James E. Humphreys

Linear Algebraic Groups

Corrected Second Printing

Springer-Verlag
New York Heildelberg Berlin

James E. Humphreys
Department of Mathematics and Statistics
University of Massachusetts
Amherst, MA 01003
USA

AMS Subject Classification (1981): 20G15

Library of Congress Cataloging in Publication Data

Humphreys, James E
Linear algebraic groups.
(Graduate texts in mathematics; v. 21)
Bibliography: p.
1. Linear algebraic groups. I. Title. II. Series.
QA171.H83 512'.2 74-22237

9 8 7 6 5 4 3 2

ISBN 0-387-90108-6 Springer-Verlag New York
ISBN 3-540-90108-6 Springer-Verlag Berlin Heidelberg

Preface to the Second Printing

For this printing, I have corrected some errors and made numerous minor changes in the interest of clarity. The most significant corrections occur in Sections 4.2, 4.3, 5.5, 30.3, 32.1, and 32.3. I have also updated the bibliography to some extent. Thanks are due to a number of readers who took the trouble to point out errors, or obscurities; especially helpful were the detailed comments of José Antonio Vargas.

James E. Humphreys

Preface to the First Printing

Over the last two decades the Borel–Chevalley theory of linear algebraic groups (as further developed by Borel, Steinberg, Tits, and others) has made possible significant progress in a number of areas: semisimple Lie groups and arithmetic subgroups, p-adic groups, classical linear groups, finite simple groups, invariant theory, etc. Unfortunately, the subject has not been as accessible as it ought to be, in part due to the fairly substantial background in algebraic geometry assumed by Chevalley [8], Borel [4], Borel, Tits [1]. The difficulty of the theory also stems in part from the fact that the main results culminate a long series of arguments which are hard to "see through" from beginning to end. In writing this introductory text, aimed at the second year graduate level, I have tried to take these factors into account.

First, the requisite algebraic geometry has been treated in full in Chapter I, modulo some more-or-less standard results from commutative algebra (quoted in §0), e.g., the theorem that a regular local ring is an integrally closed domain. The treatment is intentionally somewhat crude and is not at all scheme-oriented. In fact, everything is done over an algebraically closed field K (of arbitrary characteristic), even though most of the eventual applications involve a field of definition k. I believe this can be justified as follows. In order to work over k from the outset, it would be necessary to spend a good deal of time perfecting the foundations, and then the only rationality statements proved along the way would be of a minor sort (cf. (34.2)). The deeper rationality properties can only be appreciated after the reader has reached Chapter X. (A survey of such results, without proofs, is given in Chapter XII.)

Second, a special effort has been made to render the exposition transparent. Except for a digression into characteristic 0 in Chapter V, the development from Chapter II to Chapter XI is fairly "linear", covering the foundations, the structure of connected solvable groups, and then the structure, representations and classification of reductive groups. The lecture notes of Borel [4], which constitute an improvement of the methods in Chevalley [8], are the basic source for Chapters II–IV, VI–X, while Chapter XI is a hybrid of Chevalley [8] and SGAD. From §27 on the basic facts about root systems are used constantly; these are listed (with suitable references) in the Appendix. Apart from §0, the Appendix, and a reference to a theorem of Burnside in (17.5), the text is self-contained. But the reader is asked to verify some minor points as exercises.

While the proofs of theorems mostly follow Borel [4], a number of improvements have been made, among them Borel's new proof of the normalizer theorem (23.1), which he kindly communicated to me.

I had an opportunity to lecture on some of this material at Queen Mary College in 1969, and at New York University in 1971–72. Several colleagues have made valuable suggestions after looking at a preliminary version of the manuscript; I especially want to thank Gerhard Hochschild, George Seligman, and Ferdinand Veldkamp. I also want to thank Michael J. DeRise for his help. Finally, I want to acknowledge the support of the National Science Foundation and the excellent typing of Helen Samoraj and her staff.

James E. Humphreys

Conventions

K^* = multiplicative group of the field K
char K = characteristic of K
char exp K = characteristic exponent of K, i.e., max $\{1, \text{char } K\}$
det = determinant
Tr = trace
Card = cardinality
$\perp\!\!\!\perp$ = direct sum

Table of Contents

I. Algebraic Geometry 1

0. Some Commutative Algebra 1

1. Affine and Projective Varieties 4
   - 1.1 Ideals and Affine Varieties 4
   - 1.2 Zariski Topology on Affine Space 6
   - 1.3 Irreducible Components 7
   - 1.4 Products of Affine Varieties 9
   - 1.5 Affine Algebras and Morphisms 9
   - 1.6 Projective Varieties 11
   - 1.7 Products of Projective Varieties 13
   - 1.8 Flag Varieties 14

2. Varieties 16
   - 2.1 Local Rings 16
   - 2.2 Prevarieties 17
   - 2.3 Morphisms 18
   - 2.4 Products 20
   - 2.5 Hausdorff Axiom 22

3. Dimension 24
   - 3.1 Dimension of a Variety 24
   - 3.2 Dimension of a Subvariety 25
   - 3.3 Dimension Theorem 26
   - 3.4 Consequences 28

4. Morphisms 29
   - 4.1 Fibres of a Morphism 29
   - 4.2 Finite Morphisms 31
   - 4.3 Image of a Morphism 32
   - 4.4 Constructible Sets 33
   - 4.5 Open Morphisms 34
   - 4.6 Bijective Morphisms 34
   - 4.7 Birational Morphisms 36

5. Tangent Spaces 37
   - 5.1 Zariski Tangent Space 37
   - 5.2 Existence of Simple Points 39
   - 5.3 Local Ring of a Simple Point 40
   - 5.4 Differential of a Morphism 42
   - 5.5 Differential Criterion for Separability 43

6. Complete Varieties 45
6.1 Basic Properties 45
6.2 Completeness of Projective Varieties 46
6.3 Varieties Isomorphic to $\mathbf{P}^1$ 47
6.4 Automorphisms of $\mathbf{P}^1$ 47

II. Affine Algebraic Groups **51**

7. Basic Concepts and Examples 51
7.1 The Notion of Algebraic Group 51
7.2 Some Classical Groups 52
7.3 Identity Component 53
7.4 Subgroups and Homomorphisms. 54
7.5 Generation by Irreducible Subsets 55
7.6 Hopf Algebras 56

8. Actions of Algebraic Groups on Varieties 58
8.1 Group Actions 58
8.2 Actions of Algebraic Groups 59
8.3 Closed Orbits 60
8.4 Semidirect Products 61
8.5 Translation of Functions 61
8.6 Linearization of Affine Groups 62

III. Lie Algebras **65**

9. Lie Algebra of an Algebraic Group 65
9.1 Lie Algebras and Tangent Spaces 65
9.2 Convolution 66
9.3 Examples 67
9.4 Subgroups and Lie Subalgebras 68
9.5 Dual Numbers 69

10. Differentiation 70
10.1 Some Elementary Formulas 71
10.2 Differential of Right Translation 71
10.3 The Adjoint Representation 72
10.4 Differential of Ad 73
10.5 Commutators 75
10.6 Centralizers 76
10.7 Automorphisms and Derivations 76

IV. Homogeneous Spaces **79**

11. Construction of Certain Representations 79
11.1 Action on Exterior Powers 79
11.2 A Theorem of Chevalley 80
11.3 Passage to Projective Space 80

11.4 Characters and Semi-Invariants 81
11.5 Normal Subgroups 82

12. Quotients 83
12.1 Universal Mapping Property 83
12.2 Topology of Y 84
12.3 Functions on Y 84
12.4 Complements 85
12.5 Characteristic 0 85

V. Characteristic 0 Theory **87**

13. Correspondence Between Groups and Lie Algebras . . 87
13.1 The Lattice Correspondence 87
13.2 Invariants and Invariant Subspaces 88
13.3 Normal Subgroups and Ideals 88
13.4 Centers and Centralizers 89
13.5 Semisimple Groups and Lie Algebras 89

14. Semisimple Groups 90
14.1 The Adjoint Representation 90
14.2 Subgroups of a Semisimple Group 91
14.3 Complete Reducibility of Representations . . . 92

VI. Semisimple and Unipotent Elements **95**

15. Jordan-Chevalley Decomposition 95
15.1 Decomposition of a Single Endomorphism . . . 95
15.2 $\mathrm{GL}(n, \mathsf{K})$ and $\mathfrak{gl}(n, \mathsf{K})$ 97
15.3 Jordan Decomposition in Algebraic Groups . . 98
15.4 Commuting Sets of Endomorphisms 99
15.5 Structure of Commutative Algebraic Groups . . 100

16. Diagonalizable Groups 101
16.1 Characters and d-Groups 101
16.2 Tori 103
16.3 Rigidity of Diagonalizable Groups 105
16.4 Weights and Roots 106

VII. Solvable Groups **109**

17. Nilpotent and Solvable Groups 109
17.1 A Group-Theoretic Lemma 109
17.2 Commutator Groups 110
17.3 Solvable Groups 110
17.4 Nilpotent Groups 111
17.5 Unipotent Groups 112
17.6 Lie-Kolchin Theorem 113

18. Semisimple Elements 115
18.1 Global and Infinitesimal Centralizers 116
18.2 Closed Conjugacy Classes 117
18.3 Action of a Semisimple Element on a Unipotent Group 118
18.4 Action of a Diagonalizable Group 119

19. Connected Solvable Groups 121
19.1 An Exact Sequence 122
19.2 The Nilpotent Case 122
19.3 The General Case 123
19.4 Normalizer and Centralizer 124
19.5 Solvable and Unipotent Radicals 125

20. One Dimensional Groups 126
20.1 Commutativity of G 126
20.2 Vector Groups and e-Groups 127
20.3 Properties of p-Polynomials 128
20.4 Automorphisms of Vector Groups 130
20.5 The Main Theorem 131

VIII. Borel Subgroups **133**

21. Fixed Point and Conjugacy Theorems 133
21.1 Review of Complete Varieties 133
21.2 Fixed Point Theorem 134
21.3 Conjugacy of Borel Subgroups and Maximal Tori . 134
21.4 Further Consequences 136

22. Density and Connectedness Theorems 138
22.1 The Main Lemma 138
22.2 Density Theorem 139
22.3 Connectedness Theorem 140
22.4 Borel Subgroups of $C_G(S)$ 141
22.5 Cartan Subgroups: Summary 142

23. Normalizer Theorem 143
23.1 Statement of the Theorem 143
23.2 Proof of the Theorem 144
23.3 The Variety G/B 145
23.4 Summary 145

IX. Centralizers of Tori **147**

24. Regular and Singular Tori 147
24.1 Weyl Groups 147
24.2 Regular Tori 149
24.3 Singular Tori and Roots 149
24.4 Regular 1-Parameter Subgroups 150

25. Action of a Maximal Torus on G/B 151
25.1 Action of a 1-Parameter Subgroup 152
25.2 Existence of Enough Fixed Points 153
25.3 Groups of Semisimple Rank 1 154
25.4 Weyl Chambers 156

26. The Unipotent Radical 157
26.1 Characterization of $R_u(G)$ 158
26.2 Some Consequences 159
26.3 The Groups U_α 160

X. Structure of Reductive Groups **163**

27. The Root System 163
27.1 Abstract Root Systems 163
27.2 The Integrality Axiom 164
27.3 Simple Roots 165
27.4 The Automorphism Group of a Semisimple Group . 166
27.5 Simple Components 167

28. Bruhat Decomposition 169
28.1 T-Stable Subgroups of B_u 169
28.2 Groups of Semisimple Rank 1 171
28.3 The Bruhat Decomposition 172
28.4 Normal Form in G 173
28.5 Complements 173

29. Tits Systems 175
29.1 Axioms 176
29.2 Bruhat Decomposition 177
29.3 Parabolic Subgroups 177
29.4 Generators and Relations for W 179
29.5 Normal Subgroups of G 181

30. Parabolic Subgroups 183
30.1 Standard Parabolic Subgroups 183
30.2 Levi Decompositions 184
30.3 Parabolic Subgroups Associated to Certain Unipotent Groups 185
30.4 Maximal Subgroups and Maximal Unipotent Subgroups 187

XI. Representations and Classification of Semisimple Groups **188**

31. Representations 188
31.1 Weights 188
31.2 Maximal Vectors 189
31.3 Irreducible Representations 190
31.4 Construction of Irreducible Representations . . 191

31.5 Multiplicities and Minimal Highest Weights . . . 193
31.6 Contragredients and Invariant Bilinear Forms . . 193

32. Isomorphism Theorem 195
32.1 The Classification Problem 195
32.2 Extension of φ_T to $N(T)$ 198
32.3 Extension of φ_T to Z_α 199
32.4 Extension of φ_T to TU_α 201
32.5 Extension of φ_T to B 203
32.6 Multiplicativity of φ 204

33. Root Systems of Rank 2 207
33.1 Reformulation of (A), (B), (C) 207
33.2 Some Preliminaries 208
33.3 Type A_2 209
33.4 Type B_2 211
33.5 Type G_2 212
33.6 The Existence Problem 215

XII. Survey of Rationality Properties **217**

34. Fields of Definition 217
34.1 Foundations 217
34.2 Review of Earlier Chapters 218
34.3 Tori 219
34.4 Some Basic Theorems 219
34.5 Borel-Tits Structure Theory 220
34.6 An Example: Orthogonal Groups 221

35. Special Cases 222
35.1 Split and Quasisplit Groups 223
35.2 Finite Fields 224
35.3 The Real Field 224
35.4 Local Fields 225
35.5 Classification 226

Appendix. Root Systems 229

Bibliography 233

Index of Terminology 247

Index of Symbols 251

Chapter I

Algebraic Geometry

0. Some Commutative Algebra

Algebraic geometry is heavily dependent on commutative algebra, the study of commutative rings and fields (notably those arising from polynomial rings in many variables); indeed, it is impossible to draw a sharp line between the geometry and the algebra. For reference, we assemble in this section some basic concepts and results (without proof) of an algebraic nature. The theorems stated are in most cases "standard" and readily accessible in the literature, though not always encountered in a graduate algebra course.

We shall give explicit references, usually by chapter and section, to the following books:

L = S. Lang, Algebra, Reading, Mass.: Addison-Wesley 1965.

ZS = O. Zariski, P. Samuel, Commutative Algebra, 2 vol., Princeton: Van Nostrand 1958, 1960.

AM = M. F. Atiyah, I. G. Macdonald, Introduction to Commutative Algebra, Reading, Mass.: Addison-Wesley 1969.

J = N. Jacobson, Basic Algebra II, San Francisco: W. H. Freeman 1980.

There are of course other good sources for this material, e.g., Bourbaki or van der Waerden. We remark that [AM] is an especially suitable reference for our purposes, even though some theorems there are set up as exercises.

All rings are assumed to be commutative (with 1).

0.1 *A ring R is* **noetherian** $\Leftrightarrow$ *each ideal of R is finitely generated* $\Leftrightarrow$ *R has* ACC *(ascending chain condition) on ideals* $\Leftrightarrow$ *each nonempty collection of ideals has a maximal element, relative to inclusion. Any homomorphic image of a noetherian ring is noetherian.* [L, *VI* §1] [AM, *Ch. 6, 7*]. **Hilbert Basis Theorem:** *If R is noetherian, so is* $R[\mathsf{T}]$ *(polynomial ring in one indeterminate). In particular, for a field* K, $\mathsf{K}[\mathsf{T}_1, \mathsf{T}_2, \ldots, \mathsf{T}_n]$ *is noetherian.* [L, *VI* §2] [ZS, *IV* §1] [AM, *7.5*].

0.2 *If* K *is a field,* $\mathsf{K}[\mathsf{T}_1, \ldots, \mathsf{T}_n]$ *is a* UFD *(unique factorization domain).* [L, *V* §6].

0.3 Weak Nullstellensatz: *Let* K *be a field,* $\mathsf{L} = \mathsf{K}[x_1, \ldots, x_n]$ *a finitely generated extension ring of* K. *If* L *is a field, then all* x_i *are algebraic over* K. [L, *X* §2] [ZS, *VII* §3] [AM, *5.24; Ch. 5, ex. 18; 7.9*].

0.4 *Let* L/K *be a field extension. Elements* $x_1, \ldots, x_d \in \mathsf{L}$ *are* **algebraically independent** *over* K *if no nonzero polynomial* $f(\mathsf{T}_1, \ldots, \mathsf{T}_d)$ *over* K *satisfies*

$f(x_1, \ldots, x_d) = 0$. *A maximal subset of* L *algebraically independent over* K *is called a* **transcendence basis** *of* L/K. *Its cardinality is a uniquely defined number, the* **transcendence degree** $\text{tr. deg.}_{\mathsf{K}} \mathsf{L}$. *If* $\mathsf{L} = \mathsf{K}(x_1, \ldots, x_n)$, *a transcendence basis can be chosen from among the* x_i, *say* $x_1, \ldots, x_d$. *Then* $\mathsf{K}(x_1, \ldots, x_d)$ *is* **purely transcendental** *over* K *and* $\mathsf{L}/\mathsf{K}(x_1, \ldots, x_d)$ *is (finite) algebraic.* [L, *X* §1] [ZS, *II* §12] [J, *8.12*].

Lüroth Theorem: *Let* $\mathsf{L} = \mathsf{K}(\mathsf{T})$ *be a simple, purely transcendental extension of* K. *Then any subfield of* L *properly including* K *is also a simple, purely transcendental extension.* [J, *8.13*].

0.5 *Let* E/F *be a finite field extension. There is a map* $N_{\mathsf{E}/\mathsf{F}}: \mathsf{E} \to \mathsf{F}$, *called the* **norm**, *which induces a homomorphism of multiplicative groups* $\mathsf{E}^* \to \mathsf{F}^*$, *such that* $N_{\mathsf{E}/\mathsf{F}}(a)$ *is a power of the constant term of the minimal polynomial of* a *over* F, *and in particular,* $N_{\mathsf{E}/\mathsf{F}}(a) = a^{[\mathsf{E}:\mathsf{F}]}$ *whenever* $a \in \mathsf{F}$. *To define the norm, view* E *as a vector space over* F. *For each* $a \in \mathsf{E}$, $x \mapsto ax$ *defines a linear transformation* $\mathsf{E} \to \mathsf{E}$; *let* $N_{\mathsf{E}/\mathsf{F}}(a)$ *be its determinant.* [L, *VIII* §5] [ZS, *II* §10].

0.6 *Let* $R \supset S$ *be an extension of rings. An element* $x \in R$ *is* **integral** *over* $S \Leftrightarrow x$ *is a root of a monic polynomial over* $S \Leftrightarrow$ *the subring* $S[x]$ *of* R *is a finitely generated* S*-module* $\Leftrightarrow$ *the ring* $S[x]$ *acts on some finitely generated* S*-module* V *faithfully (i.e.,* $y.V = 0$ *implies* $y = 0$). R *is* **integral** *over* S *if each element of* R *is integral over* S. *The* **integral closure** *of* S *in* R *is the set (a subring) of* R *consisting of all elements of* R *integral over* S. *If* R *is an integral domain, with field of fractions* F, R *is said to be* **integrally closed** *if* R *equals its integral closure in* F. *If* R *is integrally closed, so is the polynomial ring* $R[\mathsf{T}]$. [L, *IX* §1] [ZS, *V* §1] [AM, *Ch. 5*]

0.7 Noether Normalization Lemma: *Let* K *be an arbitrary field,* $R = \mathsf{K}[x_1, \ldots, x_n]$ *a finitely generated integral domain over* K *with field of fractions* F, $d = \text{tr. deg.}_{\mathsf{K}} \mathsf{F}$. *Then there exist elements* $y_1, \ldots, y_d \in R$ *such that* R *is integral over* $\mathsf{K}[y_1, \ldots, y_d]$ *(and the* y_i *are algebraically independent over* K). [L, *X* §4] [ZS, *V* §4] [AM, *Ch. 5, ex. 16*].

0.8 *Let* R/S *be a ring extension, with* R *integral over* S.

Going Up Theorem: *If* P *is a prime (resp. maximal) ideal of* S, *there exists a prime (resp. maximal) ideal* Q *of* R *for which* $Q \cap S = P$. [L, *IX* §1] [ZS, *V* §2] [AM, *5.10, 5.11*].

Going Down Theorem: *Let* S *be integrally closed. If* $P_1 \supset P_2$ *are prime ideals of* S, Q_1 *a prime ideal of* R *for which* $Q_1 \cap S = P_1$, *there exists a prime ideal* $Q_2 \subset Q_1$ *for which* $Q_2 \cap S = P_2$. [ZS, *V* §3] [AM, *5.16*].

Extension Theorem: *Let* R/S *be an integral extension,* K *an algebraically closed field. Then any homomorphism* $\varphi: S \to \mathsf{K}$ *extends to a homomorphism* $\varphi': R \to \mathsf{K}$. *If* $x \in R$, $a \in \mathsf{K}$, φ *can first be extended to a homomorphism* $S[x] \to \mathsf{K}$

sending x to a (then be further extended to R, R being integral over $S[x]$), provided $f(x) = 0$ implies $f_\varphi(a) = 0$ for $f(\mathsf{T}) \in S[\mathsf{T}]$ ($f_\varphi(\mathsf{T})$ the polynomial over K gotten by applying φ to each coefficient of $f(\mathsf{T})$). [L, *IX* §3] [AM, *Ch. 5*].

0.9 *Let $P_1, \ldots, P_n$ be prime ideals in a ring R. If an ideal lies in the union of the P_i, it must already lie in one of them.* [ZS, *IV* §6, *Remark p. 215*].

0.10 *Let S be a* **multiplicative set** *in a ring R ($0 \notin S$, $1 \in S$, $a, b \in S \Rightarrow ab \in S$). The* **generalized ring of quotients** *$S^{-1}R$ is constructed using equivalence classes of pairs $(r, s) \in R \times S$, where $(r, s) \sim (r', s')$ means that for some $s'' \in S$, $s''(rs' - r's) = 0$. The (prime) ideals of $S^{-1}R$ correspond bijectively to the (prime) ideals of R not meeting S. In case R is an integral domain, with field of fractions F, $S^{-1}R$ may be identified with the set of fractions r/s in F. In general, the canonical map $R \to S^{-1}R$ (sending r to the class of $(r, 1)$) is injective only when S contains no zero divisors. For example, take $S = \{x^n | n \in \mathbb{Z}^+\}$ for x not nilpotent, to obtain $S^{-1}R$, denoted R_x; R is a subring of R_x provided x is not a zero divisor. Or take $S = R - P$, P a prime ideal. Then $S^{-1}R$ is denoted R_P and is a* **local ring** *(i.e., has a unique maximal ideal PR_P, consisting of the nonunits of R_P). The prime ideals of R_P correspond naturally to the prime ideals of R contained in P. If R is an integrally closed domain, then so is R_P. If R is noetherian, so is R_P. If M is a maximal ideal, the fields R/M and R_M/MR_M are naturally isomorphic; the canonical map $R \to R_M$ induces a vector space isomorphism of M/M^2 onto $MR_M/(MR_M)^2$.* [L, *II* §3] [AM, *Ch. 3*].

0.11 Nakayama Lemma: *Let R be a ring, M a maximal ideal, V a finitely generated R-module for which $V = MV$. Then there exists $x \notin M$ such that $xV = 0$. In particular, if R is local (with unique maximal ideal M), x must be a unit and therefore $V = 0$.* [AM, *2.5, 2.6*] [L, *IX* §1].

0.12 *If R is a (noetherian) local ring with maximal ideal M, the powers of M can be taken as a fundamental system of neighborhoods of 0 for a topology (the M-***adic topology***) on R. This topology is Hausdorff, since $\bigcap M^n = 0$.* [AM, §10] [ZS, *IV* §7, *VIII* §2]. *The* **Krull dimension** *of R is the maximum length k of a chain of prime ideals $0 \subsetneqq P_1 \subsetneqq P_2 \subsetneqq \cdots \subsetneqq P_k \subsetneqq R$. If this equals the minimum number of generators of M, R is called* **regular**. **Theorem:** *A regular local ring is an integral domain, integrally closed (in its field of fractions).* [AM, *Ch. 11*] [ZS, *VIII* §11; *cf. Appendix 7*].

0.13 *Let I be an ideal in a noetherian ring R, and let $P_1, \ldots, P_t$ be the minimal prime ideals containing I. The image of $P_1 \cap \cdots \cap P_t$ in R/I is the nilradical of R/I, a nilpotent ideal. In particular, for large enough n, $P_1^n P_2^n \cdots P_t^n \subset (P_1 \cap \cdots \cap P_t)^n \subset I$.* [AM, *7.15*] [L, *VI* §4].

0.14 *A field extension E/F is* **separable** *if either $\operatorname{char} \mathsf{F} = 0$, or else $\operatorname{char} \mathsf{F} = p > 0$ and the p^{th} powers of elements $x_1, \ldots, x_n \in \mathsf{E}$ linearly independent over F are again so. This generalizes the usual notion when E/F is finite.*

$E = F(x_1, \ldots, x_n)$ *is* **separably generated** *over* F *if* E *is a finite separable extension of a purely transcendental extension of* F. *For finitely generated extensions* E/F, "*separably generated*" *is equivalent to* "*separable*", *and* E/F *is automatically separable when* F *is perfect. If* $F \subset L \subset E$, E/F *separable, then* L/F *is separable. If* $F \subset L \subset E$, E/L *and* L/F *separable, then* E/F *is separable* [ZS, *II* §13] [L, *X* §6] [J, *8.14*].

0.15 *A* **derivation** $\delta: E \to L$ (E *a field*, L *an extension field of* E), *is a map which satisfies* $\delta(x + y) = \delta(x) + \delta(y)$ *and* $\delta(xy) = x\,\delta(y) + \delta(x)\,y$. *If* F *is a subfield of* E, δ *is called an* F-**derivation** *if in addition* $\delta(x) = 0$ *for all* $x \in F$ (*so* δ *is* F-*linear*). *The space* $\mathrm{Der}_F(E, L)$ *of all* F-*derivations* $E \to L$ *is a vector space over* L, *whose dimension is* $\mathrm{tr.deg.}_F E$ *if* E/F *is separably generated.* E/F *is separable if and only if all derivations* $F \to L$ *extend to derivations* $E \to L$ (L *an extension field of* E). *If* $\mathrm{char}\, E = p > 0$, *all derivations of* E *vanish on the subfield* E^p *of* p^{th} *powers.* [ZS, *II* §17] [J, *8.15*] [L, *X* §7].

1. Affine and Projective Varieties

In this section we consider subsets of affine or projective space defined by polynomial equations, with special attention being paid to the way in which geometric properties of these sets translate into algebraic properties of polynomial rings. K always denotes an algebraically closed field, of arbitrary characteristic.

1.1. Ideals and Affine Varieties

The set $K^n = K \times \cdots \times K$ will be called **affine n-space** and denoted $\mathbf{A}^n$. By **affine variety** will be meant (provisionally) the set of common zeros in $\mathbf{A}^n$ of a finite collection of polynomials. Evidently we have in mind curves, surfaces, and the like. But the collection of polynomials defining a geometric configuration can vary quite a bit without affecting the geometry, so we aim for a tighter correspondence between geometry and algebra. As a first step, notice that the ideal in $K[T] = K[T_1, \ldots, T_n]$ generated by a set of polynomials $\{f_\alpha(T)\}$ has precisely the same common zeros as $\{f_\alpha(T)\}$. Moreover, the Hilbert Basis Theorem (0.1) asserts that each ideal in $K[T]$ has a finite set of generators, so every ideal corresponds to an affine variety. Unfortunately, this correspondence is not 1–1: e.g., the ideals generated by T and by T^2 are distinct, but have the same zero set $\{0\}$ in $\mathbf{A}^1$. We shall see shortly how to deal with this phenomenon.

Formally, we can assign to each ideal I in $K[T]$ the set $\mathscr{V}(I)$ of its common zeros in $\mathbf{A}^n$, and to each subset $X \subset \mathbf{A}^n$ the collection $\mathscr{I}(X)$ of all polynomials vanishing on X. It is clear that $\mathscr{I}(X)$ is an ideal, and that we have inclusions:

$$X \subset \mathscr{V}(\mathscr{I}(X)),$$
$$I \subset \mathscr{I}(\mathscr{V}(I)).$$

Of course, neither of these need be an equality (examples?). Let us examine more closely the second inclusion. By definition, the **radical** $\sqrt{I}$ of an ideal I is $\{f(\mathsf{T}) \in \mathsf{K}[\mathsf{T}] \mid f(\mathsf{T})^r \in I \text{ for some } r \geqslant 0\}$. This is easily seen to be an ideal, including I. If $f(\mathsf{T})$ fails to vanish at $x = (x_1, \ldots, x_n)$, then $f(\mathsf{T})^r$ also fails to vanish at x for each $r \geqslant 0$. From this it follows that $\sqrt{I} \subset \mathscr{I}(\mathscr{V}(I))$, which refines the above inclusion. Indeed, we now get equality—a fact which is crucial but not at all intuitively obvious.

Theorem (Hilbert's Nullstellensatz). *If I is any ideal in $\mathsf{K}[\mathsf{T}_1, \ldots, \mathsf{T}_n]$, then $\sqrt{I} = \mathscr{I}(\mathscr{V}(I))$.*

Proof. In view of the finite generation of I, the theorem is equivalent to the statement: "Given $f(\mathsf{T}), f_1(\mathsf{T}), \ldots, f_s(\mathsf{T})$ in $\mathsf{K}[\mathsf{T}]$, such that $f(\mathsf{T})$ vanishes at every commor zero of the $f_i(\mathsf{T})$ in $\mathbf{A}^n$, there exist $r \geqslant 0$ and $g_1(T), \ldots, g_s(T) \in \mathsf{K}[\mathsf{T}]$ for which $f(\mathsf{T})^r = \sum_{i=1}^{s} g_i(\mathsf{T}) f_i(\mathsf{T})$."

We show first that this statement follows from the assertion:

(*) $$\text{If } \mathscr{V}(I) = \emptyset \quad \text{then} \quad I = \mathsf{K}[\mathsf{T}].$$

(Notice that this is just a special case of the theorem, since only the ideal $\mathsf{K}[\mathsf{T}]$ can have $\mathsf{K}[\mathsf{T}]$ as radical!) Indeed, given $f(\mathsf{T}), f_1(\mathsf{T}), \ldots, f_s(\mathsf{T})$ as indicated, we can introduce a new indeterminate T_0 and consider the collection of polynomials in $n+1$ indeterminates, $f_1(\mathsf{T}), \ldots, f_s(\mathsf{T}), 1 - \mathsf{T}_0 f(\mathsf{T})$. These have no common zero in $\mathbf{A}^{n+1}$, thanks to the original condition imposed on $f(\mathsf{T})$, so (*) implies that they generate the unit ideal. Find polynomials $h_i(\mathsf{T}_0, \ldots, \mathsf{T}_n)$ and $h(\mathsf{T}_0, \ldots, \mathsf{T}_n)$ for which $1 = h_1(\mathsf{T}_0, \mathsf{T}) f_1(\mathsf{T}) + \cdots + h_s(\mathsf{T}_0, \mathsf{T}) f_s(\mathsf{T}) + h(\mathsf{T}_0, \mathsf{T})(1 - \mathsf{T}_0 f(\mathsf{T}))$. Then substitute $1/f(\mathsf{T})$ for T_0 throughout, and multiply both sides by a sufficiently high power $f(\mathsf{T})^r$ to clear denominators. This yields a relation of the desired sort.

It remains to prove (*), or equivalently, to show that a proper ideal in $\mathsf{K}[\mathsf{T}]$ has at least one common zero in $\mathbf{A}^n$. (In the special case $n = 1$, this would follow directly from the fact that K is algebraically closed.) Let us attempt naively to construct a common zero. By Zorn's Lemma, I lies in some maximal ideal of $\mathsf{K}[\mathsf{T}]$, and common zeros of the latter will serve for I as well; so we might as well assume that I is maximal. Then the residue class ring $\mathsf{L} = \mathsf{K}[\mathsf{T}]/I$ is a *field*; K may be identified with the residue classes of scalar polynomials. If we write t_i for the residue class of T_i, it is clear that $\mathsf{L} = \mathsf{K}[t_1, \ldots, t_n]$ (the smallest subring of L containing K and the t_i). Moreover, the n-tuple $(t_1, \ldots, t_n)$ is by construction a common zero of the polynomials in I. If we could identify L with K, the t_i could already be found inside K. But K is algebraically closed, so for this it would be enough to show that the t_i are *algebraic* over K, which is precisely the content of (0.3). □

The Nullstellensatz ("zeros theorem") implies that the operators $\mathscr{V}, \mathscr{I}$ set up a 1–1 correspondence between the collection of all **radical ideals** in $\mathsf{K}[\mathsf{T}]$ (ideals equal to their radical) and the collection of all affine varieties in $\mathbf{A}^n$.

Indeed, if $X = \mathscr{V}(I)$, then $\mathscr{I}(X) = \mathscr{I}(\mathscr{V}(I)) = \sqrt{I}$, so that X may be recovered as $\mathscr{V}(\mathscr{I}(X))$ (I and $\sqrt{I}$ having the same set of common zeros). On the other hand, if $I = \sqrt{I}$, then I may be recovered as $\mathscr{I}(\mathscr{V}(I))$. Notice that the correspondences $X \mapsto \mathscr{I}(X)$ and $I \mapsto \mathscr{V}(I)$ are *inclusion-reversing*. So the noetherian property of $\mathsf{K}[\mathsf{T}]$ implies DCC (descending chain condition) on the collection of affine varieties in $\mathbf{A}^n$.

Examples of radical ideals are *prime* (in particular, *maximal*) ideals. We shall examine in (1.3) the varieties corresponding to prime ideals. For the moment, just consider the case $X = \mathscr{V}(I)$, I maximal. The Nullstellensatz guarantees that X is nonempty, so let $x \in X$. Clearly $I \subset \mathscr{I}(\{x\}) \subsetneq \mathsf{K}[\mathsf{T}]$, so $I = \mathscr{I}(\{x\})$ by maximality, and $X = \mathscr{V}(I) = \mathscr{V}(\mathscr{I}(\{x\})) = \{x\}$. On the other hand, if $x \in \mathbf{A}^n$, then $f(\mathsf{T}) \mapsto f(x)$ defines a homomorphism of $\mathsf{K}[\mathsf{T}]$ onto K, whose kernel $\mathscr{I}(\{x\})$ is maximal because K is a field. Thus the points of $\mathbf{A}^n$ correspond 1–1 to the maximal ideals of $\mathsf{K}[\mathsf{T}]$.

A **linear variety** through $x \in \mathbf{A}^n$ is the zero set of linear polynomials of the form $\sum a_i(\mathsf{T}_i - x_i)$. This is just a vector subspace of $\mathbf{A}^n$ if the latter is viewed as a vector space with origin x. From the Nullstellensatz (or linear algebra!) we deduce that any linear polynomial vanishing on such a variety is a K-linear combination of the given ones.

1.2. Zariski Topology on Affine Space

If K were the field of complex numbers, $\mathbf{A}^n$ could be given the usual topology of complex n-space. Then the zero set of a polynomial $f(\mathsf{T})$ would be closed, being the inverse image of the closed set $\{0\}$ in $\mathbf{C}$ under the continuous mapping $x \mapsto f(x)$. The set of common zeros of a collection of polynomials would equally well be closed, being the intersection of closed sets. Of course, complex n-space has plenty of other closed sets which are unobtainable in this way, as is clear already in case $n = 1$.

The idea of topologizing affine n-space by decreeing that the **closed** sets are to be precisely the affine varieties turns out to be very fruitful. This is called the **Zariski topology**. Naturally, it has to be checked that the axioms for a topology are satisfied: (1) $\mathbf{A}^n$ and $\emptyset$ are certainly closed, as the respective zero sets of the ideals (0) and $\mathsf{K}[\mathsf{T}]$. (2) If I, J are two ideals, then clearly $\mathscr{V}(I) \cup \mathscr{V}(J) \subset \mathscr{V}(I \cap J)$. To establish the reverse inclusion, suppose x is a zero of $I \cap J$, but not of I or J. Say $f(\mathsf{T}) \in I$, $g(\mathsf{T}) \in J$, with $f(x) \neq 0$, $g(x) \neq 0$. Since $f(\mathsf{T})g(\mathsf{T}) \in I \cap J$, we must have $f(x)g(x) = 0$, which is absurd. This argument implies that finite unions of closed sets are closed. (3) Let I_α be an arbitrary collection of ideals, so $\sum_\alpha I_\alpha$ is the ideal generated by this collection. Then it is clear that $\bigcap_\alpha \mathscr{V}(I_\alpha) = \mathscr{V}(\sum_\alpha I_\alpha)$, i.e., arbitrary intersections of closed sets are closed.

What sort of topology is this? Points are closed, since $x = (x_1, \ldots, x_n)$ is the only common zero of the polynomials $\mathsf{T}_1 - x_1, \ldots, \mathsf{T}_n - x_n$. But the Hausdorff separation axiom fails. This is evident already in the case of $\mathbf{A}^1$,