1 in the i-th position of a tensor (we start the numbering of the positions with 0). Thus for instance

$$d_1(a\otimes b) = a\otimes 1\otimes b \quad .$$

It is customary to use the same symbol d_i for the various maps. The map s_i (the "degeneracy") is the one which multiplies the i-th and (i+1)-th entries in a tensor. Thus

$$s_1(a\otimes b\otimes c) = a\otimes(bc) \ .$$

These maps are all homomorphisms of R-algebras, and they satisfy certain <u>identities</u> such as

$$(2) \qquad s_0d_0 = s_1d_1 = \text{identity},$$
$$d_0s_0 = s_1d_0 \ , \quad \text{etc...}$$

which are easy to see. We leave the verification of such things to the reader. The identities make (1) into what is called a "co-simplicial algebra". This one is known as the <u>Amitsur complex</u>. We will need just as much as is depicted explicitly in (1) , and a few identities of the type (2) .

A standard list of identities could be found in a treatment of simplicial theory (but the arrows usually go the other way).

Suppose now that N is an R-module. Then we can extend scalars in N to any R-algebra A. We will often denote the result of this operation by N_A. Thus N_A is an A-module which is canonically isomorphic to either of the modules

$$N\otimes A \approx N_A \approx A\otimes N$$

and for notational reasons, it is convenient to avoid choosing one or the other.

If $A \longrightarrow B$ is a homomorphism of R-algebras, then there is of course an induced map $N_A \longrightarrow N_B$, which is in fact A-linear. Applying this fact to diagram (1), we get a bunch of maps

$$(3)\quad \begin{tikzcd} N_A \arrow[r, shift left=2, "d_0"] \arrow[r, shift right=2, "d_1"'] & N_{A\otimes A} \arrow[l, shift left=6, "s_0"] \arrow[r, shift left=4, "d_0"] \arrow[r, "d_1"] \arrow[r, shift right=4, "d_2"'] & N_{A\otimes A\otimes A} \arrow[l, shift left=8, "s_0"'] \arrow[l, shift left=10, "s_1"] & \cdots\cdots \end{tikzcd}$$

by tensoring with N, which satisfy the same identities (2) as (1).

<u>Notation 5:</u> We will call a diagram

$$\begin{tikzcd} X \arrow[r] & Y \arrow[r, shift left, "u"] \arrow[r, shift right, "v"'] & Z \end{tikzcd}$$

of abelian groups an <u>exact sequence</u> if the sequence

$$0 \longrightarrow X \longrightarrow Y \xrightarrow{u-v} Z$$

is exact. This means that X is mapped (injectively) onto the subset of those elements of Y which are carried to the same element by u and by v. The group X is called the <u>kernel of the pair of maps</u> (u,v). This is a notational convenience, and it provides a definition of kernel for maps of sets.

The descent theory is based on the following observation:

<u>Proposition 6:</u> Let N be an R-module. Consider the sequence

$$N \longrightarrow N_A \underset{d_1}{\overset{d_0}{\rightrightarrows}} N_{A\otimes A}$$

where the first map is, say, $n \rightsquigarrow n\otimes 1$ if we identify N_A with $N \otimes A$. <u>This sequence is exact.</u> In particular, the sequence (obtained by setting $N = R$)

(6')
$$R \longrightarrow A \underset{d_1}{\overset{d_0}{\rightrightarrows}} A\otimes A$$

is exact.

proof: We saw in (9.B.3) that the first arrow is injective. Since A is faithfully flat, it suffices to prove that the sequence obtained from (6) by tensoring with A is exact. If we tensor by A, say on the right, to fix the numbering of the positions, we get the sequence

$$N_A \xrightarrow{d_0} N_{A\otimes A} \overset{d_0}{\underset{d_1}{\rightrightarrows}} N_{A\otimes A\otimes A} \quad .$$

Let x be an element of the middle module such that

(*) $$d_0 x = d_1 x \ .$$

I claim that in the notation of (1),

$$x = d_0 s_0 x \quad ,$$

whence x is in the image of d_0, which will complete the proof. We have

$$\begin{aligned} d_0 s_0 x &= s_1 d_0 x && \text{(cf. (2), and check it!)} \\ &= s_1 d_1 x && \text{by (*)} \\ &= x && \text{by (2) ,} \end{aligned}$$

qed.

Now let M be an A-module. Extending scalars in M by the <u>two structures of A-algebra on</u> $A\otimes A$ (given by d_0, d_1 of (1)), we obtain <u>two</u> $A\otimes A$-<u>modules</u>, which we will write as

(7) $$\begin{aligned} (A\otimes A) \otimes_A M &\approx A\otimes M \\ M \otimes_A (A\otimes A) &\approx M\otimes A \end{aligned} \qquad \text{(canon. isoms.)}$$

where in the top line, the operation of A on $A\otimes A$ is understood to be via d_0, and in the bottom via d_1. The operation of $A\otimes A$ on $M\otimes A$, $A\otimes M$ is the obvious one.

If M were obtained from an R-module N by extension of scalars (i.e., $M = N_A$), then the two $A\otimes A$-modules (7) would be <u>canonically isomorphic</u>, namely to $N_{A\otimes A}$. This is just "transitivity of extension of scalars", since the structure of R-algebra on $A\otimes A$ is obtained by the single homomorphism $d_0f = d_1f$ from R to $A\otimes A$ (cf. (6')). However, <u>in general, they will not be isomorphic at all</u>. It is easy to give such examples.* Of course, there is the symmetry of the tensor product, but it does not preserve the structure of $A\otimes A$-module. Thus since our problem is to determine those M which are obtained by extension of scalars, we can put an extra structure on the module by insisting that there be an isomorphism Θ between the $A\otimes A$-modules (7) , more precisely, by <u>assigning</u> such an isomorphism:

<u>Definition 8:</u> Let M be an A-module. <u>Descent data</u> for M relative to the algebra structure $R \longrightarrow A$ consists of an isomorphism of $A\otimes A$-modules

$$\Theta:\ M\otimes A \longrightarrow A\otimes M$$

satisfying the compatibility condition that

$$\Theta_0\Theta_2 = \Theta_1 ,$$

i.e., that the diagram

---

*For instance, let $R = k$ be a field and $A = k[x]$. Then $A\otimes A \approx k[x_0,x_1]$. If M is an A-module with support at the point $x = 0$, eg. $M = A/(x)$, then $A\otimes M$ has the x_0-axis as support, while $\mathrm{supp}(M\otimes A)$ is the x_1-axis.

(9)
$$\begin{tikzcd} M\otimes A\otimes A \arrow[rr, "\theta_2"] \arrow[dr, "\theta_1"'] & & A\otimes M\otimes A \arrow[dl, "\theta_0"] \\ & A\otimes A\otimes M & \end{tikzcd}$$

commute,

where θ_i is the map obtained from θ by tensoring with the identity map on A in the i-th position, viz.,

$$\theta_2(m\otimes a\otimes b) = [\theta(m\otimes a)]\otimes b$$

$$\theta_0(a\otimes m\otimes b) = a\otimes[\theta(m\otimes b)] .$$

The map θ_1 is unpleasant to write out, since you have to tensor with A in the middle. It can be written

$$\theta_1(m\otimes a\otimes b) = (1\otimes a\otimes 1)\cdot d_1(\theta(m\otimes b))$$

where the dot indicates scalar multiplication in the $A\otimes A\otimes A$-module $A\otimes A\otimes M$.

<u>Theorem 10:</u> Given an A-module M together with descent data θ (8) , there is an R-module N and an A-isomorphism

$$\phi\colon N_A \longrightarrow M$$

such that the diagram of $A\otimes A$-modules and maps

$$\begin{tikzcd} & N_A\otimes A \arrow[r, "\phi\otimes A"] & M\otimes A \arrow[d, "\theta"] \\ N_{A\otimes A} \arrow[ur, "\approx"] \arrow[dr, "\approx"'] & & \\ & A\otimes N_A \arrow[r, "A\otimes\phi"'] & A\otimes M \end{tikzcd}$$

commutes. The pair (N,ϕ) is determined up to unique isomorphism, in an obvious sense. It will be called the <u>descended module</u>.

Proof: We have the diagram

(11)
$$\begin{tikzcd} M \arrow[rr, "d_0"] \arrow[dr, "d_1"'] & & A\otimes M \\ & M\otimes A \arrow[ur, "\theta"'] & \end{tikzcd} .$$

This is a non-commutative triangle of (at least R-linear) maps. Thus we obtain a pair of maps

$$M \overset{d_0}{\underset{\theta d_1}{\rightrightarrows}} A\otimes M \quad .$$

Following the clue of (6), let K be the kernel of this pair, so that

(12)
$$K \longrightarrow M \overset{d_0}{\underset{\theta d_1}{\rightrightarrows}} A\otimes M$$

is exact. Since d_0, θd_1 are homomorphisms of R-modules, K is an R-module. The inclusion of K in M induces a correspondence map of A-modules

$$\phi: K\otimes A \longrightarrow M \qquad (k\otimes 1 \rightsquigarrow k) ,$$

and our problem is essentially to show that it is bijective.

Now if we tensor (11, 12) on the right by A, we get a diagram of A-modules

$$\begin{tikzcd} K\otimes A \arrow[r] & M\otimes A \arrow[rr, shift left, "d_0"] \arrow[rr, shift right] \arrow[dr, "d_1"'] & & A\otimes M\otimes A \\ & & M\otimes A\otimes A \arrow[ur, "\theta_2"'] & \end{tikzcd} ,$$

the bottom triangle being commutative, where we let A operate on the right. The row is exact, since A is flat over R.

By (6), we also have an exact sequence

$$M \longrightarrow A \otimes M \underset{d_1}{\overset{d_0}{\rightrightarrows}} A \otimes A \otimes M$$

obtained by viewing M as an R-module. If we let A operate on the right again, this is a sequence of A-modules.

The square of A-homomorphisms (operation on the right)

$$\begin{tikzcd} M \otimes A \arrow[r, shift left, "d_0"] \arrow[r, shift right, "\theta_2 d_1"'] \arrow[d, "\theta", "\wr"'] & A \otimes M \otimes A \arrow[d, "\theta_0", "\wr"'] \\ A \otimes M \arrow[r, shift left, "d_0"] \arrow[r, shift right, "d_1"'] & A \otimes A \otimes M \end{tikzcd} \tag{13}$$

commutes if we take the top horizontal arrows. Since the compatibility condition (9) holds, we have

$$\theta_0 \theta_2 d_1 = \theta_1 d_1 = d_1 \theta ,$$

the last equality being clear. Thus (13) again commutes if we take the bottom horizontal arrows, and so θ induces a bijective map of the kernels

$$K \otimes A \xrightarrow{\sim} M .$$

Since θ carries a tensor $k \otimes 1$ to $\theta(k \otimes 1) = 1 \otimes k$ $(k \in K)$, this is just the map ϕ.

From (13), we get a commutative square of A-modules

$$\begin{array}{ccc} K_A & \longrightarrow & M\boxtimes A \\ \Big\downarrow \phi & & \Big\downarrow \phi \\ M & \longrightarrow & A\boxtimes M \end{array} .$$

Recall that the right hand members are viewed as A-modules via d_0, i.e., A operates on the right. Thus we obtain the corresponding diagram of $A\boxtimes A$-modules

$$\begin{array}{ccc} K_{A\boxtimes A} & \longrightarrow & M\boxtimes A \\ \Big\downarrow \phi\boxtimes A & & \Big\downarrow \theta \\ (A\boxtimes A)\boxtimes_A M & \approx & A\boxtimes M \end{array}$$

and it is clear from the fact that the top horizontal arrow is induced by (12) that it is $\phi\boxtimes A$. This shows the commutativity required by the theorem, and proves the existence of $(N,\phi) = (K,\phi)$.

It remains to prove uniqueness: Suppose that (K,ϕ) and (N,ψ) are two solutions, and consider the isomorphism $\varepsilon = \psi^{-1}\phi$

$$\begin{tikzcd} K_A \arrow[rr, "\varepsilon"] \arrow[dr, "\phi"'] & & N_A \arrow[dl, "\psi"] \\ & M & \end{tikzcd}$$

We obtain two maps $K_{A\boxtimes A} \longrightarrow N_{A\boxtimes A}$, by the two structures of A-algebra d_0, d_1 on $A\boxtimes A$, which we may write as $\varepsilon\boxtimes A$ and $A\boxtimes\varepsilon$. The resulting diagram

$$\begin{tikzcd}
 & M\boxtimes A \arrow[dd, "\Theta"'] & \\
K_{A\boxtimes A} \arrow[ur, "\phi\boxtimes A"] \arrow[dr, "A\boxtimes\phi"'] \arrow[rr, bend left=60, "\varepsilon\boxtimes A"] \arrow[rr, bend right=60, "A\boxtimes\varepsilon"'] & & N_{A\boxtimes A} \arrow[ul, "\psi\boxtimes A"'] \arrow[dl, "A\boxtimes\psi"] \\
 & A\boxtimes M &
\end{tikzcd}$$

commutes, hence

(*) $$A\boxtimes\varepsilon = \varepsilon\boxtimes A \quad .$$

Thus we are reduced to proving the following proposition:

<u>Proposition 14:</u> Let X, Y be R-modules. The functorial property of extension of scalars induces from (6') a sequence

$$\mathrm{Hom}_R(X,Y) \longrightarrow \mathrm{Hom}_A(X_A,Y_A) \rightrightarrows \mathrm{Hom}_{A\boxtimes A}(X_{A\boxtimes A},Y_{A\boxtimes A}) \ .$$

This sequence is exact.

For, by (14), the equality (*) implies that the isomorphism ε is induced by extension of scalars from a unique map (necessarily an isomorphism) $K \xrightarrow{\delta} N$, and $\delta_A = \varepsilon$ has the property that

$$\begin{tikzcd}
K_A \arrow[rr, "\delta_A"] \arrow[dr, "\phi"'] & & N_A \arrow[dl, "\psi"] \\
 & M &
\end{tikzcd}$$

commutes, which is clearly what shall be meant by an isomorphism $(K,\phi) \approx (N,\psi)$.

Proof of 14: Let $u: X \longrightarrow Y$ be a map. The extension of scalars is such that the squares of the following diagram commute, where the rows are (6) :

$$\begin{tikzcd} X \arrow[r] \arrow[d, "u"] & X_A \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "u_A"] & X_{A\boxtimes A} \arrow[d, "u_{A\boxtimes A}"] \\ Y \arrow[r] & Y_A \arrow[r, shift left] \arrow[r, shift right] & Y_{A\boxtimes A} \end{tikzcd}$$

Since $Y \longrightarrow Y_A$ is injective, it is clear that u_A determines u . Suppose now that $v: X_A \longrightarrow Y_A$ is a map such that the two induced maps $v\boxtimes A$ and $A\boxtimes v$ from $X_{A\boxtimes A}$ to $Y_{A\boxtimes A}$ are equal. Let us view X as a subset of X_A and Y as a subset of Y_A for the moment. Then to show that v induces a map from X to Y , it suffices to show that v carries X into Y . The induced map will be obviously R-linear. Now because of (6) applied to the module Y , we need only show that for $x \in X$, the element $v(x)$ has the property that

$$d_0 v(x) = d_1 v(x) .$$

But

$$\begin{aligned} d_0 v(x) = (A\boxtimes v)d_0(x) &= (v\boxtimes A)d_0(x) \quad \text{(by assumption)} \\ &= (v\boxtimes A)d_1(x) \quad (\text{since } x \in X) \\ &= d_1 v(x) , \end{aligned}$$

qed.

B. The case of localization.

Let $\{s_i\} \subset R$ be a finite subset which generates the unit ideal. We can interpret the discussion of gluing of modules (3.C) in the context of descent by the following trick:

Let A be the product $A = \prod_i R_i$ $(R_i = R_{s_i})$. Then by (9.B.6) the ring A is a faithfully flat R-algebra. For, Spec A is the disjoint union of the spectra $X_i = \operatorname{Spec} R_i$ (1.E.1), which maps onto $X = \operatorname{Spec} R$ because $\{s_i\}$ generates the unit ideal, and since R_i is flat (4.D.2), so is A (9.A.3). To give an A-module M just amounts to giving a module M_i over each R_i (why? cf. (7.A.7)).

Now $R_i \otimes R_j$ is immediately seen to be canonically identified with the ring $R_{ij} = R_{s_i s_j}$. Since $\otimes$ distributes over products, we have an isomorphism

$$A \otimes A = \left(\prod_i R_i\right) \otimes \left(\prod_j R_j\right) \approx \prod_{i,j} R_{ij} \quad .$$

Thus (A.1) is seen to be equivalent with a diagram

$$\begin{tikzcd}[column sep=huge]
\prod_i R_i \arrow[r, shift left=2, "d_0"] \arrow[r, shift right=2, "d_1"'] & \prod_{i,j} R_{ij} \arrow[l, "s_0"] \arrow[r, shift left=4, "d_0"] \arrow[r, "d_1"] \arrow[r, shift right=4, "d_2"'] & \prod_{i,j,k} R_{ijk} \arrow[l, shift left=2, "s_0"] \arrow[l, shift right=2, "s_1"']
\end{tikzcd} \tag{1}$$

where for instance the operator d_0 carries an element $(\ldots, r_i, \ldots) \in \prod_i R_i$ to the element $(\ldots, a_{ij}, \ldots) \in \prod_{i,j} R_{ij}$ such that $a_{ij} = r_j$. The operator s_0 carries $(\ldots, a_{ij}, \ldots)$

to the element $(\ldots,r_i,\ldots)$ where $r_i = a_{ii}$, etc... The reader should write down explicitly the induced maps of the spectra.

An A-module M (the "collection of R_i-modules M_i") induces two modules over $A \otimes A$, as in (A.7) . Such a module corresponds to giving a collection of modules, one for each R_{ij} , and one sees immediately that the module over R_{ij} yielding $A \otimes M$ is just $R_{ij} \otimes M_j = (M_j)_{s_i}$ while the one giving $M \otimes A$ is $M_i \otimes R_{ij} = (M_i)_{s_j}$. Hence an isomorphism

$$\theta\colon M \otimes A \longrightarrow A \otimes M$$

just means an isomorphism for each i, j

$$\theta_{ij}\colon (M_i)_{s_j} \longrightarrow (M_j)_{s_i}$$

and the compatibility condition (C.9) reads

$$\theta_{jk}\theta_{ij} = \theta_{ik} \quad \text{in} \quad R_{ijk}$$

Thus descent data for M is just the same as gluing data.
<u>Note</u>: I seem unfortunately to have written the compatibility condition (3.C.6) backwards.

<u>C. Descent with extra structure.</u>

In the notation of (A) , let N be an R-module, and suppose, for example, that we are given some A-algebra structure on N_A . Recall that such a structure is given by an A-linear map

$$N_A \otimes_A N_A \longrightarrow N_A \quad ,$$

possibly required to be associative, etc..

Let us ask whether this structure is induced from an R-algebra structure on N .

Now there is a canonical isomorphism

$$N_A \boxtimes N_A \approx (N \boxtimes N)_A \ .$$

Thus we can apply (A.14) , and if we set $X = N \boxtimes N$, and $Y = N$, it tells us that <u>the algebra structure</u>, which is an element of $\mathrm{Hom}_A((N \boxtimes N)_A, N_A)$, <u>is induced by an algebra structure on</u> N <u>iff. the two structures of</u> $A \boxtimes A$-<u>algebra on</u> $N_{A \boxtimes A}$ <u>obtained via</u> d_0, d_1 <u>are equal</u>, and that the algebra structure on N thus determined is unique.

Let us continue the investigation: Suppose the algebra structure on N_A is induced from N , and that N_A is an associative algebra. The associative law for N_A is the assertion that two maps

$$N_A \boxtimes_A N_A \boxtimes_A N_A \longrightarrow N_A$$

(obtained in the usual way from the multiplication) are equal. Thus, again by (A.14) , the associative law for N_A implies it for N , and conversely. Similarly, N_A is commutative iff. N is. Moreover, N_A has an identity iff. N does. For, an identity in N is an element $e \in N$ such that $en=ne=n$ for all $n \in N$. It is unique. If there is an identity e in N_A , its two images in $N_{A \boxtimes A}$ under d_0, d_1

are both identities for that algebra, hence are equal, and so the element e came from N, by (A.6). It is immediately seen that it is an identity in N.

This discussion has the following important corollary:

Corollary 1: With notation as in (A.10), let M be an A-algebra, and let descent data

$$\Theta\colon M\otimes A \longrightarrow A\otimes M$$

be given. Assume that Θ is an isomorphism of $A\otimes A$-algebras, between the structures induced from M on the two modules. Then the descended module (A.10) N has a unique structure of R-algebra making ϕ into an algebra isomorphism. The structure is associative, or commutative, or with identity, etc..., iff. N_A is.

For, the isomorphism $\phi\colon N_A \longrightarrow M$ induces an A-algebra structure on N_A, which is associative etc.. iff. M is. By the above discussion, we need only check that the two structures of $A\otimes A$-algebra induced on $N_{A\otimes A}$ via d_0, d_1 are equal. But this is just the fact that Θ is an algebra isomorphism, combined with the commutative diagram of (A.10). The induced structure on N_A is such that the diagram

$$(*)\qquad \begin{array}{ccc} (N\otimes N)_A \approx N_A \otimes_A N_A & \longrightarrow & N_A \\ \phi\otimes_A\phi \Big\downarrow & & \Big\downarrow \phi \\ M\otimes_A M & \longrightarrow & M \end{array}$$

where the horizontal arrows are the laws of composition. Extending scalars to A via d_0, d_1, we get a diagram

$$(**)\qquad \begin{tikzcd}
 & (N\otimes N)_{A\otimes A} \arrow[dl] \arrow[d] & & & N_{A\otimes A} \arrow[dl, "\phi\otimes A"'] \arrow[dd, "A\otimes\phi"] \\
(M\otimes_A M)\otimes A \arrow[rrr] \arrow[dr] & A\otimes(M\otimes_A M) \arrow[d, phantom] & & M\otimes A \arrow[dr, "\theta"] & \\
 & A\otimes(M\otimes_A M) \arrow[rrr] & & & A\otimes M
\end{tikzcd}$$

in which the horizontal arrows are the laws of composition, and where we leave it to the reader to label the arrows on the left. The bottom square commutes since θ is an algebra isomorphism. The triangles commute because they are the diagram of (A.10) for the descent data $\theta\otimes_A\theta$ and θ, respectively. Tensoring $(*)$ by A on the left (resp. right) gives the induced structure on $N_{A\otimes A}$, and makes the appropriate square obtained in $(**)$ commute. Thus it follows that the two structures are equal.

It is clear that the above discussion would apply equally well for other types of structure, such as that of co-algebra, etc... but we are not going to state a result formally.

D. Twisted forms of a structure.

Suppose we are given an R-module N, let us say with some extra structure (such as: no extra structure, or the structure of associative R-algebra, etc...) to which a discussion analogous to (c) applies. We will denote the given structure in a neutral way by S. Then we can use the symbol S_A to denote the structure over A induced by extension of scalars, and so on. In the notation of (A), consider the following problem:

Determine all structures (of the same type) S' *over* R, *such that* S'_A *is isomorphic with* S_A.

Such a structure S' will be called a *twisted form* of S relative to the extension $R \longrightarrow A$.

Using the technique of descent, we can in principal reduce this problem to a calculation involving the automorphisms of the objects involved. The discussion is analogous to that of (3.D):

Let S' be a twisted form of S. By assumption, there is an isomorphism

$$u\colon S_A \longrightarrow S'_A .$$

Now if $A \xrightarrow{\alpha} B$ is a ring homomorphism, an isomorphism $u\colon S_A \longrightarrow S'_A$ induces in an obvious way by extension of scalars an isomorphism $S_B \longrightarrow S'_B$. Let us denote it by $\alpha{*}u$. Since $A \boxtimes A$ is an A-algebra in two ways, we obtain two isomorphisms

$$S_{A\boxtimes A} \underset{d_1 * u}{\overset{d_0 * u}{\rightrightarrows}} S'_{A\boxtimes A} .$$

Put

(1) $$\Theta = (d_0{*}u)^{-1}(d_1{*}u) \quad .$$

It is an automorphism of $S_{A\boxtimes A}$. Then using the identities $d_0d_1 = d_2d_0$, etc... (cf. (A.2)) , we find

(2) $$\Theta_0\Theta_2 = (d_0{*}\Theta)(d_2{*}\Theta) = (d_1{*}\Theta) = \Theta_1 \quad ,$$

i.e., Θ is descent data (A.8) for the structure S_A over A . For,

$$\begin{aligned}(d_0{*}\Theta)(d_2{*}\Theta) &= [(d_0d_0){*}u^{-1}(d_0d_1){*}u][(d_2d_0){*}^{-1}u(d_2d_1){*}u]\\ &= (d_0d_0){*}u^{-1}(d_2d_1){*}u\\ &= (d_1d_0){*}u^{-1}(d_1d_1){*}u\\ &= (d_1{*}\Theta) \ .\end{aligned}$$

Clearly, the descended structure (C) obtained from the descent data Θ can be none other than (S',u) .

To eliminate the choice of the map u , suppose u' is another, yielding descent data Θ' . Then if we let

$$g = u'^{-1}u$$

be the resulting automorphism of S_A , so that $u' = ug^{-1}$ we find

$$\Theta' = (d_0{*}u')^{-1}(d_1{*}u')$$

(3) $$= (d_0{*}g)(d_0{*}u)^{-1}(d_1{*}u)(d_1{*}g)^{-1}$$

$$= (d_0{*}g)\Theta(d_1{*}g)^{-1} \ .$$

<u>Corollary 4:</u> The twisted forms of a structure S over R, relative to the map $R \longrightarrow A$, are in one-one correspondence with equivalence classes of automorphisms Θ of $S_{A\otimes A}$ satisfying the condition (2), two such automorphisms Θ, Θ' being equivalent if there is an automorphism g of S_A such that

$$\Theta' = (d_0 * g)\, \Theta\, (d_1 * g)^{-1} .$$

This is immediate. It is not even necessary to make the (trivial) verification that the relation is an equivalence relation.

One customarily denotes the set of equivalence classes introduced above by

(5) $$H^1(A/R, \underline{\mathrm{Aut}}\ S)$$

which is to be read as "1-cohomology of the extension $R \longrightarrow A$ with values in $\underline{\mathrm{Aut}}\ S$". To make sense of this, it has to be understood that $\underline{\mathrm{Aut}}\ S$ is the <u>functor</u>

(6) $$\underline{\mathrm{Aut}}\ S\colon (R\text{-algebras}) \longrightarrow (\text{groups})$$

defined by

(6) $$\underline{\mathrm{Aut}}\ S[B] = (\text{group of automs. of the structure } S_B) .$$

We can in fact define the 1-cohomology

$$H^1(A/R, G)$$

of the extension $R \longrightarrow A$ with values in any <u>functor</u>

$$G\colon (\text{R-algebras}) \longrightarrow (\text{groups}) .$$

It is just the set of equivalence classes of elements

$$\Theta \in G[A\otimes A]$$

such that the induced elements $d_i{*}\Theta \in G[A\otimes A\otimes A]$ (induced by the map d_i because G is a functor) satisfy the identity

$$(d_0{*}\Theta)(d_2{*}\Theta) = (d_1{*}\Theta) ,$$

where two such elements Θ, Θ' are called equivalent if there is a $g \in G[A]$ such that

$$\Theta' = (d_0{*}g)\ \Theta\ (d_1{*}g)^{-1} .$$

The set $H^1(A/R,G)$ has a structure of abelian group if G has its values in abelian groups.

E. Some examples.

Suppose that we ask for twisted forms of a free module F of rank n over R, relative to the extension $R \longrightarrow A$. The group of automorphisms of a free module of rank n over a ring B is the group $Gl_n[B]$ of invertible $n{\times}n$-matrices with entries in B. The corresponding functor on R-algebras will be denoted

(1) $$\underline{Gl}_n\colon (\text{R-algebras}) \longrightarrow (\text{groups})$$
$$B \rightsquigarrow Gl_n[B] .$$

If $n=1$, it is the functor

(2) "units": $B \rightsquigarrow B^*$

which is often denoted by G_m = multiplicative group.

The recipe (D.4,5) tells us that exactly as in (3.D,E)

Corollary 3: The twisted forms of a free module of rank n relative to $R \longrightarrow A$ are classified by

$$H^1(A/R, \underline{Gl}_n) .$$

This example is not of too much interest. For, it follows from ((.A.11) and (9.B.7) that such a twisted form is always locally free. Hence we do not get any more twisted forms from general faithfully flat extensions than we would by the process localization discussed in (3.D) .

Since every locally free module over a field is free, there are no twisted forms when R is a field. Thus we obtain a statement which is one version of what is known as "Hilbert's theorem 90":

Corollary 4: Let L/K be a field extension. Then

$$H^1(L/K, \underline{Gl}_n) = 0 .$$

In particular,

$$H^1(L/K, \text{units}) = 0 .$$

More generally, let R be a local (or even semi-local (cf. (exerc. No. 2, Prob. 3d)) ring, and A any faithfully flat extension. Then

$$H^1(A/R, \underline{Gl}_n) = 0 .$$

A more interesting example is that of the $n{\times}n$-*matrix algebra* over R, let us denote it by $M_n[R]$. Its twisted forms are classified by

(5) $$H^1(A/R, \underline{Aut}\ M_n)$$

where $\underline{Aut}\ M_n$ is the functor

$$B \rightsquigarrow (\text{group of autos. of the matrix algebra } M_n[B]) .$$

Fortunately, a great deal is known about this functor. Suppose $R = K$ is a field. Then the Skolem-Noether theorem asserts that every automorphism of $M_n[K]$ is *inner*, i.e., is obtained by conjugating with an invertible matrix from K. Thus $Gl_n[K]$ maps onto $\underline{Aut}\ M_n[K]$. The kernel of this map is the group of units of the *center* of the matrix algebra, which is just K^*, identified with the group of diagonal matrices $a \cdot I$ ($a \in K^*$ and I the identity matrix). Thus we obtain an exact sequence

(6) $$0 \longrightarrow K^* \longrightarrow \underline{Gl}_n[K] \longrightarrow \underline{Aut}\ M_n[K] \longrightarrow 0 .$$

The group $\underline{Gl}_n/(\text{center})$ is called the *projective general linear group*, and is often denoted by $\underline{PGl}_n$, whence

$$\underline{Aut}\ M_n[K] = \underline{PGl}_n[K] .$$

For a general ring R, the sequence corresponding to (6) is no longer exact. However, it can be shown that the sequence of <u>sheaves</u> on $X = \text{Spec } R$, defined in an evident way,

$$(7) \qquad 0 \longrightarrow \tilde{R}^* \longrightarrow \widetilde{\underline{Gl}}_n \longrightarrow \widetilde{\underline{PGl}}_n \longrightarrow 0$$

is still exact, and that $\underline{PGl}_n = \underline{Aut}\ M_n$. Thus from the exact cohomology sequence (4,C,3), the extent to which exactness fails is measured by $H^1(X,\tilde{R}^*)$ = group of locally free rank one modules over R.

Suppose that $R = K$ is a field, and let us apply the Wedderburn theory of simple rings: Some corollaries of this theory are that if M' is a finite dimensional simple algebra over K with center K, then the algebra M'_L induced by extension of scalars to a field L/K is again simple, and it has center L. Moreover, the only such algebras are the matrix algebras, when the field is algebraically closed. It is not difficult to show that if, conversely, M' is a K-algebra such that M'_L is simple and central over L, then M' is also simple and central over K. This can be shown by arguments of the type which we discussed in (C); the proof is left as an instructive exercise for the reader. Therefore, these central, simple algebras over K are just twisted forms of the matrix algebra $M_n[K]$, relative to the extension $K \longrightarrow \overline{K}$ ($\overline{K}$ an algebraic closure of K):

Corollary 8: The twisted forms of the matrix algebra $M_n[K]$ relative to the extension $K \longrightarrow \bar{K}$ are the central, simple algebras over K of rank n^2.

Twisted matrix algebras over other rings are of considerable importance. They are called Azumaya Algebras. The interested reader can consult the original papers of Azumaya (Nagoya M. J. (1951)) and Auslander-Goldman (Transactions (1960)), or he can profit by working exercises 13-17, Ch. II, §5 of Bourbaki, Alg. Comm.

As a third example, consider the R-algebra $R^n = R \times \cdots \times R$ (n copies), where R operates by scalar multiplication on a "vector" $(a_1, \ldots, a_n) \varepsilon R^n$, and the addition and multiplication of vectors is component-wise. Suppose to begin with that R has no non-trivial idempotents (i.e., none other than $0,1$). Then $R \times \cdots \times R$ has only the idempotents $e_1 = (1,0,\ldots,0)$, $\ldots$, $e_n = (0,\ldots,0,1)$ (why?). An R-automorphism ϕ of the algebra R^n must permute these idempotents. Since every vector is of the form

$$(a_1, \ldots, a_n) = \sum_i a_i e_i \quad (a_i \varepsilon R) ,$$

we have

$$\phi(a_1, \ldots, a_n) = \sum_i a_i \phi(e_i) .$$

Hence the automorphism ϕ is determined when the permutation of e_i is given. Conversely, any permutation of e_i

gives rise to an automorphism ϕ .

If R has finitely many idempotents $\{\varepsilon_\nu\}$, so that R is a product of rings $R = \prod R_\nu$, in a canonical way (equivalently, (1.E), Spec $R = X$ is a disjoint union of a finite number of connected components), then it is easily seen that the automorphism ϕ can be described by a permutation of each of the sets of idempotents $e_{\nu 1},\dots,e_{\nu n}$ where $e_{\nu i} = (0,\dots,\varepsilon_\nu,0,\dots)$ (ε_ν in the i-th position). Thus the group of automorphisms of the algebra R^n is canonically isomorphic to the product

$$(S_n)^c ,$$

where $c = c(R)$ denotes the set of connected components of Spec R , and $(S_n)^c$ is the product of copies of the symmetric group S_n indexed by the elements of $c(R)$.

It follows that if $R \longrightarrow A$ is an extension (f. flat) such that A , $A\otimes A$, ... each have only finitely many idempotents (eg. if they are all noetherian rings), then the twisted forms of the algebra R^n relative to the extension $R \longrightarrow A$ are classified by

$$H^1(A/R, \underline{S}_n) \tag{9}$$

where $\underline{S}_n$ is the rule

$$B \rightsquigarrow \underline{S}_n[B] = (S_n)^{c(B)} .$$

We leave it to the reader to describe how this is made into a functor.

Such a twisted form of R^n is analogous to a covering space in topology; the spectrum of R^n is

$$\operatorname{Spec} R^n = X \amalg \dots \amalg X \quad \text{(n copies)}$$

where $X = \operatorname{Spec} R$, i.e., is the "trivial n-sheeted covering of X". Note the striking fact that the classification (8) depends only on the sets of connected components of the spectrum of the algebra A and of its tensor powers.

If $R = K$ is a field, then any finite separable field extension L/K decomposes completely when tensored with a splitting field L' containing it. This is because the polynomials whose roots are adjoined to obtain the extension L split completely in L'. Thus L is an example of a twisted form of K^n, if $[L:K] = n$. It is a good exercise for the reader to prove that the twisted forms of K^n (relative to various extensions) are exactly the separable algebras (products of separable field extensions) over K of rank n. (This was a homework problem in 18.731.)

<u>Remark 10:</u> If L/K is a galois extension, then $L \otimes L$ decomposes into n copies of L, $n=[L:K]$. Thus automorphisms of a structure over $S_{L \otimes L}$ will just be n-tuples of automorphisms of the corresponding structure S_L over L. Using this fact, one can express the cohomology (F.5)

$$H^1(L/K, \underline{\operatorname{Aut}}\, S)$$

as the cohomology of the <u>group</u> $G(L/K)$ operating on <u>Aut</u> $S[L]$.

We leave it to the reader who is familiar with cohomology of groups to work out this identification.

Some aspects of this discussion have been treated in detail by Harrison, Chase, Rosenberg (AMS Memoir, No. 52, 1965).

Tensor Products

A. The universal property of tensor products.

Let R be a commutative ring with unit, and let X, Y, Z be R-modules. A bilinear map

$$f: X \times Y \to Z$$

is one satisfying

$$\begin{aligned} f(x+x',y) &= f(x,y) + f(x',y) \ , \\ f(rx,y) &= rf(x,y) \ , \\ f(x,y+y') &= f(x,y) + f(x,y') \ . \\ f(x,ry) &= rf(x,y) \ . \end{aligned}$$

We want to relate bilinear maps to linear ones (i.e., homoms. of modules). This will be done by constructing a certain R-module called the tensor product $X \otimes Y$ of X and Y. The tensor product has the following characteristic property:

"There is a natural 1-1 correspondence between homomorphisms of $X \otimes Y$ to an R-module Z and bilinear maps $X \times Y \to Z$."

More precisely, we will construct not only an R-module $X \otimes Y$ but also a bilinear map

$$t: X \times Y \longrightarrow X \otimes Y \ ,$$

denoted by

$$(x,y) \rightsquigarrow x \otimes y \ .$$

(The image element $x \otimes y$ is called the tensor product of the elements x, y.) This bilinear map is universal in the following sense:

Given an R-module Z and an R-homom. $\phi: X \otimes Y \to Z$, we can construct a bilinear map

$$f: X \times Y \longrightarrow Z$$

by

$$f(x,y) = \phi(x \otimes y) \qquad \text{(verify axioms)},$$

i.e., by composing the maps ϕ and t:

$$\begin{tikzcd} X \times Y \arrow[r, "t"] \arrow[dr, "\phi t = f"'] & X \otimes Y \arrow[d, "\phi"] \\ & Z \end{tikzcd}$$

Thus we get a map

$$\mathrm{Hom}_R(X \otimes Y, Z) \xrightarrow{\text{"}\circ t\text{"}} \text{Bilin. Maps }(X \times Y, Z).$$

The universal property is that this map is bijective, i.e., that every bilinear map $f: X \times Y \to Z$ is obtained in exactly one way from such a ϕ.

Notice that the "tensors" $x \otimes y$ must satisfy (in order that t be bilinear)

Rules:
$$\begin{aligned} (x+x') \otimes y &= x \otimes y + x' \otimes y \\ (rx) \otimes y &= r(x \otimes y) \\ x \otimes (y+y') &= x \otimes y + x \otimes y' \\ x \otimes (ry) &= r(x \otimes y). \end{aligned}$$

These identities are used in the construction. They should be contrasted with those holding in the direct sum $X \oplus Y \simeq X \times Y$. If we denote the pair (x,y) by $x \oplus y$, then the module structure on $X \oplus Y$ yields

$$(x+x') \oplus (y+y') = (x \oplus y) + (x' \oplus y')$$

$$(rx) \oplus (ry) = r(x \oplus y) .$$

Thus we are looking for a completely different module.

Before constructing $X \otimes Y$, we will prove its uniqueness:

Prop: Let T, T' be two constructions having the universal property of $X \otimes Y$. Then T, T' are naturally isomorphic.

proof: By assumption, T, T' are R-modules and we are given bilinear maps t, t' from $X \times Y$ to T, T' respectively. Since t is universal there exists a unique homomorphism $\phi: T \to T'$ such that $t' = \phi \circ t$. Since t' is universal there exists a unique $\phi': T' \to T$ such that $t = \phi' \circ t'$. Then $t = (\phi' \circ \phi) \circ t$. Also $t = (\mathrm{id}) \circ t$. But the universal property says that a given bilinear f (in this case, $f = t$) can be obtained in only one way as $\phi \circ t$ (in this case, ϕ is $\phi' \circ \phi$ or id). Therefore

$$\phi' \circ \phi = \mathrm{id} .$$

This shows that ϕ , ϕ are isomorphisms.

B. Construction of tensor product.

The construction is a "cheat".

Let S be any set. We will first construct an R-module $F(S)$ = "the free module on the set S". The elements of $F(S)$ shall consist of formal linear combinations of elements of S with coefficients in R, i.e., equivalence classes of expressions of the form

$$(*) \qquad \sum_{i=1}^{n} r_i s_i \qquad r_i \in R \ , \ s_i \in S \ \text{ and } \ s_i \ \text{ all distinct}$$

subject to the "obvious" conditions needed to insure that the elements $\{1\cdot s \mid s\in S\}$ will form a (lin. indep.) basis of $F(S)$. To construct $F(S)$ formally, it is convenient to view (*) as associating to the element $s_i \in S$ a "coefficient" $r_i \in R$. We associate the coefficient zero to any $s \in S$ not appearing in (*). Thus the expression (*) corresponds to a map $S \longrightarrow R$ ($S \rightsquigarrow$ its coefficient) such that all but a finite number of elements of S get mapped to zero. Hence

<u>Definition</u>: Let S be a set. The set of maps $S \to R$, Maps (S,R) is an R-module by addition and scalar multiplication of functions:

$$[f+g](s) = f(s) + g(s)$$

$$[rf](s) = r(f(s)) \ .$$

Let $F(S) \subset$ Maps (S,R) be the subset consisting of those maps such that all but a finite number of elements of S get mapped to zero. $F(S)$ is a submodule of Maps (S,R) , and is called the <u>free module on the set</u> S .

$F(S)$ has the following universal property:
"Maps from S to an R-module Z are in 1-1 correspondence with homomorphisms from $F(S)$ to Z ."
More precisely, there is an injective map $i: S \to F(S)$ given by $s \rightsquigarrow$ "the map sending s to 1 , all other elements to zero in R". (We will denote $i(s)$ just by s .) There-

fore, we get

$$\mathrm{Hom}_R\ (F(S),\ Z) \longrightarrow \mathrm{Maps}\ (S,Z)$$

by

$$\phi \rightsquigarrow \phi \circ i \quad .$$

This map is <u>bijective</u>, i.e., every $f\colon S \to Z$ arises in <u>exactly</u> <u>one</u> <u>way</u> as $f = \phi \circ i$, $\phi\colon F(S) \to Z$ a homom. In fact, if $f\colon S \to Z$ is any map, define $\phi\colon F(S) \to Z$ by

$$\phi\ (\sum_\nu r_\nu s_\nu) \ = \ \sum_\nu r_\nu f(s_\nu)$$

since $\{s \in S\}$ form a (lin. indep.) basis for $F(S)$, this is well defined. Clearly $f = \phi \circ i$, and clearly ϕ is uniquely determined.

Now to define $X \otimes Y$, consider the submodule M of $F(X \times Y)$ generated by elements of the form

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

$$(rx,y) - r(x,y)$$

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

$$(x,ry) - r(x,y) \quad \text{with} \quad x,x' \in X \ , \ y,y' \in Y \ , \ r \in R$$

(these are all linear combinations of elts. of $X \times Y$). Set $X \otimes Y = F(X \times Y)/M$, and let $t\colon X \times Y \to X \otimes Y$ be the composition of $i\colon X \times Y \to F(X \times Y)$ with the canonical map

$$\varepsilon\colon F(X \times Y) \longrightarrow F(X \times Y)/M = X \otimes Y \quad .$$

Then for $x,x' \in X$, $y \in Y$

$$(x+x',y) - (x,y) - (x',y) \ \in M \text{ , hence}$$

$$t(x+x',y) - t(x,y) - t(x',y) = 0 \quad , \quad \text{i.e.}$$

$$t(x+x',y) = t(x,y) + t(x',y) \quad .$$

The other axioms for a bilinear map are verified in the same way. Hence t is bilinear. Now let $f: X \times Y \to Z$ be any bilinear map. f is a map, hence $f = \phi \circ i$ for some unique homom. $\phi: F(X \times Y) \to Z$. Since f is bilinear,

$$\begin{aligned} &\phi[(x+x',y) - (x,y) - (x',y)] \\ &= \phi(x+x',y) - \phi(x,y) - \phi(x',y) \\ &= f(x+x',y) - f(x,y) - f(x',y) \\ &= 0 . \qquad \text{etc. } \ldots . \end{aligned}$$

Therefore, $M \subset$ kernel of ϕ. So by the universal property of $F(X \times Y)/M$, there is a unique map $\overline{\Phi}: X \otimes Y \to Z$ such that

$$\phi = \overline{\Phi} \circ \varepsilon \quad .$$

Then

$$f = \phi i = \overline{\Phi}\, \varepsilon\, i = \overline{\Phi} t \quad .$$

Hence f is induced by a homom. $\overline{\Phi}: X \otimes Y \to Z$. The uniqueness of $\overline{\Phi}$ follows immediately from the uniqueness of ϕ. This shows that $X \otimes Y$ has the desired universal property, and completes the construction.

C. Elementary properties.

1) The tensors of the form $x \otimes y$ generate $X \otimes Y$, i.e., every element of $X \otimes Y$ is of the form $\Sigma(x_i \otimes y_i)$.

In fact, the images of $X \times Y$ generate $F(X \times Y)$, hence a fortiori $X \otimes Y$. However, the tensors $x \otimes y$ are not independent, as the rules show.

2) (commutativity). $X \otimes Y$ and $Y \otimes X$ are canonically isomorphic.

The isomorphism sends $x \otimes y$ to $y \otimes x$. It can be constructed first as $F(X \times Y) \xrightarrow{\approx} F(Y \times X)$. Another approach is to notice that the map $X \times Y \to Y \otimes X$ given by $(x,y) \rightsquigarrow y \otimes x$ is bilinear,

3) $R \otimes X \approx X \quad (\approx X \otimes R)$.

Consider the map $R \times X \to X$

$$(r,x) \rightsquigarrow rx \quad .$$

It is clearly bilinear, hence is induced by a map $R \otimes X \to X$. On the other hand, there is the linear map

$$X \longrightarrow R \otimes X$$

$$x \rightsquigarrow 1 \otimes x \quad .$$

These are easily seen to be inverses of each other.

4) (distributivity). Let x, x', y, y' be R-modules. There are natural isomorphisms

$$(X \otimes Y) \oplus (X' \otimes Y) \xrightarrow{\approx} (X \oplus X') \otimes Y$$

and

$$(X \otimes Y) \oplus (X \otimes Y') \xrightarrow{\approx} X \otimes (Y \oplus Y') \quad .$$

To verify for instance the first, notice that the bilinear map $(X \oplus X') \times Y \longrightarrow (X \oplus X') \otimes Y$ gives bilinear maps $X \times Y \longrightarrow (X \oplus X') \otimes Y$

and $X' \times Y \longrightarrow (X \oplus X') \otimes Y$

by

$(x,y) \rightsquigarrow (x,0) \otimes y$

and $(x',y) \rightsquigarrow (0,x') \otimes y$.

Hence we get

$$X \otimes Y \longrightarrow (X \oplus X') \otimes Y \text{ sending } x \otimes y \text{ to } (x,0) \otimes y$$

$$X' \otimes Y \longrightarrow (X \oplus X') \otimes Y \text{ sending } x' \otimes y \text{ to } (0,x') \otimes y \,.$$

Therefore

$$(X \otimes Y) \oplus (X' \otimes Y) \longrightarrow (X \oplus X') \otimes Y \quad .$$

Now consider the map

$$(X \oplus X') \times Y \longrightarrow (X \otimes Y) \oplus (X' \otimes Y)$$

given by

$$((x,x'),y) \rightsquigarrow (x \otimes y \,,\, x' \otimes y) \quad .$$

It is clearly bilinear, hence there is a map

$$(X \oplus X') \otimes Y \longrightarrow (X \otimes Y) \oplus (X' \otimes Y)$$

inducing it, sending

$$((x,x') \otimes y) \rightsquigarrow (x \otimes y \,,\, x' \otimes y) \,.$$

Clearly the two maps are inverses of each other, hence isomorphisms.

5) Suppose X, Y are free modules with bases $\{x_i\}$ $(i = 1,\ldots,m)$ and $\{y_j\}$ $(j = 1,\ldots,n)$. Then $X \otimes Y$ is free with basis $\{x_i \otimes y_j\}$.

For, let U be a free module with basis $\{u_{ij}\}$ $i = 1,\ldots,m$; $j = 1,\ldots,n$. Let $f\colon X \times Y \to U$ be the map sending $(\Sigma\, r_i x_i \,,\, \Sigma\, r'_j y_j)$ to $\sum_{i,j} r_i r'_j u_{ij}$. Since $\{x_i\}$, $\{y_j\}$ are bases, this is well defined. The map is bilinear, and so gives a map

$$X \otimes Y \longrightarrow U$$

sending

$$x_i \otimes y_j \rightsquigarrow u_{ij} \quad .$$

Since the $\{u_{ij}\}$ are lin. indep., it follows that $\{x_i \otimes y_j\}$ are lin. indep. They generate $X \otimes Y$ because of (1) and the rules, hence form a basis.

6) If U, V are vector spaces over F of dimensions m, n respectively, then $U \otimes V$ has dimension mn.

7) (functorality). Let X, X', Y, Y' be R-modules and $\alpha: X \to X'$, $\beta: Y \to Y'$ be homomorphisms. There is a unique homom. "$\alpha \otimes \beta$": $X \otimes Y \to X' \otimes Y'$ mapping $x \otimes y \rightsquigarrow \alpha(x) \otimes \beta(y)$. Since $X \otimes Y$ is generated by the tensors, the uniqueness is clear. To construct $\alpha \otimes \beta$, one may first construct a map $F(X \times Y) \to F(X' \times Y')$. Another way is to note that the map

$$(\alpha,\beta): X \times Y \longrightarrow X' \times Y'$$
$$(x,y) \rightsquigarrow (\alpha(x), \beta(y))$$

when composed with $t': X' \times Y' \to X' \otimes Y'$ gives a bilinear map

$$X \times Y \longrightarrow X' \otimes Y' ,$$

hence a homomorphism

$$X \otimes Y \longrightarrow X' \otimes Y' .$$

8) Let $M \subset X$, $N \subset Y$ be submodules, and

$$\overline{X} = X/M , \quad \overline{Y} = Y/N .$$

Then there is a natural isomorphism

$$(X \otimes Y)/W \xrightarrow{\sim} \overline{X} \otimes \overline{Y}$$

where W is the submodule of $X \otimes Y$ generated by tensors of the form $m \otimes y$ or $x \otimes n$, where $m \in M$, $n \in N$.

The map $X \otimes Y \to \overline{X} \otimes \overline{Y}$ given by (7) (it sends $x \otimes y$ to $\overline{x} \otimes \overline{y}$, where $\overline{x}$ = residue of x and $\overline{y}$ = residue of y)

has any tensor $m \otimes y$ or $x \otimes n$ in the kernel. Hence there is an induced map

$$\varepsilon: (X \otimes Y)/W \longrightarrow \overline{X} \otimes \overline{Y} .$$

We need to show it is an isomorphism. Consider the map

$$\delta: \overline{X} \times \overline{Y} \longrightarrow (X \otimes Y)/W$$

given by

$$(\overline{x},\overline{y}) \rightsquigarrow \text{"residue of } x \otimes y \text{ (mod } W)\text{"}, \text{ where}$$

x, y are coset representatives of $\overline{x}$, $\overline{y}$ respectively. If x', y' are other coset representatives of $\overline{x}$, $\overline{y}$, so that

$x' - x \in M$ (say $x'-x = m$)

$y' - y \in N$ (say $y'-y = n$)

then

$$\begin{aligned} x \otimes y - x' \otimes y' &= (x-x') \otimes y + x' \otimes (y-y') \\ &= m \otimes y + x' \otimes n \in W . \end{aligned}$$

Therefore $x \otimes y \equiv x' \otimes y'$ (mod W). This shows the map δ is well defined. It is obviously bilinear, and so induces a map $\overline{X} \otimes \overline{Y} \longrightarrow (X \otimes Y)/W$ which is the inverse of ε. Therefore ε is an isomorphism.

9) Let U, V, U', V' be vector spaces over F with bases $\{u_i\}$, $\{v_j\}$, $\{u'_i\}$, $\{v'_j\}$ respectively. Let $T: U \to V$, $T': U' \to V'$ be linear transformations. Let $A = (a_{ij})$, $B = (b_{i'j'})$ be the matrices for T, T' w.r.t. the given bases. Then the matrix for $T \otimes T': U \otimes U' \to V \otimes V'$ w.r.t. the bases $\{u_i \otimes u'_{i'}\}$, $\{v_j \otimes v'_{j'}\}$ is $C = (c_{(i,i')(j,j')})$ where

$$c_{(i,i'),(j,j')} = a_{ii'} b_{jj'}$$

i.e.,

$$T \otimes T'(u_i \otimes u'_{j'}) = \sum_{(j,j')} a_{ii'} b_{jj'} (v_j \otimes v'_{j'}) \ .$$

The matrix C is called the Kronecker product of A, B. To write it in a rectangular array, it is necessary to choose an ordering for the sets of pairs of indices $\{(i,i')\}$ and $\{j,j'\}$. The "lexicographic" order is usual.

10) (associativity). If W, X, Y are three R-modules then there is a unique isomorphism $W \otimes (X \otimes Y) \approx (W \otimes X) \otimes Y$, carrying $w \otimes (x \otimes y)$ to $(w \otimes x) \otimes y$.

This means that when considering tensor products of several factors, we can ignore the parentheses. To construct the isomorphism, it is best to show that both have the following universal property (you insert parentheses).

The map
$$t: W \times X \times Y \longrightarrow W \otimes X \otimes Y$$
$$(w,x,y) \rightsquigarrow w \otimes x \otimes y$$
is trilinear (i.e.,

$$(w+w') \otimes x \otimes y = w \otimes x \otimes y + w' \otimes x \otimes y \text{ etc. } \ldots),$$

and the map

$$\mathrm{Hom}_R(W \otimes X \otimes Y, Z) \longrightarrow \text{Trilin. Maps } (W \times X \times Y, Z)$$

obtained by composing with t is bijective. As in Section A, this universal property characterizes $W \otimes X \otimes Y$ up to isomorphism.

In the same way, homomorphisms from a tensor product of n modules to Z correspond to n-multilinear maps to Z.

D. Extension of ring of operators of a module.

Let R, R' be commutative rings, and let $\varphi: R \to R'$ be a homomorphism. Recall (supp. notes I) that every R'-module M' can be made into an R-module by

$$r \cdot m = \varphi(r)m \quad .$$

Let M be an R-module, and consider the R-module $R' \otimes M$ (R' is an R-module, cf. supp. notes IB3). It can be given the structure of R'-module as follows:

The map $R' \times R' \times M \longrightarrow R' \otimes M$

sending $(r', s', m) \rightsquigarrow r's' \otimes m$

is clearly trilinear (verify!) . Hence if r' is fixed, the map

$$R' \times M \longrightarrow R' \otimes M$$
$$(s', m) \rightsquigarrow r's' \otimes m$$

is bilinear, and defines a map

$$R' \otimes M \longrightarrow R' \otimes M$$

sending

$$s' \otimes m \rightsquigarrow r's' \otimes m \quad .$$

Hence letting r' vary again, we get a map

$$R' \times (R' \otimes M) \longrightarrow (R' \otimes M)$$

which sends

$$(r', s' \otimes m) \rightsquigarrow (r's' \otimes m) \quad .$$

I claim this law of composition makes $R' \otimes M$ into an R'-module. We need to check the associativity, distributivity, etc.

For instance,

$$[r_1'+r_2']\cdot(s' \otimes m) = ((r_1'+r_2')s) \otimes m$$
$$= r_1's \otimes m + r_2's \otimes m$$
$$= r_1'\cdot(s \otimes n) + r_2'\cdot(s \otimes m) \quad .$$

We list a few properties:

(1) (Characteristic property). Let M be an R-module and M' an R'-module. Consider the map $\varepsilon\colon M \longrightarrow R' \otimes M$ given by $m \rightsquigarrow 1_{R'} \otimes m$. This map is an R-homomorphism. If $f'\colon R' \otimes M \to M'$ is any R'-homomorphism, then $f'\varepsilon\colon M \to M'$ is immediately seen to be an R-homomorphism. Thus we get the map "compose with ε"

$$\mathrm{Hom}_{R'}(R' \otimes M, M') \longrightarrow \mathrm{Hom}_R(M, M') \quad .$$

<u>This map is bijective.</u>

The property says roughly that the operation of viewing M' as R-module by letting R operate through ϕ (restriction of scalars), and that of constructing $R' \otimes M$ (extension of scalars) are "opposite". One actually says they are <u>adjoint</u>.

To prove the bijectivity of the map, let $f\colon M \to M'$ be an R-homomorphism, and consider the map

$$R' \times M \longrightarrow M'$$
$$(r',m) \rightsquigarrow r'f(m) \quad .$$

It is bilinear, hence gives a map

$$f'\colon R' \otimes M \longrightarrow M'$$

sending $r' \otimes m \rightsquigarrow r'\cdot f(m)$. Clearly $\varepsilon f' = f$. Therefore every f is of the form $\varepsilon f'$ for some $f'\colon R' \otimes M \to M'$. We leave the uniqueness of f' as an exercise.

(2) (Comparison with supp. notes ID.). Suppose $R' = R/I = \bar{R}$ where I is an ideal. Then $\bar{R} \otimes M \approx M/IM$ where IM is the submodule of M generated by elements of the form sm, $s \in I$, $m \in M$. To show this, we refer to property 8) of Section C. Replace Y by M, N by $\{0\}$, X by R, M by I, $\bar{Y}$ by M, $\bar{X}$ by $\bar{R}$. Then we get

$$R \otimes M/W \approx \bar{R} \otimes M$$

where W is the submodule generated by elements

$$s \otimes m \quad \text{or} \quad r \otimes 0 \ (=0) \ , \ s \in I \ , \ m \in M \ , \ r \in R \ , \ 0 \in \{0\} \ ,$$

i.e., generated by elements $s \otimes m$. By property 3) of C, $R \otimes M \approx M$. Clearly this isomorphism (sending $r \otimes m$ to rm) identifies W with the submodule IM, giving

$$M/IM \approx R \otimes M/W \approx \bar{R} \otimes M \ .$$

(3) Notation: When dealing with several rings, there is often some confusion about which ring is intended as ring of scalars in a tensor product $M \otimes N$. When this is so, one writes

$$M \otimes N = M \otimes_R N$$

to indicate that M and N are considered as R-modules for the tensor product.

(4) (Transitivity). If R, R', R'' are three rings and if $\phi: R \to R'$, $\phi': R' \to R''$ are homomorphisms then we get $\phi'\phi: R \to R''$. There is a natural isomorphism

$$R'' \otimes_R M \approx R'' \otimes_{R'} (R' \otimes_R M) \ ,$$

sending

$$r'' \otimes m \longmapsto r'' \otimes (1' \otimes m) \qquad \text{(various tensors).}$$

(Proof for homework).

(5) (Extension of scalars in a free module).

If M is a free R-module with basis $\{x_i\}$, then $R' \otimes M$ is a free R'-module with basis $\{1 \otimes x_i\}$.

It is customary to use the symbols x_i also for $1 \otimes x_i$. This property expresses formally what is meant for instance if, given a vector space V over R with basis $\{x_i\}$, you consider the vector space over C "with basis $\{x_i\}$".

To make the verification, let M' be a free module over R' with a basis $\{x_i'\}$ having the same index set. Since $\{x_i\}$ are linearly independent, we can extend the map

$$\{x_i\} \to \{x_i'\}$$

$$x_i \rightsquigarrow x_i'$$

to an R-homomorphism $f: M \to M'$. By property 1, this corresponds to a certain R'-homomorphism $f': R' \otimes M \to M'$ sending $r' \otimes m \rightsquigarrow r' \cdot f(m)$, hence

$$1 \otimes x_i \rightsquigarrow x_i' .$$

Since $\{x_i'\}$ are lin. independent, so are $\{1 \otimes x_i\}$. They generate (because of property 1) of C), and so $\{1 \otimes x_i\}$ is a basis of $R' \otimes M$.

18.26 Supplementary Notes

A. The Tensor Algebra.

Let X be an R-module. We use the notation

$$\overset{p}{\otimes} X = X \otimes \dots \otimes X \qquad \text{(p times)}.$$

The elements of this module are called contravariant tensors of order p (covariant tensors are elements of $\overset{p}{\otimes} \hat{X}$ where $\hat{X} = \mathrm{Hom}_R(X,R)$ is the dual module. One also considers mixed tensors = elements of a tensor product of some Xs, some $\hat{X}$s).

An element of $\overset{p}{\otimes} X$ which is of the form

$$x = x_1 \otimes x_2 \otimes \dots \otimes x_p \qquad x_i \in X$$

is called a decomposable tensor.

Because of associativity of tensor products, there is a canonical isomorphism

$$(\overset{p}{\otimes} X) \otimes (\overset{q}{\otimes} X) \xrightarrow{\sim} \overset{p+q}{\otimes} X .$$

This means there is a bilinear map

$$(\overset{p}{\otimes} X) \times (\overset{q}{\otimes} X) \longrightarrow \overset{p+q}{\otimes} X$$

and it sends

$$(x_1 \otimes \dots \otimes x_p , x_1' \otimes \dots \otimes x_q') \rightsquigarrow x_1 \otimes \dots \otimes x_p \otimes x_1' \otimes \dots \otimes_q' .$$

This bilinear map is called multiplication of tensors.

We extend the notation $\overset{p}{\otimes} X$ by setting

$$\overset{o}{\otimes} X = R .$$

Using the isomorphisms $R \otimes Y \approx Y \approx Y \otimes R$, multiplication of tensors can still be defined if p or q (or both) are zero. It is just scalar multiplication, e.g.,

$$(r, x_1' \otimes \dots \otimes x_q') \rightsquigarrow r(x_1' \otimes \dots \otimes x_q') .$$

Consider the module

$$R(X) = \text{direct sum of } \overset{p}{\otimes} X \quad , \quad p = 0,1,2,\ldots \quad .$$

We will write elements of $T(X)$ as finite sums

$$\sum_p x_p \qquad (x_p \in \overset{p}{\otimes} X)$$

with the convention that

$$\sum_p x_p = \sum_p x_p' \quad \text{if and only if} \quad x_p - x_p' = 0 \text{ for all } p \; .$$

Since every x_p is a sum of decomposable tensors of order p, every element of $T(X)$ can be written in some way (not uniquely) as a sum of decomposable tensors of various lengths. Two sums of decomposable tensors are equal if and only if for each p the sums of those tensors of order p are equal.

One can make $T(X)$ into a ring by defining products via multiplication of tensors, viz.:

If $\quad Z = \sum_p x_p \quad , \quad Z' = \sum_p x_p' \qquad x_p, \, x_p' \in \overset{p}{\otimes} X \quad ,$

then

$$Z \cdot Z' = \sum_{p,q} x_p \otimes x_q' \quad .$$

The part of $Z \cdot Z'$ of order n is $\sum_{p+q=n} x_p \otimes x_q'$.

The axioms for a ring are easily verified. However, the ring is <u>not</u> commutative.

$T(X)$ is called the <u>tensor algebra</u> of X . It is an <u>algebra</u> over R . This means that there is a ring homom. $R \to T(X)$ and the images of elements of R commute with arbitrary elements of $T(X)$.

B. Symmetric tensor product.

Let X be an R-module. Then $X \otimes X$ has a universal property with respect to bilinear maps

$$f: X \times X \longrightarrow Z \ .$$

Suppose we are interested only in symmetric bilinear maps f, i.e., ones satisfying (in addition to the bilinear axioms)

$$f(x,x') = f(x',x) \quad , \quad \text{all } x,x' \in X \ .$$

We can get such a map by introducing in $X \otimes X$ the extra relations $x \otimes x' - x' \otimes x = 0$: Let $N \subseteq X \otimes X$ be the submodule generated by elements of the form

$$x \otimes x' - x' \otimes x \quad ,$$

and put $S^2(X) = X \otimes X/N$. Then the map

$$X \times X \longrightarrow S^2(X)$$

is symmetric and bilinear, and it is easily seen that $S^2(X)$ has the universal property for symmetric bilinear maps.

Similarly, $S^p(X) = \overset{p}{\otimes} X/N$

where N is the submodule generated by elements of the form

$$(x_1 \otimes \dots \otimes x_p) - (x_{\sigma(1)} \otimes \dots \otimes x_{\sigma(p)}) \ ,$$

σ a permutation of the integers from 1 to p. $S^p(X)$ has the universal property for symmetric p-multilinear maps $X \times \dots \times X \to Z$. Note that $S^1(X) \cong X$. We set $S^0(X) = R$.

Let $\overline{x}_p \in S^p(X)$ denote the residue class of an element $x_p \in \overset{p}{\otimes} X$. It is easily seen that the multiplication of tensors induces a bilinear map

$$S^p(X) \quad S^q(X) \longrightarrow S^{p+q}(X)$$

sending

$$(\overline{x}_p, \overline{x}_q) \rightsquigarrow \overline{x_p \otimes x_q} \quad ,$$

called multiplication of symmetric tensors. This multiplication can be used to introduce a ring structure on $S(X) =$ direct sum of $S^p(X)$, $p = 0,1,2,\ldots$. $S(X)$ is a commutative ring, called the <u>symmetric algebra</u> of X.

<u>Theorem:</u> (for homework). Suppose X is a vector space of dimension n over a field F. Let $\{x_1,\ldots,x_n\}$ be a basis for X, and denote by x_i also the corresponding element in $S^1(X) \cong X$. Then the symmetric algebra $S(X)$ is isomorphic to the polynomial ring

$$F[x_1,\ldots,x_n] \quad \text{in } n \text{ variables over } F.$$

C. <u>Exterior Product.</u>

Instead of asking for symmetric bilinear maps, we could have asked for <u>alternating</u> ones: A bilinear map

$$f\colon X \times X \longrightarrow Z$$

is <u>alternating</u> (= skew symmetric) iff.

$$f(x,x) = 0 \qquad \text{all } x \in X .$$

More generally, an n-multilinear map

$$f\colon X \times X \times \ldots \times X \longrightarrow Z$$

is called <u>alternating</u> iff.

$$f(x_1,\ldots,x_n) = 0$$

whenever two of the x_i s are equal. Notice that for an alternating map,

$$f(\ldots,a,\ldots,b,\ldots) = -f(\ldots,b,\ldots,a,\ldots) \quad ,$$

as is seen by expansion of

$$f(\ldots,a+b,\ldots,a+b,\ldots) \quad (=0) \quad .$$

Let $N \subset \overset{p}{\otimes} X$ be the submodule generated by the tensors $x_1 \otimes \ldots \otimes x_p$ having two (or more) x_i s equal, and set

$$\overset{p}{\wedge} X = \overset{p}{\otimes} X/N \quad .$$

Denote the residue of a tensor $x_1 \otimes \ldots \otimes x_p$ by $x_1 \wedge \ldots \wedge x_p$. $\overset{p}{\wedge} X$ is called the pth exterior power of the module X. The map $\lambda\colon X \times \ldots \times X \longrightarrow \overset{p}{\wedge} X$ sending $(x_1,\ldots,x_p) \rightsquigarrow x_1 \wedge \ldots \wedge x_p$ is clearly alternating, and $\overset{p}{\wedge} X$ has the universal property for alternating maps, viz.

(1) Given an alternating multilinear map

$$f\colon X \times \ldots \times X \longrightarrow Z$$

there is a unique homomorphism $\phi\colon \overset{p}{\wedge} X \to Z$ such that $f = \phi\lambda$.

(2) In addition to the rules making the function λ p-multilinear, an element $x_1 \wedge \ldots \wedge x_p$ is zero if two x_i s are equal, and if σ is a permutation of $\{1,\ldots,p\}$, then

$$x_1 \wedge \ldots \wedge x_p = \operatorname{sgn}(\sigma)\, x_{\sigma(1)} \wedge \ldots \wedge x_{\sigma(p)} \quad .$$

(3) Suppose X is generated by elements $\{x_1,\ldots,x_n\}$. Then $\overset{p}{\wedge} X$ is generated by the elements

$$x_{i_1} \wedge \ldots \wedge x_{i_p} \quad \text{with} \quad i_1 < i_2 < \ldots < i_p$$
$$\text{and} \quad 1 \leq i_\nu \leq n \quad .$$

In particular, $\overset{p}{\wedge} X = 0$ if $p > n$.

To show this, note first that since the tensor product $\overset{p}{\otimes} X$ is generated by tensors of the form

$$x_{j_1} \otimes \ldots \otimes x_{j_p} \quad \text{with} \quad 1 \leq j_\nu \leq n \ ,$$

the exterior power $\overset{p}{\wedge} X$ is generated by the elements

$$x_{j_1} \wedge \ldots \wedge x_{j_p} \quad .$$

Now using the rules (2), any such element is either zero, or is equal to

$$\pm x_{i_1} \wedge \dots \wedge x_{i_p}$$

where $i_1 < i_2 < \dots < i_p$.

(4) Suppose $\{x_1,\dots,x_n\}$ is a basis for X . Then the elements

$$x_{i_1} \wedge \dots \wedge x_{i_p},\ i_1 < i_2 < \dots < i_p$$

form a basis of $\overset{p}{\wedge} X$.

Proof. We need to show that the elements are linearly independent. Let U be a free module with basis $\{u_{(i_1,\dots,i_p)}\}$ where $(i_1,\dots,i_p)$ runs over sets of integers with $1 \leq i_\nu \leq n$ and $i_1 < i_2 < \dots < i_p$. If we can construct an alternating p-multilinear map

$$f\colon X \times \dots \times X \longrightarrow U$$

sending $(x_{i_1},\dots,x_{i_p}) \rightsquigarrow u_{(i_1,\dots,i_p)}$ (if $i_1 < i_2 < \dots < i_n$) then we are done. For, $f = \phi\lambda$ for some $\lambda\colon \overset{p}{\wedge} X \to U$ and λ sends $x_{i_1} \wedge \dots \wedge x_{i_p} \rightsquigarrow u_{(i_1,\dots,i_p)}$. Since $\{u_{(i)}\}$ are linearly independent, it will follow that $\{x_{i_1} \wedge \dots \wedge x_{i_p}\}$ are also linearly independent.

Now to construct a p-multilinear map $X \times \dots \times X \to U$ it suffices to give the images of p-tuples of basis elements $(x_{j_1},\dots,x_{j_p})$, and these can be assigned arbitrarily. For, then f is uniquely determined by

$$f(\sum r_i x_i , \sum s_j x_j , \ldots)$$

$$= \sum_{i,j,\ldots} (r_i s_j \ldots \ldots) f(x_i, x_j, \ldots) .$$

Define f as follows: If two indices are equal in $(x_{j_1}, \ldots, x_{j_p})$, set $f(x_{j_1}, \ldots, x_{j_p}) = 0$. If no two indices are equal, there is a unique permutation σ of $\{1, \ldots, p\}$ such that permutation of $(x_{j_1}, \ldots, x_{j_p})$ by σ yields $(x_{i_1}, \ldots, x_{i_p})$ with $i_1 < i_2 < \ldots < i_p$. Set

$$f(x_{j_1}, \ldots, x_{j_p}) = \mathrm{sgn}(\sigma)\, u(i_1, \ldots, i_p) .$$

This definition extends to a p-multilinear map, as above. I claim it is alternating, and the verification is immediate. This completes the proof.

(5) Let X be a vector space of dimension n over a field F. Then $\overset{p}{\wedge} X$ is of dimension $\binom{n}{p}$, $1 \leq p \leq n$.

(6) For any R-module X, $\overset{1}{\wedge} X \approx X$. One also defines the o-th exterior power by $\overset{0}{\wedge} X = R$.

D. Grassman Algebra.

The bilinear map

$$(\overset{p}{\otimes} X) \times (\overset{q}{\otimes} X) \longrightarrow \overset{p+q}{\wedge} X$$

sending

$$(x_1 \otimes \ldots \otimes x_p, y_1 \otimes \ldots \otimes y_q)$$

$$\rightsquigarrow (x_1 \wedge \ldots \wedge x_p \wedge y_1 \wedge \ldots \wedge y_q)$$

(it is obtained from multiplication of tensors by composing with the map $\otimes X \longrightarrow \wedge X$) clearly annihilates any pair of tensors with two x's or two y's equal. Hence it induces a bilinear map called <u>multiplication</u> of exterior powers,

$$(\overset{p}{\wedge} X) \times (\overset{q}{\wedge} X) \longrightarrow \overset{p+q}{\wedge} X \quad .$$

The definition is extended as for tensors to the case p or $q = 0$. Using this multiplication, we can make

$$\wedge X = \text{direct sum of } \overset{p}{\wedge} X \text{ , } p = 0,1,2,\ldots$$

into a (non-commutative) ring, called the <u>exterior algebra</u> or <u>Grassman algebra</u>. (It is an algebra over R.) The construction and verifications are the same as for the tensor algebra $T(X)$. If we want to be efficient about verification, we can consider the ideal I in $T(X)$ generated by tensors $x_1 \otimes \ldots \otimes x_p$ having two x_i s equal. I actually consists of all elements which are sums of such tensors, i.e., I is the direct sum of the sub-modules $N_p \subset \overset{p}{\otimes} X$ where $\overset{p}{\otimes} X/N_p = \overset{p}{\wedge} X$ (cf. C). Therefore

$$T(X)/I \xrightarrow{\sim} \wedge X \text{ ,}$$

and so the ring structure on $\wedge X$ is induced by that on $T(X)$.

E. <u>Functorial Behavior</u>.

Let $\phi: X \to Y$ be a homomorphism of R-modules. Then we get (cf. III C. 7) a map "$\overset{p}{\otimes} \phi$": $\overset{p}{\otimes} X \to \overset{p}{\otimes} Y$ sending $x_1 \otimes \ldots \otimes x_p$ to $\phi(x_1) \otimes \ldots \otimes \phi(x_p)$. Clearly if $x_1 \otimes \ldots \otimes x_p$ has two x_i s equal, then so does its image. Hence $\overset{p}{\otimes} \phi$ induces a map of exterior products

$$\overset{p}{\wedge} \phi: \overset{p}{\wedge} X \overset{\phi}{\longrightarrow} \wedge Y \quad ,$$

sending $x_1 \wedge \dots \wedge x_p \rightsquigarrow \phi(x_1) \wedge \dots \wedge \phi(x_p)$.

Similarly, $\overset{p}{\otimes} \phi$ induces a map of symmetric powers

$$S^p(\phi): S^p(X) \longrightarrow S^p(Y) .$$

Extending these maps to direct sums, we get maps

$$T(\phi): T(X) \to T(Y)$$

$$S(\phi): S(X) \to S(Y)$$

$$\wedge(\phi): \wedge X \to \wedge Y .$$

These maps are easily seen to be ring homomorphisms.

F. Determinants.

Let X be a free module over R with basis $\{x_1,\dots,x_n\}$. Then $\overset{n}{\wedge} X$ has a basis consisting of the single element $x_1 \wedge \dots \wedge x_n$ (cf. IV C4). In other words, every element Z of $\overset{n}{\wedge} X$ can be written in exactly one way in the form

$$(*) \qquad Z = r(x_1 \wedge \dots \wedge x_n) \qquad r \in R .$$

Let $T: X \to X$ be an R-homomorphism (eg. R a field, T a lin. trasf.!). As above, T induces a homomorphism $\overset{n}{\wedge} T: \overset{n}{\wedge} X \to \overset{n}{\wedge} X$.

Write $[\overset{n}{\wedge} T](x_1 \wedge \dots \wedge x_n)$ in the form (*), say

$$[\overset{n}{\wedge} T](x_1 \wedge \dots \wedge x_n) = d(x_1 \wedge \dots \wedge x_n) , \; d \in R .$$

Then for any $Z \in \overset{n}{\wedge} X$, by (*) , $[\overset{n}{\wedge} T](Z) = r[\overset{n}{\wedge} T](x_1 \wedge \dots \wedge x_n)$

$$= rd(x_1 \wedge \dots \wedge x_n)$$

$$= d\, Z .$$

In other words, $\overset{n}{\wedge} T$ is just multiplication by the scalar d

in the module $\overset{n}{\wedge} X$. Note d is independent of the choice of basis $\{x_1,\ldots,x_n\}$.

Let M be the matrix of T w.r.t. the basis $\{x_1,\ldots,x_n\}$, i.e.,

$$T(x_i) = \sum a_{ij}\, x_j \qquad a_{ij} \in R ,$$

and

$$M = (a_{ij}) .$$

Theorem: $d = \det M$.

Proof: We calculate:

By construction of $\overset{n}{\wedge} T$,

$$\overset{n}{\wedge} T(x_1 \wedge \ldots \wedge x_n) = T(x_1) \wedge T(x_2) \wedge \ldots \wedge T(x_n)$$

$$= (\sum_{j_1} a_{1j_1}\, x_{j_1}) \wedge (\sum_{j_2} a_{2j_2}\, x_{j_2}) \wedge \ldots \wedge (\sum_{j_n} a_{nj_n}\, x_{j_n}) .$$

We can expand this expression out according to the rules. We get to begin with a big sum

$$= \sum_{(j_1,\ldots,j_n)} (a_{1j_1} \cdots a_{nj_n})(x_{j_1} \wedge \ldots \wedge x_{j_n}) .$$

Now if two j_ν s are equal, the term $x_{j_1} \wedge \ldots \wedge x_{j_n}$ is zero. Hence the summation need only be extended over those indices $(j_1,\ldots,j_n)$ (where $1 \leq j_\nu \leq n$) such that no integer occurs twice, i.e., we need sum only over those indices $(j_1,\ldots,j_n)$ which are permutations σ of the set $(1,\ldots,n)$. Thus the sum may be written as

$$\sum_\sigma (a_{1\sigma(1)} \cdots a_{n\sigma(n)})(x_{\sigma(1)} \wedge \ldots \wedge x_{\sigma(n)}) , \quad (\sigma \in S_n) .$$

Now $x_{\sigma(1)} \wedge \ldots \wedge x_{\sigma(n)} = \pm\, x_1 \wedge \ldots \wedge x_n$, the sign being

$\operatorname{sgn}(\sigma)$. Hence

$$= \sum_{\sigma} (\operatorname{sgn} \sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)} (x_1 \wedge \cdots \wedge x_n)$$

$$= (\det M)\, x_1 \wedge \cdots \wedge x_n \qquad \text{Q.E.D.}$$

G. Duality in tensor products.

Let X, Y be R-modules and $u \in \hat{X}$, $v \in \hat{Y}$ ($\hat{X} = \operatorname{Hom}_R(X,R)$) . If we map

$$X \times Y \longrightarrow R$$

by $(x,y) \rightsquigarrow (x)u + (y)v$ (writing transformations on the right)

we get a homomorphism

$$X \oplus Y \longrightarrow R \; .$$

If however, we map

$$X \times Y \longrightarrow R$$

by $(x,y) \rightsquigarrow (x)u \cdot (y)v$

we get a bilinear map, and hence a homomorphism

$$\phi\colon X \otimes Y \longrightarrow R$$

sending $x \otimes y \rightsquigarrow (x)u \cdot (y)v$.

Therefore we have described a map

$$\hat{X} \times \hat{Y} \longrightarrow \widehat{X \otimes Y} = \operatorname{Hom}_R(X \otimes Y, R) \; ,$$

namely, the pair $(u,v) \in \hat{X} \times \hat{Y}$ is sent to ϕ . Since the symbol $(x)u$ is linear in u (as well as in x) , it is clear that this map is bilinear, and hence gives rise to a homomorphism

$$\sigma\colon \hat{X} \otimes \hat{Y} \longrightarrow \widehat{X \otimes Y} \; ,$$

sending $u \otimes v$ to the map ϕ above.

<u>Proposition:</u> Suppose X is a free module with basis $\{x_1,\ldots,x_m\}$, Y is free with basis $\{y_1,\ldots,y_n\}$. Let $\{\hat{x}_i\}$ be the dual basis of $\hat{X}$, $\{\hat{y}_i\}$ the dual basis of $\hat{Y}$, so that

$$\langle x_i,\hat{x}_j\rangle = \langle y_i,\hat{y}_j\rangle = \delta_{ij} .$$

Then the map

$$\varepsilon:\ \hat{X}\otimes\hat{Y} \longrightarrow \widehat{X\otimes Y}$$

is an <u>isomorphism</u>, and the image of $\{\hat{x}_i \otimes \hat{y}_j\}$ is the basis of $\widehat{X\otimes Y}$ dual to $\{x_i \otimes y_j\}$.

<u>Proof:</u> Let ϕ_{ij} be the image of $\hat{X}_i \otimes \hat{Y}_j$ in $\widehat{X\otimes Y}$. Then by the construction above,

$$(x_u \otimes y_\nu)\phi_{ij} = (x_\mu)\hat{x}_i \cdot (y_\nu)\hat{y}_j = \delta_{\mu i}\delta_{\nu j}$$

is zero if $(\mu,\nu) \neq (i,j)$, 1 if $(\mu,\nu) = (i,j)$. Hence the images of $\{\hat{x}_i \otimes \hat{y}_j\}$ form a dual basis to $\{x_i \otimes y_j\}$. This means a basis of $\hat{X}\otimes\hat{Y}$ is mapped to a basis of $\widehat{X\otimes Y}$ and shows that ε is an isomorphism.

The proposition allows us to identify $\hat{X}\otimes\hat{Y}$ with the dual module to $X \otimes Y$ where we are dealing with free modules. Thus if $u \in \hat{X}$, $v \in \hat{Y}$ we view $u \otimes v$ as a linear functional on $X \otimes Y$, defined by

$$(x \otimes y)(u \otimes v) = (x)u\cdot(y)v .$$

In the same way, the dual of a tensor product of p factors may be identified with the tensor product of the duals.

H. <u>Duality in Exterior Products.</u>

Let X be a free R-module with basis $\{x_1,\ldots,x_n\}$. Not all elements of $\overset{p}{\otimes}\hat{X}$ induce linear maps $\overset{p}{\wedge} X \to R$. In order to do so, the element must annihilate all tensors $x_1 \otimes \ldots \otimes x_p$ with two terms equal. However, we can easily find some elements of $(\overset{p}{\wedge} X)$ as follows:

Consider the map:

$$(X \times \ldots \times X) \times (\hat{X} \times \ldots \times \hat{X}) \longrightarrow R \quad \text{(p of each kind)}$$

sending (we use the inner product notation $< , >$)

$$((x_1,\ldots,x_p), (u_1,\ldots,u_p)) \rightsquigarrow \det(<x_i,u_j>) ,$$

for $x_i \in X$, $u_i \in \hat{X}$.

Since $< , >$ is linear in the first variable, and since det is a linear function of each row, the map is p-multilinear in $(x_1,\ldots,x_p)$. Since $< , >$ is linear in the second variable and det is a linear function of columns, the map is p-multilinear in $(u_1,\ldots,u_p)$. Moreover, $\det(<x_i,u_j>)$ vanishes if two x_i s or two u_j s are equal. It is easily seen that therefore there is an induced <u>bilinear</u> <u>form</u>

$$(\overset{p}{\wedge} X) \times (\overset{p}{\wedge} \hat{X}) \longrightarrow R$$

which sends

$$(x_1 \wedge \ldots \wedge x_p , u_1 \wedge \ldots \wedge u_p) \rightsquigarrow \det(<x_i,u_j>) .$$

Such a form induces a homomorphism

$$\varepsilon\colon \overset{p}{\wedge} \hat{X} \longrightarrow \widehat{\overset{p}{\wedge} X} .$$

<u>Proposition:</u> Let X be a free module with basis $\{x_1,\ldots,x_n\}$. Let $\{\hat{x}_i\}$ be the dual basis of $\hat{X}$. The map

$$\varepsilon\colon \overset{p}{\wedge} \hat{X} \longrightarrow \widehat{\overset{p}{\wedge} X}$$

is bijective, and the image of the elements

$$\hat{x}_{i_1} \wedge \dots \wedge \hat{x}_{i_p} \quad (i_1 < \dots < i_p)$$

form the dual basis to the basis

$$x_{i_1} \wedge \dots \wedge x_{i_p} \quad (i_1 < \dots < i_p) .$$

Proof: By construction of ε , if $\phi = \varepsilon(\hat{x}_{i_1} \wedge \dots \wedge \hat{x}_{i_p})$

then

$$(x_{j_1} \wedge \dots \wedge x_{j_p})\phi = \det(\langle x_{j_\mu} , \hat{x}_{i_\nu}\rangle) \quad (\nu,\mu = 1,\dots,p) .$$

Now

$$\langle x_{j_\mu} , \hat{x}_{i_\nu}\rangle = \delta_{j_\mu, i_\nu}$$

and since $j_1 < \dots < j_\mu$ this can be 1 only for a single index μ , if ν is given. Thus each column contains at most one 1 , the rest 0 . Hence we get zero for the determinant unless for each ν , $i_\nu = j_\mu$, some μ . Since

$$j_1 < \dots < j_p \quad \text{and} \quad i_1 < \dots < i_p$$

this can occur only if $j_\nu = i_\nu$ for all ν . Then the matrix

$$(\langle x_{j_\nu} , \hat{x}_{i_\nu}\rangle)$$

is the identity, hence the determinant is 1 . Thus

$$(x_{j_1} \wedge \dots \wedge x_{j_p})\phi = \delta_{(j_1,\dots,j_p),(i_1,\dots,i_p)}$$ as required.

This shows ε maps a basis of $\overset{p}{\wedge} \hat{X}$ to a basis of $\widehat{\overset{p}{\wedge} X}$, and thus is an isomorphism.

This proposition allows us to identify $\overset{p}{\wedge} \hat{X}$ and $\widehat{\overset{p}{\wedge} X}$. Thus we view an element $u_1 \wedge \dots \wedge u_p \in \overset{p}{\wedge} \hat{X}$ as a linear function on $\overset{p}{\wedge} X$, acting by (innerproduct notation)

$$\langle x_1 \wedge \dots \wedge x_p , u_1 \wedge \dots \wedge u_p\rangle = \det(\langle x_i,u_j\rangle) .$$

Elements of $\overset{p}{\wedge} X$ are often called p-<u>vectors</u>, and elements of $\overset{p}{\wedge} \hat{X}$ are called p-<u>forms</u>.

18.732 exercises. No. 1.

These exercises are meant as a guide. They are examples of geometric interpretations of certain spectra, and are by no means exhaustive. It would be worth while for you to think longer along the lines indicated by certain exercises rather than to try to work them all at once. In some exercises you have the opportunity to make precise definitions and to prove some things about them. Try to do it. k denotes a field.

1. (a) Let A be a k-algebra. Interpret geometrically a map from A to $k[t]/t^2$, as was done in class.

(b) Interpret a map of A to $k[t]/t^3$ in a similar way. For ease of visualization, treat the case $A = k[x,y]$ (the "plane") first.

2. (a) List all ideals I of $R = k[x,y]$ whose radical is the ideal of the "origin" (generated by x and y), and such that the dimension of the algebra R/I over k is 2. Interpret geometrically.

(b) dimension 3.

3. (a) Let $R = k[x,y]$. Given a polynomial $f = f(x,y)$, the variety $C = V(f)$ in the "plane" Spec R is called a plane curve. It corresponds naturally to Spec $R/(f)$. Sometimes it is assumed that f has no multiple factors (the curve is reduced) or that f is a prime polynomial (the curve is irreducible). Suppose that C passes through the origin, i.e., that $f(0,0) = 0$. Give conditions on f which insure that C has a well defined tangent line at the origin, and give the equation of this line in terms of the coefficients of f. These are the conditions which assure that the origin is a simple point of C. Otherwise the origin is said to be a singular point of the curve. Interpret the tangent direction defined by f in terms of 1(a), 2(a).

(b) Let $g = 0$ define another curve D, also passing through the origin. One says that C meets D transversally if their tangent directions are distinct. Otherwise they have a tangency. Describe a condition on the ideal generated by f and g which determines whether or not the curves are transversal at the origin.

(c) Practice drawing a few plane curves.

4. The plane curve $y^2 = x^3$ has an algebraic parametrization

$$y = t^3$$
$$x = t^2$$

(a) This yields a map $\operatorname{Spec} k[t] \longrightarrow \operatorname{Spec}(k[x,y]/(y^2-x^3))$.

(b) The map is a homeomorphism of topological spaces.

5. (a) Let $A \subset k[x] \times k[x]$ (the product of the ring $k[x]$ with itself) be the subring consisting of pairs (f,g) of polynomials having the property that $f(a) = g(b)$, where a and b are chosen elements of k. Draw $\operatorname{Spec} A$, and describe the map from $\operatorname{Spec}(k[x] \times k[x])$ to $\operatorname{Spec} A$. Find explicit generators and relations for the ring.

(b) What if A is the subring of pairs (f,g) such that $f(a) = g(b)$ and $f'(a) = g'(b)$ (the values of the derivatives are equal)?

(c) How should one draw the spectrum of the subring of $k[x]$ of functions f such that $f'(0) = 0$?

6. Let $R \subset k \times k \times k \times k \times \ldots$ (the ring of sequences of elements of k) be the subring consisting of those sequences $a_1, a_2, \ldots$ which become constant for sufficiently large n, i.e.,

such that $a_n = a_m$ for n and m large enough. The required largeness is allowed to vary with the sequence. Draw Spec R.

7. (a) Draw Spec $\mathbb{Z}[x]$. You should view it as a plane, letting say the horizontal axis represent the "direction of Spec $\mathbb{Z}$", and the vertical axis the "x direction" in a rather vague way. For each of the closed points of Spec $\mathbb{Z}$, given by the prime numbers ($\approx$ prime ideals) $2,3,\ldots,p,\ldots$ let the vertical line above the point p represent the locus $V(p)$ in Spec $\mathbb{Z}[x]$. It corresponds to Spec $\mathbb{Z}[x]/(p)$ = Spec $F[x]$ where F is the field $\mathbb{Z}/(p)$, i.e. to a "line". This line has on it the points given by $x = 0,1,\ldots,p-1$. Draw them in for primes less than or equal 7.

(b A locus $V(f)$, where f is a polynomial (in x with integral coefficients) should be drawn as a curve. This is a purely schematic drawing, and you should not worry about where the curves go, except that when they pass through one of the points you have drawn, you should draw them as passing through. Try to figure out, when two curves meet, whether the intersection should be considered as transversal or not, and draw accordingly (cf. 3.(b)). Now draw the loci $x=0$, $x=1$, $x=2$, ..., $x=7$.

(c) How does the locus $x^2=2$ (i.e., the curve $V(x^2-2)$) meet the vertical "line" $V(2)$? The line $V(7)$? The line $V(3)$? Draw it.

(d) How should the locus $x^2 = 8$ be drawn ?

1. Let R be a ring, M_1, M_2 two maximal ideals of R, and $x_1, x_2 \in X = \operatorname{Spec} R$ the corresponding points. Let $\varphi : k(x_1) \xrightarrow{\sim} k(x_2)$ be an isomorphism between the residue fields $k(x_i) = R/M_i$. Let $R_o \subset R$ be the subring of elements $a \in R$ such that $\varphi(a(x_1)) = a(x_2)$ (notation of (1.B)). Describe $\operatorname{Spec} R_o$.

2. (a) Show that the rank of a free module is uniquely determined, i.e., that a module can not be free of rank n and free of rank m $(n \neq m)$ at the same time.

(b) Suppose that R contains no idempotents other than $0, 1$. Show that if a module M over R is locally free then it has a well defined rank.

3. (a) Describe localization with respect to an element in a ring R with dcc. Describe all modules over R. Describe the sheaf associated to an R-module, and show that every locally free rank n R-module is free.

(b) Let R be a local ring with maximal ideal m, $k = R/m$ its residue field. Let F be a free R-module with basis $\{x_1, \ldots, x_n\}$. Denote by $\overline{z}$ the residue of an element $z \in F$ in the k-vector space $\overline{F} = F/mF$. Show that a set $\{y_1, \ldots, y_n\} \subset F$ is a basis of F iff. $\{\overline{y}_1, \ldots, \overline{y}_n\}$ is a basis of $\overline{F}$. (Hint: consider the determinant of the matrix of the endomorphism of F sending x_i to y_i).

(c) A locally free module over a local ring is free.

(d) A semi-local ring R is one having only finitely many maximal ideals. Show that every locally free module of rank n over R is free. (Use the Chinese Remainder Theorem and (b)).

4. Prove that if a finite set $S \subset R$ generates the unit ideal, then the 1-cohomology of a quasi-coherent sheaf F on the covering $\{X_s | s \in S\}$ of X is zero. Do the case that S consists of two elements first.

5. Let $f : R \to R'$ be a ring homomorphism. We get a map $\varphi : X \leftarrow X'$ between the spectra. The fibre of the map φ at a point $x \in X$ is defined to be $\mathrm{Spec}(R' \otimes_R k)$ where $k = k(x)$ is the residue field at x (cf. (1.B)). If x is a closed point, the fibre is a closed subspace of X' (why?).

Spec $R[t_1, \ldots, t_n]$ is called affine n-space over $X = \mathrm{Spec}\, R$. It maps naturally to X, and the fibres are of the form Spec $k[t_1, \ldots, t_n]$ $(k = k(x))$.

(a) Let M be a free R-module with basis $\{v_1, \ldots, v_n\}$. The symmetric algebra $S(M)$ is isomorphic with $R[v_1, \ldots, v_n]$ (cf. T.P.). Prove this.

(b) A section of a map of sets $\varphi : X' \to X$ is a map $\psi : X \to X'$ such that the composition $\varphi\psi$ = identity. When dealing with spectra, it is usual to consider only those sections which come from ring homomorphisms $g : R \to R'$ such that gf = identity. In this sense, the sections of Spec $S(M)$ over Spec R are in 1-1 correspondence with elements of the dual module $\check{M} = \mathrm{Hom}_R(M,R)$.

5. (c) Generalize (b) to the case of an arbitrary R-module M.

(d) Interpret geometrically (in analogy with vector bundles) in case M is locally free of rank n. Justify your assertions.

6. (a) Every locally free module over a PID is free. What theorem does this follow from, and why?

(b) Using problem 4 of No. 1, we can identify the spectra X of the rings $R = k[t]$ and $R_o = k[x,y]/(y^2 - x^3)$. Show that there is an exact sequence of sheaves of additive groups on X.

$$0 \to \widetilde{R}_o \to \widetilde{R} \to \epsilon \to 0$$

where ϵ is a sheaf "concentrated at the point $p : t = 0$" whose sections on an open $U \subset X$ are zero if $p \notin U$, and $\epsilon(U) \approx k$ if $p \in U$.

(c) Show that the sheaves of units form an exact sequence of multiplicative groups

$$0 \to \widetilde{R}^*_o \to \widetilde{R}^* \to \delta \to 0$$

where δ is isomorphic to ϵ via a map $z \rightsquigarrow 1+z$.

(d) Use the exact cohomology sequence obtained from (c) to calculate the isomorphism classes of locally free rank 1 modules on $\operatorname{Spec} k[x,y]/(y^2 - x^3)$.

7. In a similar way, calculate the group of isomorphism classes of locally free rank 1 sheaves on $\operatorname{Spec} Z[x]/(x^2 - 8)$. (cf. problem 7 (c), (d) of No. 1).

1. Consider the $R = k[x,y]$-module M obtained by dividing R by the ideal generated by xy and y^2.

   a) What is $\operatorname{supp} M$?

   b) What is $\operatorname{ass} M$?

   c) Give a primary decomposition of M.

2. Let R be a dedekind domain, $X = \operatorname{Spec} R$, and x the generic point of X (which corresponds to the zero ideal). The field of fractions of R is thus just the stalk $\tilde{R}_x = K$. Let M be a module of finite type over R.

   a) Show that if the map $M \longrightarrow \tilde{M}_x = K \otimes_R M$ (which is a K-vector space) is injective, then M is locally free. (Hint: treat the case of a discrete valuation ring first.)

   b) For any finitely generated module M, let N be the kernel of the map $M \longrightarrow \tilde{M}_x$. Show that N has its support at finitely many closed points of $\operatorname{Spec} R$, and that M/N is locally free.

   c) Show that M is isomorphic to a direct sum $M \approx N \oplus M/N$.

   d) Complete the classification of finitely generated R-modules by showing that a module N whose support is a finite set of closed points is a direct sum of cyclic modules (i.e., ones generated by one element) isomorphic to R/p^e for some prime ideal p and integer e (Hint: Show that if N is p-coprimary, it comes from an R_p-module by restriction of scalars, and solve the problem when the ring is a discrete valuation ring.).

3. In the notation of problem 2, replace R by the ring $k[x,y]/(y^2-x^3)$.

   a) Give an example of a module M of finite type such that the map $M \to \tilde{M}_x$ is injective, but which is not locally free.

   b) Give an example of a module N whose support is the singular point $x=y=0$, but which is not a direct sum of cyclic modules. Proofs are required.