Affine Varieties and Dimension.

Let $R = k[x_1, \ldots, x_n]$ be the ring of polynomials over an algebraically closed field k. For any ideal I of R, the set $\mathcal{V}(I)$ of zeroes of all $f \in I$ is called the *affine variety* of I. Since I is finitely generated $\mathcal{V}(I)$ is the set of solutions of a finite system of polynomial equations $f_1 = \cdots = f_m = 0$. It is useful to think of it also as the set $\mathrm{Alg}_k(R/I, k)$ of k-algebra homomorphisms $R/I \to k$.

Given an affine variety $V = \mathcal{V}(I)$, consider the ideal $\mathcal{I}(V) = \{f \in R |\, f(x) = 0 \;\forall x \in V\}$. Hilbert's Nullstellensatz says that $\mathcal{I}(\mathcal{V}(I)) = \mathrm{rad}\ I$; in other words I is almost retrievable from $\mathcal{V}(I)$. Since obviously $\mathcal{V}(I) = \mathcal{V}(\mathrm{rad}\ I)$, we see that two ideals give rise to the same variety iff they have the same radical. In particular, if I is P-primary, we have $\mathrm{rad}\ I = P$, $\mathcal{V}(I) = \mathcal{V}(P)$, and $\mathcal{I}(\mathcal{V}(I)) = P$.

Obviously $I_1 \subset I_2$ implies $\mathcal{V}(I_1) \supset \mathcal{V}(I_2)$, and it is easy to see that $\mathcal{V}(I_1 \cap I_2) = \mathcal{V}(I_1) \cup \mathcal{V}(I_2)$. Hence a primary decomposition $I = Q_1 \cap \cdots \cap Q_r$ results in a break-up $\mathcal{V}(I) = \mathcal{V}(Q_1) \cup \cdots \cup \mathcal{V}(Q_r)$ with unique components $\mathcal{V}(Q_i) = \mathcal{V}(P_i)$. A variety V is *irreducible*, i.e. not the union of proper subvarieties, iff $\mathcal{I}(V)$ is prime, or equivalently $V = \mathcal{V}(Q)$ with Q primary.

Let $V = \mathcal{V}(P_0)$ with P_0 prime. Irreducible subvarieties of V correspond to primes of R containing P_0, or equivalently, prime ideals of the domain $A = R/P_0$. As in vector spaces, one can define the *dimension* of V to be the length s of the longest possible chain $V = V_0 \supset V_1 \supset \cdots \supset V_s$ of irreducible subvarieties. This corresponds to a chain $0 \subset P_1 \subset P_2 \subset \cdots \subset P_s$ of prime ideals in A, which is why we also write $s = \dim A$.

On the other hand, dimension should have something to do with degrees of freedom. There are two variants of this notion, a global one and a local one. Globally we can take the transcendence degree over k of the quotient field of A. By Noether's Normalization Lemma, A is integral over a subring $B = k[t_1, \ldots, t_s]$ with independent parameters t_i. To get a point of V, i.e. a homomorphism $A \to k$, we can freely assign values to the t_i (whence s degrees of freedom) and then have finitely many choices for the x_j by the theorem of Cohen-Seidenberg. By a refinement of that theorem, chains of primes in A correspond to chains of primes in B, and vice versa, so that $\dim A = \dim B$. Now it is easy to see that the latter is exactly s. For instance, if $B = k[x, y, z]$, the chain of ideals $0 \subset (x) \subset (x, y) \subset (x, y, z)$ is maximal.

The third notion of dimension has to do with the number of local parameters at a point. It is analogous to the dimension of the tangent space in differential geometry. A point of V is a 0-dimensional subvariety belonging to a maximal ideal M of A. Intuitively, we want something like the minimal number of generators of M . However, the point in question is equally well given by any M-primary ideal Q, which, being smaller than M, may need fewer generators. So, we define the local dimension $\delta_M(A)$ to be the smallest number of elements required to generate any M-primary ideal. To compare $\delta_M(A)$ with $\dim A$, we can work in the local ring A_M which has the same quotient field as A and hence the same dimension. Ameneties like Nakayamas Lemma make local rings relatively pleasant to work with. Given a minimal set of generators for an M- primary ideal it is not very difficult to construct a chain of primes of the same length (along the line of the x, y, z-story above). Thus one can show $\dim A_M \geq \delta(A_M)$.

The reverse inequality is more interesting. The trick is to introduce yet another dimension $d(A)$, which is the degree of a polynomial associated with the graded ring $\sum_{\nu \geq 0} Q^\nu/Q^{\nu+1}$ for any M-primary Q, and which has the virtue of being $\leq \delta(A)$ from the start. Using the Artin-Rees Theorem, it is then shown that $d(A)$ decreases strictly when A changes to $A/(f)$. From there a straightforward induction proves that $d(A) \geq \dim A$.

Freedom and Finiteness.

Let R be a (commutative) domain. We shall mainly be interested in finitely generated (hereinafter called 'fig') R-modules. Any choice of generators of a fig module M produces a surjection $F \to M \to 0$ from a free module F onto M. If the kernel of this is also fig free, M is said to be *finitely presented.* This is is true for any M, as long as R is principal. When R is noetherian (i.e. every ideal is fig), every submodule of a fig module is fig, so that M has a *free resolution*

$$\cdots \to F_n \to \cdots \to F_1 \to F_0 \to M \to 0.$$

If such a resolution breaks off after finitely many terms, we say that M is *finitely resolvable.* If this happens for every fig M, let us call R *strongly noetherian.* If R is (strongly) noetherian, so is the polynomial ring $R[X]$ — courtesy of Messrs. Hilbert and Serre, respectively. In particular, any polynomial ring over a field is strongly noetherian.

A module M is *projective*, if every surjection from a free module $F \to M \to 0$ has a right inverse. For fig modules this happens iff the localization M_S is a free R_S-module, whenever we admit the complement S of a maximal ideal of R as a set of denominators. In this sense, a fig projective module is locally free. In view of the technical usefulness and ubiquity of localization, it is clear that projectivity is a convenient property this side of freedom. A little better than projective are the *stably free* modules. A module M qualifies for this distinction, if $M \oplus F$ is free for suitable fig free F. It is not hard to show that M is stably free iff it is projective and finitely resolvable.

To prove that some ring R does not have any non-free, stably free modules, an easy induction shows that it suffices to verify: for any module M, the freedom of $M \oplus R$ implies that of M. This, in turn, amounts to the following statement about matrices: every left- invertible $n \times 1$-matrix over R occurs as a column in an invertible square matrix. A theorem by Quillen and Suslin says that this is true for $R = k[x_1, \ldots, x_r]$, thus corroborating a conjecture of Serre's to the effect that, for such R, every projective fig module is free.

If R is the coordinate ring of an affine variety $V = \mathrm{Alg}_k(R, k)$, a projective R-module (being locally free) gives rise to an algebraic vector bundle over V (and vice versa). The Quillen-Suslin Theorem asserts that, if V is affine r-space, every such bundle is *algebraically* isomorphic to a trivial one. Even for $k = \mathbf{C}$ this is a lot more than the obvious topological result.

R is called a *dedekind* domain if every ideal is projective (forcing *every* fig torsion-free R-module to be so). The projectivity of an ideal $I \neq 0$ is equivalent to *invertibility*: the existence of generators $\{a_i\}$ of I and elements $\{b_j\}$ of the field of quotients of R such that $\sum_i a_i b_i = 1$ and all $a_i b_j \in R$. This property entails that the non-zero ideals in a dedekind domain R are automatically fig and that they form a semi-group *with cancellation*, i.e. $I_0 I_1 = I_0 I_2 \Rightarrow I_1 = I_2$. Together with the primary decomposition available in any noetherian ring, this leads to unique factorization of ideals into products of prime powers. Since all prime localizations of R are principal (ideals become free!), a dedekind domain is noetherian, integrally closed, and one-dimensional. Conversely, these three conditions are equivalent to the dedekind property, thus ensuring that it is transmitted to the integral closure of R in any finite separable extension of its field of quotients.

Bits and Pieces.

To begin with, let R be any ring, M any R-module. The finite filtrations $M = M_0 \supset M_1 \supset \cdots \supset M_n = 0$ and $M = M'_0 \supset M'_1 \supset \cdots \supset M'_n = 0$ are said to be isomorphic, if their *bits* M_i/M_{i+1} and M'_j/M'_{j+1} nre pairwise isomorphic after suitable reordering of indices. A theorem of Schreier, having to do with Butterflies, asserts that any two finite filtrations have isomorphic refinements, whence any two *simple* finite filtrations must *be* isomorphic (Jordan- Hölder). A module allowing finite simple filtrations is said to be of finite length. It is both artinian and noetherian and can, moreover, be expressed as a direct sum $M = M_1 \oplus \cdots \oplus M_r$ of indecomposable *pieces*, which may, however, not be simple. Up to isomorphism and reordering of indices, these pieces are unique by the Theorem of Krull-Remak-Schmidt, which is most Fittingly derived from the fact that a non-invertible endomorphism of an indecomposable piece must be nilpotent. It is important to note that, so far on this page, R was not required to be commutative. The artinian-noetherian condition is always fulfilled for modules which are also finite dimensional vector spaces. The aforementioned results are most frequently used in representation theory.

From now on, let R again be commutative and noetherian. If $\dim R > 0$, the powers of a maximal ideal are necessarily distinct and any hopes for finite length go up in smoke. However, unique decomposition into indecomposables is not limited to the artinian context — cf. modules over principal domains. Taking a cue from the latter, we consider an R-module M *coprimary* if every $a \in R$ acts on it either injectively or nilpotently. The nilpotent actors a will then form a prime ideal $P \subset R$ *associated* to M, and M is called P-coprimary.

The terminology in these parts is somewhat baffling because one always considers submodules as well as factor modules. A submodule $E' \subset E$ is called primary (relative to E) if E/E' is coprimary. In particular, an ideal Q is primary if R/Q is coprimary. If P is the associated prime, we always have some $P^n \subset Q$, but P^n itself may not be primary. However, if P is maximal, any ideal caught between P and one of its powers *is* primary — whew!

Here is what we get in this general setting. Every fig R-module E is a *sub*direct sum of coprimary modules; i.e. $E \subseteq M_1 \oplus \cdots \oplus M_r$, and the projection maps $E \to M_i$ are (separately) surjective; the set of primes associated with the components in an irredundant "decomposition" of this sort depends only on E, hence is denoted $\mathrm{Ass}(E)$; the components belonging to minimal (jargon:"isolated") elements of $\mathrm{Ass}(E)$ are actually unique themselves, provided that components belonging to the same prime have been lumped together; even more: for the isolated components, the kernels of the projection maps are unique as submodules ("primary" ones) of E. In fact, these matters are usully dicussed in terms of kernels; i.e., one aims at representing a submodule as an intersection of primary ones. In the case of $E = R/I$, we get the primary decomposition $I = Q_1 \cap \cdots \cap Q_r$ of an ideal I.

Apart from decompositions, the associated primes can be characterized as follows: $P \in \mathrm{Ass}(E)$, iff R/P is isomorphic to a submodule of E, iff P is the annihilator of some $x \in E$. Every fig R-module E has a finite filtration $E \supset E_1 \supset \cdots \supset E_m$ whose bits E_j/E_{j+1} are isomorphic to some R/P_j, with P_j prime; the primes occurring here include all the associated ones (but may not be limited to them). If $\mathrm{Supp}(E)$ stands for the set of primes at which E has a non-trivial localization, it turns out that $P \in \mathrm{Supp}(E)$ iff it contains an associated prime.

Filters and Grades.

With any filtration $E = E_0 \supset E_1 \supset \cdots \supset E_n \supset \cdots$ on an abelian group, we can associate two new, and in some sense "nicer" groups:

$$G(E) = \bigoplus_{n=0}^{\infty} E_n/E_{n+1} \qquad \text{and} \qquad \hat{E} = \varprojlim E/E_n,$$

called *graded* group and *completion*, respectively. The latter is literally the completion in the topology for which $\{E_n\}$ is a fundamental system of neighbourhoods of 0, a handy fact when it comes to comparing the effects of different filtrations. Applying these two processes to a commutative ring $R = E$ and $E_n = I^n$, where $I \subset R$ is an ideal, we again obtain natural ring structures, $G(R)$ being a *graded* ring in the sense that $A_n A_m \subset A_{n+m}$, where we have set $A_n = I^n/I^{n+1}$ for the "homogeneous" components. For instance, if R is a dedekind domain and $I = P \neq 0$ a prime ideal, it is easy to see that $G(R) \simeq k[t]$, the polynomial ring over $k = R/P$, and $\hat{R}$ is the completed discrete valuation ring $\hat{R}_P$, both of them principal domains. In general, R is noetherian if and only if $G(R)$ is noetherian; in that case $G(R) \simeq G(\hat{R})$, and hence $\hat{R}$ is noetherian.

From now on let R be noetherian, E a fig R-module with a *stable* I-filtration $\{E_n\}$, i.e. such that $IE_n \subseteq E_{n+1}$ with equality for $n >> 0$. Any two such filtrations are highly compatible: there is a fixed m such that the $(n+m)$-th term of one is contained in the n-th term of the other (either way) for all large n; in particular they yield the same topology on E. The Artin-Rees Lemma says that the filtration $\{E_n \cap E'\}$ induced on a submodule $E' \subset E$ is again stable. As a result, an exact sequence $0 \to E' \to E \to E'' \to 0$ gives rise to a similar sequence of I-adic completions. Moreover, one can use it to show that $E_S \to \hat{E}$ is injective (Krull's Theorem), where $S = 1 + I$ — a set obviously invertible (by geometric series) in $\hat{R}$. Consequently $R \to \hat{R}$ is injective if R is a domain.

In the noetherian setting it may well happen that every homogeneous piece $M_n = E_n/E_{n+1}$ of $G(E)$ is of finite length $\lambda(M_n)$, so that the non-finiteness comes only from counting all the pieces. Inverting Zeno's paradox, we then form the Poincaré series $\sum_n \lambda(M_n)t^n$, which by a theorem of Hilbert-Serre represents a rational function with a very explicit denominator. If $G(E)$ is generated over $G(R)$ by s elements from M_1, this function is of the form $f(t)(1-t)^{-d}$ with $d \leq s$ and $f(t) \in \mathbf{Z}[t]$. Comparing the Poincaré series with the binomial expansion, we see that there is a polynomial $h(x) \in \mathbf{Q}[x]$ of degree $d-1$, the Hilbert polynomial, such that $\lambda(M_n) = h(n)$ for large n. This is of particular interest when R is local and I is primary with respect to the maximal ideal P (which makes R/I artinian and gives each M_n finite length). From $h(x)$ we inductively get a polynomial $g(x)$ of degree $d = d(E)$, whose leading term depends neither on I nor on the particular filtration, and such that $\lambda(E/E_n) = g(n)$ for large n. With the help of Artin-Rees (applied to $aE \subset E$), one now proves that $d(E/aE) < d(E)$ whenever $a \in R$ acts injectively on E; whence it follows by induction that $\dim(R) \leq d(R)$. Since $d(R) \leq$ the local dimension $\delta(R)$ by construction, and since the latter is $\leq \dim(R)$ by an elementary argument, this establishes the equality of the three notions (cf. blurb on dimension).

Math 509 (April 1988)

Valuations and Absolute Values.

Let P be a prime ideal in a noetherian domain R with quotient field K. The basic idea of a valuation is to study P-divisibility by *counting*: since $\bigcap P^n = 0$ (Krull), every $a \in R$ lies in a well-defined smallest power $P^{v(a)}$. The resulting function $v : R \to \mathbf{Z}$ has the properties (1) $v(a+b) \geq \max\{v(a), v(b)\}$ and (2') $v(ab) \geq v(a) + v(b)$. What distinguishes valuation theory is its insistence on involving K: one wants to count not only "zeroes" but also "poles". There is no difficulty in extending v to the local ring R_P, but to include all of K, the inequality (2') should be sharpened to (2): $v(ab) = v(a) + v(b)$. This precision is supplied by unique ideal factorization if R_P is dedekind, e.g. if R is integrally closed and P of height 1; but in higher dimensions there is trouble. For instance, if $R = k[x, y, z]$ with $xy - z^3 = 0$, and $P = (x, y, z)$, we would have $v(x) + v(y) = 2$ but $v(xy) = 3$.

Looking at it another way, forget R and start with a valuation $v : K \to \Gamma$ onto an (additive) ordered group Γ without insisting that $\Gamma = \mathbf{Z}$. Then the set $A = \{a \in K |\ v(a) \geq 0\}$ forms a ring such that $x \in A$ or $x^{-1} \in A$ for any $x \in K$. Such a ring is called a *valuation ring*. It is always integrally closed and local, and it always *does* correspond to a valuation $v : K \to \Gamma = K^\times/A^\times$, which is ordered by the image of the maximal ideal (minus 0) defining positivity. These general valuations have two main virtues: their extendability and their relation to integrality. In fact, the integral closure in K of any subring B is the intersection of all valuation rings containing B. As to extendability, any local subring C of K (not necessarily with K as quotients) can be embedded in a valuation ring which respects its maximal ideal. Consequently, any valuation on K can be extended to any field $K' \supset K$. If $[K' : K]$ is finite, so is the number of such extensions, as well as the *ramification index* $e = [\Gamma' : \Gamma]$ for each of them; further, $e\Gamma' \subset \Gamma$ in each case, so that $\Gamma = \mathbf{Z} \Rightarrow \Gamma' = \mathbf{Z}$. Valuations with the latter property are called *discrete*. They are ulimately the most useful ones, and the only ones having noetherian valuation rings.

Discrete valutions have one leg in valuation theory and the other in the theory of *absolute values*, i.e. homomorphisms from $K^\times$ to the positive reals satisfying the triangle inequality, which, by setting $|a|_v = 2^{-v(a)}$ looks like a weakened version of (1). Although topological games can also be played with general valuations, absolute values have two important strengths in this respect: any two of them induce the same topology on K iff each is a positive real power of the other; and, if K is *complete*, any finite K-space has only one norm-topology compatible with the given absolute value. If K is complete with respect to a discrete valuation v, it follows that there is exactly *one* extension w of v to any field L of finite degree over K. More generally, if $\hat{K}$ denotes the completion of K, and if $L = K[X]/(f(X))$ for some separable monic polynomial, the completions $\hat{L}_i$ of L with respect to the various extensions w_i of v to L are just the terms occurring in the decomposition $\hat{K}[X]/(f(X)) \simeq \hat{L}_1 \times \ldots \times \hat{L}_r$ which arises from the irreducible factorization $f(X) = f_1(X) \cdots f_r(X)$ over $\hat{K}$. The latter can in large measure be studied in the the residue class field k of v (i.e. valuation ring mod maximal ideal) because Hensel's Lemma allows the lifting of relatively prime polynomial factorizations from k to $\hat{K}$.

The relaxation of (1) to the triangle inequality is no mere whim. In number theory it permits the inlusion of ordinary absolute values corresponding to the various embeddings $K \to \mathbf{C}$, which turns out to be essential. Thus the approximation theorem of Artin-Whaples, which proclaims the density of K embedded diagonally in a cartesian product $K \times \cdots \times K$ with topologically inequivalent absolute values, is more than a corollary of the Chinese Remainder Theorem.

Math 509 (Spring 88).

Example of a Stably Free Module.

Remember that the tangent bundle of the 2-sphere S^2 is non- trivial; indeed, not only does S^2 fail to be parallelizable — it does not even have *one* nowhere vanishing vector-field. However, when one adds the normal bundle, which *is* trivial, the result is a trivial $\mathbf{R}^3$ - bundle. Thus, in this case, non-trivial + trivial = trivial; weird, eh?

Our aim is to describe a (precise) algebraic counterpart to this phenomenon. We begin abstractly with an arbitrary commutative ring R, an element $\alpha = [a_1, \ldots, a_n] \in R^n$, and the submodule $R\alpha$ it generates.

LEMMA: Suppose that $R\alpha$ is faithful (hence free). Then $R^n/R\alpha$ is projective (hence stably free), if and only if there is a $\beta \in R^n$ with $\beta \cdot \alpha = 1$; it is free if and only if there is an $M \in \mathrm{GL}_n(R)$ with α as its first row.

Proof: α^t is the $n \times 1$-matrix of the injection $R \to R^n$ whose image is $R\alpha$. The latter is a direct summand iff this matrix has a left inverse β. The rest is clear.

NOTE: If $R\alpha \cong R/I$ for some ideal I, the splitting of the corresponding injection $R/I \to R^n$ (i.e. projectivity of $R^n/R\alpha$) is equivalent to the existence of a $\beta \in R^n$ such that $\beta \cdot \alpha = 1 - e$, with $e \in I$ an idempotent since $e\alpha = 0$ implies $e(1-e) = 0$.

REMARK: Suppose that, for every n, any left-invertible α^t can be embedded into an invertible square matrix. Then every finite stably free R-module is free.

Proof: By the lemma, $E \oplus R \cong R^n$ implies that E is free. Hence $E \oplus R^m \cong R^n$ implies that $E \oplus R^{m-1}$ is free, whence (induction) E is free.

EXAMPLE: Let R be any ring of continuous functions $f : S^2 \to \mathbf{R}$ containing the constant function 1 and the coordinate functions x, y, z. Put $\alpha = [x, y, z]$. Then $R^3 = R\alpha \oplus P$, where P is non-free projective.

Indeed, since $x^2 + y^2 + z^2 = 1$, the ideal A is all of R, and the lemma ensures that $R\alpha$ is a direct summand. If the complementary summmand P were free, there would be a basis $\{\alpha, \beta, \gamma\}$ of R^3. Then $\det[\alpha, \beta, \gamma]$ would be a unit in R, in particular it would be a function vanishing nowhere on S^2. More particularly still, the vector functions α and (say) β would never be parallel anywhere on S^2, and $\beta - (\beta \cdot \alpha)\alpha$ would be a non-vanishing vector field.

The smallest example of R would be $\mathbf{Z}[x, y, z]/(x^2 + y^2 + z^2 - 1)$. Whatever we take for R, it is clear that the kernel of $\xi \mapsto \xi - (\xi \cdot \alpha)\alpha$ is exactly $R\alpha$; therefore this map identifies P with an R-module of vector fields on S^2. Evidently the summands $R\alpha$ and P correspond to the normal and the tangent bundles of the sphere, respectively.

All this works, of course, for spheres of any even dimension.