Armand Borel

Linear Algebraic Groups

Second Enlarged Edition

Springer-Verlag
New York Berlin Heidelberg London
Paris Tokyo Hong Kong Barcelona
世界图书出版公司
北京·广州·上海·西安

Armand Borel
School of Mathematics
Institute for Advanced Study
Princeton, New Jersey 08450 USA

First edition published by W.A. Benjamin, Inc., 1969

Library of Congress Cataloging-in-Publication Data

Borel, Armand.
Linear algebraic groups / Armand Borel.—2nd enl. ed.
p. cm.—(Graduate texts in mathematics; 126)
Includes bibliographical references and indexes.
ISBN 0-387-97370-2 (alk. paper).—ISBN 3-540-97370-2 (alk. paper)
1. Linear algebraic groups. I. Title. II. Series.
QA564.B58 1991
512'.5—dc20 90-19774

Reprinted by World Publishing Corporation, Beijing, 1993
for distribution and sale in The People's Republic of China only
ISBN 7 – 5062 – 1432 – 6

ISBN 0-387-97370-2 Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-97370-2 Springer-Verlag Berlin Heidelberg New York

Introduction to the First Edition

These Notes aim at providing an introduction to the theory of linear algebraic groups over fields. Their main objectives are to give some basic material over arbitrary fields (Chap. I, II), and to discuss the structure of solvable and of reductive groups over algebraically closed fields (Chap. III, IV). To complete the picture, they also include some rationality properties (§§15, 18) and some results on groups over finite fields (§16) and over fields of characteristic zero (§7).

Apart from some knowledge of Lie algebras, the main prerequisite for these Notes is some familiarity with algebraic geometry. In fact, comparatively little is actually needed. Most of the notions and results frequently used in the Notes are summarized, a few with proofs, in a preliminary Chapter AG. As a basic reference, we take Mumford's Notes [14], and have tried to be to some extent self-contained from there. A few further results from algebraic geometry needed on some specific occasions will be recalled (with references) where used. The point of view adopted here is essentially the set theoretic one: varieties are identified with their set of points over an algebraic closure of the groundfield (endowed with the Zariski-topology), however with some traces of the scheme point of view here and there.

These Notes are based on a course given at Columbia University in Spring, 1968,* at the suggestion of Hyman Bass. Except for Chap. V, added later, Notes were written up by H. Bass, with some help from Michael Stein, and are reproduced here with few changes or additions. He did this with marvelous efficiency, often expanding or improving the oral presentation. In particular, the emphasis on dual numbers in §3 in his, and he wrote up Chapter AG, of which only a very brief survey had been given in the course. It is a pleasure to thank him most warmly for his contributions, without which these Notes would hardly have come into being at this time. I would also like to thank Miss P. Murray for her careful and fast typing of the manuscript, and J.E. Humphreys, J.S. Joel for their help in checking and proofreading it.

A. Borel
Princeton, February, 1969

---

*Lectures from May 7th on qualified as liberated class, under the sponsorship of the Students Strike Committee. Space was generously made available on one occasion by the Union Theological Seminary.

Introduction to the Second Edition

This is a revised and enlarged edition of the set of Notes: "Linear algebraic groups" published by Benjamin in 1969. The added material pertains mainly to rationality questions over arbitrary fields with, as a main goal, properties of the rational points of isotropic reductive groups. Besides, a number of corrections, additions and changes to the original text have been made. In particular:

§3 on Lie algebras has been revised.

§6 on quotient spaces contains a brief discussion of categorical quotients. The existence of a quotient by finite groups has been added to §6, that of a categorical quotient under the action of a torus to §8.

In §11, the original proof of Chevalley's normalizer theorem has been replaced by an argument I found in 1973, (and is used in the books of Humphreys and Springer).

In §14, some material on parabolic subgroups has been added.

§15, on split solvable groups now contains a proof of the existence of a rational point on any homogeneous space of a split solvable group, a theorem of Rosenlicht's proved in the first edition only for $\mathbf{GL}_1$ and $\mathbf{G}_a$.

§§19 to 24 are new. The first one shows that in a connected solvable k-group, all Cartan k-subgroups are conjugate under $G(k)$, a result also due to M. Rosenlicht. §§20, 21 are devoted to the so-called relative theory for isotropic reductive groups over a field k: Conjugacy theorems for minimal parabolic k-subgroups, maximal k-split tori, existence of a Tits system on $G(k)$, rationality of the quotient of G by a parabolic k-subgroup and description of the closure of a Bruhat cell. As a necessary complement, §22 discusses central isogenies.

§23 is devoted to examples and describes the Tits systems of many classical groups. Finally, §24 surveys without proofs some main results on classifications and linear representations of semi-simple groups and, assuming Lie theory, relates the Tits system on the real points of a reductive group to the similar notions introduced much earlier by E. Cartan in a Lie theoretic framework.

Many corrections have been made to the text of the first edition and my thanks are due to J. Humphreys, F.D. Veldkamp, A.E. Zalesski and V. Platonov who pointed out most of them.

I am also grateful to Mutsumi Saito, T. Watanabe and especially G. Prasad, who read a draft of the changes and additions and found an embarrassing number of misprints and minor inaccuracies. I am also glad to acknowledge help received in the proofreading from H.P. Kraft, who read parts of the proofs with great care and came up with a depressing list of corrections, and from D. Jabon.

The first edition has been out of print for many years and the question of a reedition has been in the air for that much time. After Addison–Wesley had acquired the rights to the Benjamin publications they decided not to proceed with one and released the publication rights to me. I am grateful to Springer-Verlag to have offered over ten years ago to publish a reedition in whichever form I would want it and to several technical editors (starting with W. Kaufmann–Bühler) and scientific editors for having periodically prodded me into getting on with this project. I am solely to blame for the procrastination.

In preparing the typescript for the second edition, use was made to the extent possible of copies of the first one, whose typography was quite different from the one present techniques allow one to produce. The insertions of corrections, changes and additions, which came in successive ways, presented serious problems in harmonization, pasting and cutting. I am grateful to Irene Gaskill and Elly Gustafsson for having performed them with great skill.

I would also like to express my appreciation to Springer-Verlag for their handling of the publication and their patience in taking care of my desiderata.

A. Borel

Conventions and Notation

1. Throughout these Notes, k denotes a commutative field, K an algebraically closed extension of k, k_s (resp. $\bar{k}$) the separable (resp. algebraic) closure of k in K, and p is the characteristic of k. Sometimes, p also stands for the chracteristic exponent of k, i.e. for one if $\mathrm{char}(k) = 0$, and p if $\mathrm{char}(k) = p > 0$.

All rings are commutative, unless the contrary is specifically allowed, with unit, and all ring homomorphisms and modules are unitary.

If A is a ring, A^* is the group of invertible elements of A.

$\mathbb{Z}$ denotes the ring of integers, $\mathbb{Q}$ (resp. $\mathbb{R}$, resp. $\mathbb{C}$) the field of rational (resp. real, resp. complex) numbers.

2. *References.* A reference to section $(x.y)$ of Chapter AG is denoted by (AG.$x.y$). In the subsequent chapters $(x.y)$ refers to section $(x.y)$ in one of them.

There are two bibliographies, one for Chapter AG, on p. 83, one for Chapters I to V, on p. 391.

References to original literature in Chapters I and V are usually collected in bibliographical notes at the end of certain paragraphs. However, they do not aim at completeness, and a result for which none is given need not be new.

3. Let G be a group. If (X_i) $(1 \leqq i \leqq m)$ are sets and $f_i : X_i \to G$ maps, then the map
$f : X_1 \times \ldots \times X_m \to G$ defined by

$$(x_1, \ldots, x_n) \to f_1(x_1) \ldots . f_m(x_m), \qquad (x_i \in X_i;\ 1 \leqq i \leqq m),$$

is often called the product map of the f_i's.

Let N_i $(1 \leqq i \leqq n)$ be normal subgroups of G. The group G *is an almost direct product* of the N_i's if the product map of the inclusions $N_i \to G$ is a homomorphism of the direct product $N_1 \times \ldots \times N_m$ onto G, with finite kernel.

If M, N are subgroups of G, then (M, N) denotes the subgroup of G generated by the commutators $(x, y) = x.y.x^{-1}.y^{-1}$ $(x \in M,\ y \in N)$.

4. If V is a k-variety, and k' an extension of k in K, then $V(k')$ denotes the set of points of V rational over k'. $k'[V]$ is the k'-algebra of regular functions defined over k' on V, and $k'(V)$ the k'-algebra of rational functions defined over k' on V. If W is a k-variety, and $f : V \to W$ a k-morphism, then the map $k[W] \to k[V]$ defined by $\varphi \to \varphi \circ f$ is the *comorphism* associated to f and is denoted f°.

Contents

Chapter AG

Background Material from Algebraic Geometry

This chapter should be used only as a reference for the remaining ones. Its purpose is to establish the language and conventions of algebraic geometry used in these notes. The intention is to take, in so far as is practicable, the point of view of Mumford's chapter I. Thus our varieties are identified with their points over a fixed algebraically closed field K (of any characteristic). It is technically important for us, however, not to require (as does Mumford) that varieties be irreducible.

For the most part definitions and theorems are simply stated with references and occasional indications of proofs. There are two notable exceptions. We have given essentially complete treatments of the material presented on rationality questions (i.e. field of definition), in sections 11–14, and of the material on tangent spaces, in sections 15–16. This seemed desirable because of the lack of convenient references for these results (in the form used here), and because of the important technical role both of these topics play in the notes.

§1. Some Topological Notions
(Cf. [Class., exp. 1, no. 1].)

1.1 *Irreducible components.* A topological space X is said to be *irreducible* if it is not empty and is not the union of two proper closed subsets. The latter condition is equivalent to the requirement that each non-empty open set be dense in X, or that each one be connected.

If Y is a subspace of a topological space X then is irreducible if and only if its closure $\bar{Y}$ is irreducible. By Zorn's lemma every irreducible subspace of X is contained in a maximal one, and the preceding remark shows that the maximal irreducible subspaces are closed. They are called the irreducible components of X. Since the closure of a point is irreducible it lies in an irreducible component; hence X is the union of its irreducible components.

If a subspace Y of X has only finitely many irreducible components, say $Y_1, \ldots, Y_n$, then $\bar{Y}_1, \ldots, \bar{Y}_n$ are the irreducible components (without repetition) of $\bar{Y}$.

1.2 *Noetherian spaces.* A topological space X is said to be *quasi-compact* ("quasi-" because X is not assumed to be Hausdorff) if every open cover has a finite subcover. If every open set in X is quasi-compact, or, equivalently, if the open sets satisfy the maximum condition, then X is said to be *noetherian*. It is easily seen that every subspace of a noetherian space is noetherian.

Proposition. *Let X be a noetherian space.*

(*a*) *X has only finitely many irreducible components, say $X_1, \ldots, X_n$.*
(*b*) *An open set U in X is dense if and only if $U \cap X_i \neq \phi$ $(1 \leqq i \leqq n)$.*
(*c*) *For each i, $X_i' = X_i - \bigcup_{j \neq i} (X_j \cap X_i)$ is open in X, and $U_o = \bigcup_i X_i'$ is an open dense set in X whose irreducible and connected components are $X_1', \ldots, X_n'$.*

Part (a) follows from a standard "noetherian induction" argument.

Since X_i is irreducible the set $X_i' = X - \left(\bigcup_{j \neq i} X_j \right)$ is open in X and dense in X_i. Hence every open dense set U in X must meet X_i'. Conversely if U is open and meets each X_i then $U \cap X_i$ is dense in X_i, so $\bar{U}$ contains each X_i and hence equals X. It follows, in particular, that $U_o = \bigcup_i X_i'$ is open, dense. Since the X_i' are open, irreducible, and pairwise disjoint, they are the irreducible and connected components of U_o.

1.3 *Constructible sets.* A subset Y of a topological space X is said to be *locally closed* in X if Y is open in $\bar{Y}$, or, equivalently, if Y is the intersection of an open set with a closed set. The latter description makes it clear that the intersection of two locally closed sets is locally closed. A *constructible set* is a finite union of locally closed sets. The complement of a locally closed set is the union of an open set with a closed set, hence a constructible set. It follows that the complement of a constructible set is constructible. Thus, the constructible sets are a Boolean algebra (i.e. they are stable under finite unions and intersections and under complementation) In fact they are the Boolean algebra generated by the open and (or) closed sets.

If $f: X \to X'$ is a continuous map then f^{-1} is a Boolean algebra homomorphism carrying open and closed sets, respectively, in X' to those in X. Hence f^{-1} carries locally closed and constructible sets, respectively in X' to those in X.

Proposition. *Let X be a noetherian space, and let Y be a constructible subset of X. Then Y contains an open dense subset of $\bar{Y}$.*

Remark. Conversely, by a noetherian induction argument one can show that if Y is a subset of X whose intersection with every irreducible closed subset of X has the above property, then Y is constructible.

Proof. Write $Y = \bigcup_i L_i$ with each L_i locally closed. Then $\bar{Y} = \bigcup_i \bar{L}_i$, so, if $\bar{Y}$ is irreducible, $\bar{Y} = \bar{L}_i$ for some i. Moreover $L_i (\subset Y)$ is open in $\bar{L}_i$.

In the general case write $Y = \bigcup_j Y_j$ where the Y_j are the irreducible components of Y. The latter are closed in Y and hence constructible in X. Moreover the first case shows that Y_j contains a dense open set in $\bar{Y}_j$. Since the $\bar{Y}_j$ are the irreducible components of $\bar{Y}$ (see (AG.1.1)) it follows from (AG.1.2) that $Y = \cup Y_j$ contains a dense open set in $\bar{Y}$.

1.4 (*Combinatorial*) *dimension.* For a topological space X it is the supremum of the lengths, n, of chains $F_0 \subset F_1 \subset \cdots \subset F_n$ of distinct irreducible closed sets in X; it is denoted

$$\dim X.$$

If $x \in X$ we write

$$\dim_x X$$

for the infimum of $\dim U$ where U varies over open neighborhoods of x.

It follows easily from the definitions and the properties of irreducible closed sets that $\dim \phi = -\infty$, that

$$\dim X = \sup_{x \in X} \dim_x X,$$

and that $x \mapsto \dim_x X$ is an upper semi-continuous function. Moreover, if X has a finite number of irreducible components (e.g. if X is noetherian), say $X_1, \ldots, X_m$, then $\dim X$ is the maximum of $\dim X_i (1 \leqq i \leqq m)$.

§2. Some Facts from Field Theory

2.1 *Base change for fields* (cf. [C.-C., exp. 13–14]). We fix a field extension F of k. If k' is any field extension of k we shall write

$$F_{k'} = k' \bigotimes_k F.$$

This is a k'-algebra, but it is no longer a field, or even an integral domain, in general. However, each of its prime ideals is minimal (i.e. there are no inclusion relations between them) and their intersection is the ideal of nilpotent elements in $F_{k'}$ (see (AG.3.3) below). We say a ring is *reduced* if its ideal of nilpotent elements is zero.

Here are the basic possibilities:

(a) *k' is separable algebraic over k*: Then $F_{k'}$ is reduced, but it may have more than one prime ideal.

(b) *k' is algebraic and purely inseparable over k*: Then $F_{k'}$ has a unique prime ideal (consisting of nilpotent elements) but $F_{k'}$ need not be reduced.

(c) k' *is a purely transcendental extension of* k: Then $F_{k'}$ is clearly an integral domain.

2.2 *Separable extensions.* F is said to be *separable* over k if it satisfies the following conditions, which are equivalent: We write p for the characteristic exponent of k ($= 1$ if $\mathrm{char}(k) = 0$).

(1) F^p and k are linearly disjoint over k^p.
(2) $F_{(k^{1/p})}$ is reduced.
(3) $F_{k'}$ is reduced for all field extensions k' of k.

Suppose, for some extension L of k, that F_L is an integral domain, with field of fractions (F_L). Then F *is separable over* $k \Leftrightarrow (F_L)$ *is separable over* L. The implication $\Rightarrow$ follows essentially from the associativity of tensor products, using criterion (3). To prove the converse we embed a given extension k' of k in a bigger one, k'', containing L also. Since $F_{k'} \subset F_{k''}$ it suffices to show that $F_{k''}$ is reduced. But $F_{k''} = F_L \bigotimes_L k'' \subset (F_L)_{k''}$ and the latter is reduced, by hypothesis.

2.3 *Differential criteria.* (See [N.B., (a), §9], [Z.-S., v. I, Ch. II, §17], or [C.-C., exp. 13].) A *k-derivation* $D: F \to F$ is a k-linear map such that

$$D(ab) = D(a)b + aD(b) \text{ for all } a, b \in F.$$

The set of them,

$$\mathrm{Der}_k(F, F)$$

is a vector space over F.

Theorem. *Suppose* F *is a finitely generated extension of* k. *Put*

$$n = \mathrm{tr\,deg}_k(F)$$

and

$$m = \dim_F \mathrm{Der}_k(F, F).$$

Then $m \geqq n$, *with equality if and only if* F *is separable over* k.

Let $D_1, \ldots, D_m$ *be a basis of* $\mathrm{Der}_k(F, F)$ *and let* $a_1, \ldots, a_m \in F$. *Then* F *is separable algebraic over* $k(a_1, \ldots, a_m)$ *if and only if* $\det(D_i(a_j)) \neq 0$.

If $m = n$ then a set $\{a_1, \ldots, a_m\}$ as above is called a *separating transcendence basis.*

2.4 Proposition. *Let* G *be a group of automorphisms of a field* F. *Then* F *is a separable extension of* $k = F^G$, *the fixed elements under* G.

We shall prove that F and $k^{1/p}$ are linearly disjoint over k, i.e. that if $a_1, \ldots, a_n \in k^{1/p}$ are linearly independent over k then they are linearly independent over F. The action of G extends uniquely to $F^{1/p}$ and G acts trivially on $k^{1/p}$. Suppose $a_1, \ldots, a_n$ are linearly dependent over F, but not over k; we can assume n is minimal. Let $a_1 + b_2 a_2 + \cdots + b_n a_n = 0$ be a dependence relation. If some b_i, say b_n, is not in k then it is moved by some

$g \in G$. Subtracting $a_1 + g(b_2)a_2 + \cdots + g(b_n)a_n$ from the relation above we obtain a shorter relation; contradiction.

2.5 On occasions, we shall need a generalization of 2.4. Let A be a reduced noetherian algebra over k, denote by $k(A)$ its ring of fractions (cf. 3.1, Ex. 1) and let G be a group of automorphisms of A. The action then extends to $k(A)$. By Prop. 10 in [N.B.(b):IV, §2, no. 5], $k(A)$ is uniquely a sum of fields K_i then necessarily permuted by G. Let e_i be the corresponding idempotents. Thus $1 = \sum e_i$ and the e_i's are permuted by G. If $\alpha \in A^G$ is non-divisor of zero in A^G, then it is one in A. In fact we can write $1 = \sum f_j$ where f_j is the sum of idempotents e_i forming an orbit of G; then we have $f_i \cdot \alpha \neq 0$ and therefore since $g(e_i \cdot \alpha) = g(e_i) \cdot \alpha$, $e_i \alpha \neq 0$ for all i's. Therefore $k(A^G)$ embeds in $k(A)^G$.

Proposition. *We keep the previous notation. Then* $e_i \cdot k(A)^G = K_i^{G_i}$, *where* G_i *is the isotropy group of* e_i. *If* $k(A)^G = k(A^G)$, *then* K_i *is a separable extension of* $e_i k(A^G)$.

If $a \in k(A)^G$ then $e_i \cdot \alpha$ is fixed under G_i. Conversely, if $b \in K_i$ is fixed under G_i, then the sum of the $g(b)$, where g runs through a set of representatives of G/G_i, is an element of $k(A)^G$ whose image under e_i is b. Then 2.4 shows that K_i is a separable extension of $e_i \cdot k(A)^G$. The second assertion is then obvious.

§3. Some Commutative Algebra

3.1 *Localization* [N.B., (b)]. Let S be a multiplicative set in a ring A, i.e. S is not empty and $s, t \in S \Rightarrow st \in S$. Then we have the "localization" $A[S^{-1}]$ consisting of fractions a/s ($a \in A$, $s \in S$), and the natural map $A \to A[S^{-1}]$ which is universal among homomorphisms from A rendering the elements of S invertible.

If M is an A-module we further have the localized $A[S^{-1}]$-module $M[S^{-1}]$, consisting of fractions x/s ($x \in M$, $s \in S$), which is naturally isomorphic to $A[S^{-1}] \underset{A}{\otimes} M$.

If $x \in M$ and $s \in S$ then $x/s = 0$ in $M[S^{-1}]$ if and only if $tx = 0$ for some $t \in S$. It follows directly from this that, *if* M *is finitely generated* $M[S^{-1}] = 0$ *if and only if* $tM = 0$ *for some* $t \in S$, i.e. if and only if $S \cap \operatorname{ann} M \neq \phi$, where ann M is the annihilator of M in A.

The functor $M \mapsto M[S^{-1}]$ from A-modules to $A[S^{-1}]$-modules is exact, and it preserves tensors and Hom's in the following sense: If M and N are A-modules then the natural map $\left(M \underset{A}{\otimes} N\right)[S^{-1}] \to M[S^{-1}] \underset{A[S^{-1}]}{\otimes} N[S^{-1}]$ is an isomorphism, and the natural map $\operatorname{Hom}_A(M, N)[S^{-1}] \to \operatorname{Hom}_{A[S^{-1}]}(M[S^{-1}], N[S^{-1}])$ is an isomorphism if M is finitely presented.

Examples. (1) Let S be the set of all non-divisors of zero in A. Then $A \to A[S^{-1}]$ is injective, and the latter is called the *full ring of fractions* of A. When A is an integral domain it is the field of fractions.

(2) If $S = \{f^n | n \geqq 0\}$ for some $f \in A$ then we write A_f or $A[1/f]$, and M_f for the localizations.

(3) An ideal P in A is prime if $S_P = A - P$ is a multiplicative set. The corresponding localizations are denoted A_P and M_P. In this case A_P has a unique maximal ideal, PA_P, i.e. A_P is a *local ring*.

3.2 *Local rings.* Let A be a local ring with maximal ideal $\mathfrak{m}$ and residue class field $k = A/\mathfrak{m}$. Let M be a finitely generated A-module.

(a) If $\mathfrak{m}M = M$ then $M = 0$.

For let $x_1, \ldots, x_n$ be a minimal set of generators of M, and suppose $n > 0$. Write $x_1 = \sum a_i x_i (a_i \in \mathfrak{m})$. Then $(1 - a_1)x_1 = \sum_{i>1} a_i x_i$. But $1 - a_1$ is invertible, so $x_2, \ldots, x_n$ already generate M; contradiction.

(b) If $x_1, \ldots, x_n \in M$ then they generate M if and only if they do so modulo $\mathfrak{m}M$. Hence the minimal number of generators of M is $\dim_k(M/\mathfrak{m}M)$.

This follows by applying (a) to M/N, where N is the submodule generated by $x_1, \ldots, x_n$.

(c) If M is projective then M is free.

We can write $A^n = M \oplus N$, so that $k^n = (M/\mathfrak{m}M) \oplus (N/\mathfrak{m}N)$. Lift a basis of k^n to A^n so that it lies in $M \cup N$. The result is, by (b), a set of n generators of A^n. These must clearly be a basis of A^n, e.g. because the associated matrix has an invertible determinant. Hence M, being spanned by part of a basis of A^n, is free.

3.3 *Nil radical; reduced rings.* The set of nilpotent elements in a ring A is an ideal denoted nil A. We call A *reduced* if nil $A = (0)$.

If J is any ideal the ideal $\sqrt{J}$ is defined by $\sqrt{J}/J = \text{nil}(A/J)$. Thus nil $A = \sqrt{(0)}$. Moreover, we have

$$\sqrt{J} = \text{the intersection of all primes containing } J.$$

If S is a multiplicative set then $\sqrt{J} \cdot A[S^{-1}] = \sqrt{J \cdot A[S^{-1}]}$. In particular this implies that *A is reduced if and only if the full ring of fractions of A is reduced.*

3.4 *spec*(A) [M, Ch. II, §1]. We let $X = \text{spec}(A)$ be the set of all prime ideals in A, equipped with the *Zariski topology*, in which the closed sets are those of the following form for some $J \subset A$:

$$V(J) = \{P \in X | J \subset P\}.$$

If $Y \subset X$ we put $I(Y) = \bigcap_{P \in Y} P$, and then $V(I(Y))$ is just the closure of Y.

Moreover, if J is an ideal of A it follows from 3.3 that

$$I(V(J)) = \sqrt{J}.$$

Thus closed sets correspond bijectively (with inclusions reversed) to ideals J for which $J = \sqrt{J}$. It follows that if A is noetherian then spec(A) is a noetherian space.

The map $P \mapsto \overline{\{P\}}$ is a bijection from X to the set of irreducible closed sets in X. Thus the irreducible components of X correpond to the minimal primes in A. Moreover the (combinatorial) dimension of X (measured by chains of irreducible closed sets) is called the (Krull) *dimension of* A, and it is denoted dim A. Thus

$$\dim A = \dim X.$$

If $f \in A$ and $P \in X$ one sometimes writes $f(P)$ for the image of f in the residue class field of A_P (which is the field of fractions of A/P). With this notation the complement of $V(fA)$ is

$$X_f = \{P \in X \mid f(P) \neq 0\}.$$

This is called a *principal open set*. For any J we have $V(J) = \bigcap_{f \in J} V(f)$ so the principal open sets are a base for the topology.

Suppose $\alpha_o : A \to B$ is a ring homomorphism. Then α_o induces a continuous map $\alpha : Y = \text{spec}(B) \to X$, $\alpha(P) = \alpha_o^{-1}(P)$. In fact $\alpha^{-1}(V(J)) = V(\alpha_o(J))$.

Examples. (1) If J is an ideal then $A \to A/J$ induces a homeomorphism of spec(A/J) onto $V(J) \subset X$.

(2) If S is a multiplicative set then spec$(A[S^{-1}]) \to$ spec(A) induces a homeomorphism onto the set of $P \in X$ such that $P \cap S = \phi$.

(i) If $f \in A$ then we obtain a homeomorphism spec$(A_f) \to X_f$.

(ii) If $P \in X$ it follows that $\dim_P X = \dim \text{spec}(A_P) = (\text{Krull}) \dim A_P$.

3.5 *Support of a module.* Let $X = \text{spec}(A)$ where A is a noetherian ring, and let M be a finitely generated A-module. Then it follows from 3.1 that

$$\text{supp}(M) = \{P \mid M_P \neq 0\}$$

is the closed set $V(\text{ann } M)$. In particular $M = 0$ if and only if $\text{supp}(M) = \phi$.

Let $f : L \to M$ be a homomorphism of A-modules. Since localization is exact it follows that the set of P where f_P is an epimorphism is the (open) complement of supp(coker f). Applying this to $\text{Hom}_A(M, L) \to \text{Hom}_A(M, M)$, and using the fact that the Hom's localize properly (see 3.1) we conclude that the set U of $P \in X$ such that f_P is a split epimorphism is open, and f is a split epimorphism if and only if $U = X$.

Suppose f is surjective and L is free. Then we deduce from the last remark

and 3.2(c) that:

$$U = \{P \in X \mid M_P \text{ is a free } A_P\text{-module}\}$$

is open, and M is a projective A-module if and only if $U = X$.

3.6 *Integral extensions* ([N.B., (b), Ch. 5] or [Z.-S., v. I, Ch. V]). Let $A \subset B$ be rings. A $b \in B$ is said to be *integral* over A if $A[b]$ is a finitely generated A-module, or, equivalently if b is a root of a monic polynomial with coefficients in A. The set B' of all elements of B integral over A is a subring, called the *integral closure* of A in B. We say B is *integral over* A if $B' = B$. We say A is *integrally closed* in B if $B' = A$. We call A *normal* if A is reduced and integrally closed in its full ring of fractions.

Suppose $A \subset B \subset C$ are rings. Then C is integral over A if and only if C and B are integral over B and A, respectively.

Suppose B is integral over A. Then $\operatorname{spec}(B) \to \operatorname{spec}(A)$ *is surjective and closed.* If B is a finitely generated A-algebra then B is a finitely generated A-module. If B is an integral domain then every non-zero ideal of B has non-zero intersection with A.

To see the latter let $b^n + a_{n-1}b^{n-1} + \cdots + a_o = 0$ be an integral equation of minimal degree over A of some $b \neq 0$ in B. Then $a_o = -b(a_{n-1}b^{n-2} + \cdots + a_1) \in bB \cap A$. Moreover $a_o \neq 0$; otherwise we could reduce the degree of the equation.

3.7 *Noether normalization* [M, Ch. I, p. 4]. *A* k-algebra A is said to be *affine* if it is finitely generated as a k-algebra. Such an A is a noetherian ring.

Theorem. *Let* $R = k[y_1, \ldots, y_m]$ *be an affine integral domain over* k *whose field of fractions,* $k(y_1, \ldots, y_m)$, *has transcendence degree* n *over* k. *Then there exist elements* $x_1, \ldots, x_n \in R$, *which are algebraically independent over* k, *and such that* R *is integral over the polynomial ring* $k[x_1, \ldots, x_n]$. *If* $k(y_1, \ldots, y_m)$ *is separable over* k *then* $x_1, \ldots, x_n$ *can be chosen to be a separating transcendence basis of* $k(y_1, \ldots, y_m)$ *over* k.

Except for the last assertion this theorem is essentially identical in statement and notation with that in Mumford, page 4. With the following modification, the proof in Mumford gives also the last assertion as well.

First, choose $y_1, \ldots, y_m$ so that the last n of them are a separating transcendence basis. Next, choose the integers $r_1, \ldots, r_m$ (as well as their analogues at other stages of the induction) to be divisible by p, the characteristic exponent of k. The proof in Mumford requires only that the r_i's be large and increase rapidly, so our additional restriction is harmless.

This done, the $x_1, \ldots, x_n$ produced by the proof will be congruent, modulo p^{th} powers, to the last n of the y_i's. Thus each x_i has the same image under every k-derivation as the corresponding y (if $p > 1$; otherwise there is no problem). It therefore follows that the x's, like the y's, are a separating transcendence basis (see (AG.2.3)).

3.8 *The Nullstellensatz* [M, Ch. I]. Let A be an affine K-algebra, and let $X = \max(A)$ be the subspace of maximal ideals in $\operatorname{spec}(A)$.

If $e: A \to K$ is a K-algebra homomorphism then $\ker(e) \in X$ so we have a natural map

$$\varphi: \operatorname{Mor}_{K\text{-alg}}(A, K) \to X.$$

Theorem. (Nullstellensatz).

(1) *φ is bijective.*

(2) *X is dense in* $\operatorname{spec}(A)$. *Moreover $F \mapsto F \cap X$ is a bijection from the set of closed sets in* $\operatorname{spec}(A)$ *to the set of closed sets in X. Therefore the analogous statement is valid for open sets also.*

If $x \in X$ we shall write e_x for the homomorphism $A \to K$ such that $x = \ker(e_x)$. If $f \in A$ we shall also use the functional notation

$$f(x) = e_x(f).$$

Thus each $f \in A$ determines a function $X \to K$. If f represents the zero function then $f \in I(X) = \bigcap_{x \in X} x$. It follows from part (2) that $I(x) = I(\operatorname{spec}(A)) = \operatorname{nil} A$. Thus, in general, the function on X associated with f determines f modulo $\operatorname{nil} A$. If A is reduced we can therefore view A as a ring of K-valued function on X.

We shall use for X the same notational conventions introduced for $\operatorname{spec}(A)$. For example, if $f \in A$ then $X_f = \{x \in X \mid f(x) \neq 0\}$. These principal open sets are a base for the topology on X.

If M is an A-module we also write $\operatorname{supp}_X(M) = \{x \in X \mid M_x \neq 0\}$, or simply $\operatorname{supp}(M)$ when the meaning is clear. In view of part (2) of the Nullstellensatz all the remarks of 3.5 remain valid with X in place of $\operatorname{spec}(A)$.

The correspondence in (2) also matches irreducible closed sets, clearly, and hence irreducible components. If $x \in X$, then $\dim_x X = \dim_x \operatorname{spec}(A) = \dim A_x$. Moreover $\dim X = \dim \operatorname{spec}(A)$.

3.9 *Regular local rings* [Z.-S., v. II, Ch. VIII, §11]. Let A be a noetherian local ring with maximal ideal $\mathfrak{m}$ and residue class field $k = A/\mathfrak{m}$. Then the minimal number of generators of $\mathfrak{m}$ is (see 3.2) the dimension over k of $\mathfrak{m}/\mathfrak{m}^2$. It is a basic fact that

$$\dim_k(\mathfrak{m}/\mathfrak{m}^2) \geqq \dim A,$$

where $\dim A$ is defined as in 3.4. When this inequality is an equality the local ring A is said to be *regular*.

Regularity has rather strong consequences for A, for example the fact that *A is then a unique factorization domain.*

We shall see in AG.17 that, when A is the local ring of a point x on a variety V, then regularity of A means that x is a simple point; hence the importance of the notion. A minimal set of generators of $\mathfrak{m}$ then gives the