Bourbaki algebra commutative pdf download full free full

I'm not robot!

 ACTUALITES SCIENTIFIQUES E T INDUSTRIELLES HERMA" N I C O L A S BOURBAKI ADIWES INTERNATIONAL SERIES IN MATHEMATICS A. J. Lohwater, Consulting Editor Elements of Mathematics N I C O L A S BOURBAKI Elements of Mathematics English Translations published: General Topology, Part I, 1966 General Topology, Part 11, 1966 Theory of Sets, 1968 Commutative Algebra, 1972 Commutative Algebra In firebaration : Algebra, Part I Algebra, Part I1 Functions of a Real Variable Integration Lie Groups and Lie Algebras Spectral Theories Topological Vector Spaces H E R M A N N , P U B L I S H E R S I N ARTS A N D SCIENCE 293 rue Lecourbe, Paris XV, France A W A D D I S O N - W E S L E Y P U B L I S H I N G COMPANY Advanced Book Program Reading, Massachusetts Originally published as ELEMENTS DE MATHEMATIQUE, ALGEBRE COMMUTATIVE 0 1964, 1965, 1968, 1969 by Hermann, Paris TO THE READER 1. This series of volumes, a list of which is given on pages ix and x, takes up mathematics at the beginning, and gives complete proofs. In principle, it requires no particular knowledge of mathematics on the reader’s part, but only a certain familiarity with mathematical reasoning and a certain capacity for abstract thought. Nevertheless, it is directed especially to those who have a good knowledge of at least the content of the first year or two of a university mathematics course. 2. The method of exposition we have chosen is axiomatic and abstract, and normally proceeds from the general to the particular. This choice has been dictated by the main purpose of the treatise, which is to provide a solid foundation for the whole body of modern mathematics. For this it is indispensable to become familiar with a rather large number of very general ideas and principles. Moreover, the demands of proof impose a rigorously fixed order on the subject matter. It follows that the utility of certain considerations will not be immediately apparent to the reader unless he has already a fairly extended knowledge of mathematics; otherwise he must have the patience to suspend judgment until the occasion arises. ISBN 0-201-00644-8 Library of Congress catalog card number 70-1 78262 American Mathematical Society (MOS) Subject Classification Scheme (1970) : 13-02, 13A05, 13A15 Printed in Great Britain . 3. In order to mitigate this disadvantage we have frequently inserted examples in the text which refer to facts the reader may already know but which have not yet been discussed in the series. Such examples are always placed between two asterisks: * . . . *. Most readers will undoubtedly find that these examples will help them to understand the text, and will prefer not to leave them out, even at a first reading. Their omission would of course have no disadvantage, from a purely logical point of view. 4. This series is divided into volumes (here called “Books”). The first six 0 1972 by Hermann. All rights reserved This book, or parts thereof, may not be reproduced in any form without the publisher’s written permission h o k s are numbered and, in general, every statement in the text assumes as known only those results which have already been discussed in the preceding V TO THE READER TO THE READER volumes. This rule holds good within each Book, but for convenience of exposition these Books are no longer arranged in a consecutive order. At the beginning of each of these Books (or of these chapters), the reader will find a precise indication of its logical relationship to the other Books and he will thus be able to satisfy himself of the absence of any vicious circle. tence to completeness ; in particular, references which serve only to determine questions of priority are almost always omitted. As to the exercises, we have not thought it worthwhile in general to indicate their origins, since they have been taken from many different sources (original papers, textbooks, collections of exercises). 5, The logical framework of each chapter consists of the definitions, the axioms, and the theorem of the chapter. These are the parts that have mainly to be borne in mind for subsequent use. Less important results and those which can easily be deduced from the theorems are labelled as “propositions,” “lemmas,” “corollaries,” “remarks,” etc. Those which may be omitted at a first reading are printed in small type. A commentary on a particularly important theorem appears occasionally under the name of “scholium.” T o avoid tedious repetitions it is sometimes convenient to introduce notations or abbreviations which are in force only within a certain chapter or a certain section of a chapter (for example, in a chapter which is concerned only with commutative rings, the word “ring” would always signify “commutative ring”). Such conventions are always explicitly mentioned, generally a t the beginning of the chapter in which they occur. 11. References to a part of this series are given as follows: a) If reference is made to theorems, axioms, or definitions presented in the same section, they are quoted by their number. b) If they occur in another section o f the same chapter, this section is also quoted in the reference. c) If they occur in another chapter in the same Book, the chapter and section are quoted. d) If they occur in another Book, this Book is first quoted by its title. The Summaries of Results are quoted by the letter R: thus Set Theory, R signifies “Summary of Results of the Theory o f Sets.” 6. Some passages in the text are designed to forewarn the reader against serious errors. These passages are signposted in the margin with the sign 2 (“dangerous bend”). 7. The Exercises are designed both to enable the reader to satisfy himself that he has digested the text and to bring to his notice results which have no place in the text but which are nonetheless of interest. The most difficult exercises bear the sign 7. 8. I n general, we have adhered to the commonly accepted terminology, except where there appeared to be good reasons for deviating from it. 9. We have made a particular effort always to use rigorously correct language, without sacrificingsimplicity. As far as possible we have drawn attention in the text to abuses of language, without which any mathematical text runs the risk of pedantry, not to say unreadability. 10. Since in principle the text consists of the dogmatic exposition of a theory, it contains in general no references to the literature. Bibliographical references are gathered together in Historical Notes, usually at the end of each chapter. These notes also contain indications, where appropriate, of the unsolved problems of the theory. The bibliography which follows each historical note contains in general only those books and original memoirs which have been of the greatest importance in the evolution of the theory under discussion. I t makes no sort of previ vii CONTENTS OF THE ELEMENTS OF MATHEMATICS SERIES I. THEORY OF SETS 1. Description of formal mathematics. 2. Theory of sets. 3. Ordered sets; cardinals; natural numbers. 4. Structures. 11. ALGEBRA 1. Algebraic structures. 2. Linear algebra. 3. Tensor algebras, exterior algebras, symmetric algebras. 4. Polynomials and rational fractions. 5. Fields. 6. Ordered groups and fields. 7. Modules over principal ideal rings. 8. Semi-simple modules and rings. 9. Sesquilinear and quadratic forms. 111. GENERAL TOPOLOGY 1. Topological structures. 2. Uniform structures. 3. Topological groups. 4. Real numbers. 5 . One-parameter groups. 6 . Real number spaces, a f i e and projective spaces. 7. The additive groups R". 8. Complex numbers. 9. Use of real numbers in general topology. 10. Function spaces. IV. FUNCTIONS OF A REAL VARIABLE 1. Derivatives. 2. Primitives and integrals. 3. Elementary functions. 4. Differential equations. 5. Local study of functions. 6 . Generalized Taylor expansions. The Euler-Maclaurin summation formula. 7. The gamma function. Dictionary. V. TOPOLOGICAL VECTOR SPACES 1. Topological vector spaces over a valued field. 2. Convex sets and locally convex spaces. 3. Spaces of continuous linear mappings. 4. Duality in topological vector spaces. 5. Hilbert spaces : elementary theory. Dictionary. VI. INTEGRATION 1. Convexity inequalities. 2. Riesz spaces. 3. Measures on locally compact spaces. 4. Extension of a measure. LP spaces. 5. Integration of measures. 6. Vectorial integration. 7. Haar measure. 8. Convolution and representation. 9. Integration on Hausdorff topological spaces. ix CONTENTS OF THE ELEMENTS OF MATHEMATICS SERIES CONTENTS LIE GROUPS AND LIE ALGEBRAS . . . . 4. Coxeter groups . 6 . Root systems. 1 Lie algebras 2 Free Lie algebras 3 Lie groups and Tits systems 5 . Groups generated by reflections COMMUTATIVE ALGEBRA . 1. Flat modules 2. Localization. 3 . Graduations, filtrations. and topologies. 4. Associated prime ideals and primary decomposition 5. Integers 6 Valuations 7 Divisors . . . . . . SPECTRAL THEORIES . . 2. Locally compact groups. 1 Normed algebras DIFFERENTIABLE AND ANALYTIC MANIFOLDS . Summary of results To THE READER .... CONTENTS OF THE ELEMENTS OF MATHEMATICS SERIES .... CHAPTERI . FLAT MODULES .... 5 1. Diagrams and exact sequences .... 1. Diagrams .... INTRODUCTION 2 . Commutative diagrams .... 3. Exact sequences .... 4. The snake diagram .... 5 2. Flat modules .... 1. Revision of tensor products .... 2. M-flat modules .... 3. Flat modules .... 4. Examples of flat modules .... 5. Flatness of quotient modules .... 6. Intersection properties .... 7. Tensor products of flat modules .... 8. Finitely presented modules .... 9 . Extension of scalars in homomorphism modules .... 10. Extension of scalars: case of commutative rings .... 1 1. Interpretation of flatness in terms of relations .... 5 3. Faithfully flat modules .... 1. Definition of faithhlly flat modules .... 2. Tensor products of faithfully flat modules .... 3. Change of ring .... V ix XiX 1 1 1 2 3 4 9 9 10 12 14 15 17 19 20 22 22 25 27 27 30 31 CONTENTS CONTENTS 4. Restriction of scalars .... 5 Faithfully flat rings .... 6. Faithfully flat rings and finiteness conditions .... 7 Linear equations over a faithfully flat ring .... 3 4. Flat modules and “Tor” functors .... Exercises for 3 1 .... Exercises for 3 2 .... Exercises for 4 3 .... 31 32 34 35 37 39 41 49 .... 50 CHAPTER I1 LOCALIZATION .... 3 1 Prime ideals .... 1 Definition of prime ideals .... 2. Relatively prime ideals .... 51 51 51 53 Exercises for $ 4 . . . 5 2 . Rings and modules of fractions .... 1 Definition of rings of fractions .... 2 Modules of fractions .... 3. Change of multiplicative subset .... 4 Properties of modules of fractions .... 5 Ideals in a ring of fractions .... 6. Nilradical and minimal prime ideals .... 7 Modules of fractions of tensor products and homomorphism modules .... 8. Application to algebras .... 9 Modules of fractions of graded modules .... 3 3. Local rings. Passage from the local to the global .... 1 Local rings .... 2. Modules over a local ring .... 3. Passage from the local to the global .... 4. Localization of flatness .... 5 Semi-local rings .... 3 4. Spectra of rings and supports of modules .... 1 Irreducible spaces .... 2. Noetherian topological spaces .... 3. The prime spectrum of a nng .... 4 The support of a module .... 3 5. Finitely . generated projective modules Invertible fractional ideals .... 1 Localization with respect to an element .... 2. Local characterization of finitely generated projective modules .... 3. Ranks of projective modules .... 4 Projective modules of rank 1 .... 5 Non-degenerate submodules .... 6 Invertible submodules .... 7 The group of classes of invertible modules .... 108 108 . . . 109 111 114 116 117 119 . ... 121 .... Exercises for 3 3 .... Exercises for 3 4 .... Exercises for 3 5 .... 123 CHAPTER 111. GRADUATIONS. FILTRATIONS AND TOPOLOGIES .... 1. Finitely generated graded algebras .... 1. Systems of generators of a commutative algebra .... 2 Criteria of finiteness for graded rings .... 3. Properties of the ring A(d) .... 4 Graded prime ideals .... 155 155 155 156 157 160 Exercisesfor§ 1 Exercises for 3 2 55 55 60 64 67 70 73 75 77 78 80 80 82 87 91 92 94 94 97 98 104 . . 3 2. General results on filtered rings and modules .... 1. Filtered rings and modules .... 2. The order function .... 136 140 146 162 162 165 3 The graded module associated with a filtered module .... 165 4 Homomorphisms compatible with filtrations .... 169 5 The topology defined by a filtration .... 170 6 Complete filtered modules .... 173 7 Linear compactness properties of complete filtered modules 176 8. The lift of homomorphisms of associated graded modules 177 9. The lift of families of elements of an associated graded module .... 179 10. Application: examples of Noetherian rings .... 183 11 Complete m-adic rings and inverse limits .... 185 12. The Hausdorff completion of a filtered module .... 187 13. The Hausdorff completion of a semi-local ring .... 192 . . . . . CONTENTS CONTENTS $ 3. m-adic topologies on Noetherian rings .... 1 Good filtrations .... 2. m-adic topologies on Noetherian rings .... 3 Zariski rings .... 4 . The Hausdorff completion of a Noetherian ring .... 5. The completion of a Zariski ring .... 195 195 199 201 202 206 Ej 4 Lifting in complete rings .... 1. Strongly relatively prime polynomials .... 2 . Restricted formal power series .... 3. Hensel’s Lemma .... 4 . Composition of systems of formal power series .... 5 . Systems of equations in complete rings .... 6 . Application to decompositions of rings .... 209 209 2 12 215 218 220 225 3 5. Flatness properties of filtered modules .... 1. Ideally Hausdorff modules .... 2 . Statement of the flatness criterion .... 3. Proof of the flatness criterion .... 4 . Applications .... 226 226 227 228 230 .... 232 Exercisesfor $ 1 Exercises for $ 2 Exercises for $ 3 Exercises for $ 4 Exercises for Ej 5 . CHAPTER IV ASSOCIATED PRIME IDEALS AND PRIMARY DECOMPOSITION Ej 1. Prime ideals associated with a module .... 1. Definition of associated prime ideals .... 2 Localization of associated prime ideals .... 3 Relations with the support .... 4 . The case of finitely generated modules over a Noetherian ring .... 1. Primary submodules .... 2 . The existence of a primary decomposition .... 3. Uniqueness properties in the primary decomposition .... 4. The localization of a primary decomposition .... tj 2. Primary decomposition 233 245 255 259 261 261 263 265 265 267 267 270 270 272 . 5 Rings and modules of finite length .... 274 6. Primary decomposition and extension of scalars .... 279 4 3. Primary decomposition in graded modules .... 283 1 Prime ideals associated with a graded module .... 283 2 Primary submodules corresponding to graded prime ideals 284 3 Primary decomposition in graded modules .... 285 . . . . Exercises for 3 2 .... Exercises for $ 3 .... Exercises for Ej 1 . . . 286 290 301 CHAPTERV INTEGERS .... 5 1. Notion of an integral element .... 1 Integral elements over a ring .... 2 The integral closure of a ring . Integrally closed domains 3. Examples of integrally closed domains .... 4 . Completely integrally closed domains .... 5. The integral closure of a ring of fractions .... 6. Norms and traces of integers .... 7. Extension of scalars in an integrally closed algebra ...... 8. Integers over a graded ring .... 9. Application: invariants of a group of automorphisms of an algebra .... 303 303 303 308 309 312 314 316 318 320 Ej 2 . The lift of prime ideals .... 1 The first existence theorem .... 2. Decomposition group and inertia group .... 3 Decomposition and inertia for integrally closed domains . . 4. The second existence theorem .... 325 325 330 337 343 Ej 3. Finitely generated algebras over a field .... 1. The normalization lemma .... 2 The integral closure of a finitely generated algebra over a field .... 3 The Nullstellensatz .... 4 Jacobson rings .... 344 344 .... Exercisesfor$2 .... Exercisesfor $ 3 .... 355 . . . . . Exercises for 5 1 323 348 349 351 362 370 CONrENTS CONTENTS CHAPTER VI . VALUATIONS .... $ 1. Valuation rings .... 1. The relation of domination between local rings .... 2 Valuation rings .... 3. Characterization of integral elements .... 4 Examples of valuation rings .... 375 375 375 376 378 379 $ 2. Places .... 1 The notion of morphism for laws of composition not everywhere defined .... 2. Places .... 3. Places and valuation rings .... 4. Extension of places .... 5. Characterization of integral elements by means of places . . 381 $ 3. Valuations .... 1. Valuations on a ring .... 2. Valuations on a field .... 3. Translations .... 4. Examples of valuations .... 5 . Ideals of a valuation ring .... 6. Discrete valuations .... 385 385 387 389 389 39 1 392 $ 4. The height of a valuation .... 1 Inclusion of valuation rings of the same field .... 2 Isolated subgroups of an ordered group .... 3. Comparison of valuations .... 4. The height of a valuation .... 5. Valuations of height 1 .... $ 5 . The topology defined by a valuation .... 1 The topology defined by a valuation .... 2. Topological vector spaces over a field with a valuation . . 3. The completion of a field with a valuation .... 393 393 394 395 396 397 . . . . . . $ 6. Absolute values .... 1. Preliminaries on absolute values .... 2 . Ultrametric absolute values .... 3. Absolute values on Q .... 4. Structure of fields with a non-ultrametric absolute value . . $ 7. Approximation theorem .... 1. The intersection of a finite number of valuation rings ... 2 . Independent valuations .... 3. The case of absolute values .... 381 381 383 384 385 399 399 40 1 402 403 403 405 406 407 412 412 413 415 $ 8. Extensions of a valuation to an algebraic extension .... 416 1. Ramification index. Residue class degree .... 416 2. fitension of a valuation and completion .... 418 . 3 The relation etfi < n .... 4 Initial ramification index .... 7 . . 420 422 5 The relation etfi = n .... 423 6 Valuation rings in an algebraic extension .... 427 428 7 The extension of absolute values .... $ 9. Application: locally compact fields .... 1 The modulus function on a locally compact field ...... 2 Existence of representatives .... 3. Structure of locally compact fields .... 431 431 432 433 $ 10. Extensions of a valuation to a transcendental extension ..... 1. The case of a monogenous transcendental extension .... 2. The rational rank of commutative group .... 3 The case of any transcendental extension .... 434 434 437 438 .... Exercises for $ 2 .... Exercises for $ 3 .... Exercises for $ 4 .... Exercises for 0 5 .... Exercises for $ 6 .... Exercises for $ 7 .... Exercises for 3 8 .... Exercises for 3 9 .... Exercises for $ 10 .... 441 . . . Exercises for $ 1 . C m R V I I DMSORS.................................... $ 1. Kmll domains.. 1 Divisorial ideals of an integral domain .... 2 The monoid structure on D(A) .... 3. Krull domains .... 444 446 449 454 459 460 461 470 471 475 475 475 478 480 CONTENTS CONTENTS 4. Essential valuations of a Krull domain .... 5. Approximation for essential valuations .... 6. Prime ideals of height 1 in a Krull domain .... 7 Application : new characterizations of discrete valuation rings .... 8. The integral closure of a Krull domain in a finite extension of its field of fractions .... 9 . Polynomial rings over a Krull domain .... 10. Divisor classes in Krull domains .... 482 484 485 487 487 488 489 3 2. Dedekind domains .... 1. Definition of Dedekind domains .... 2. Characterizations of Dedekind domains .... 493 493 494 3 Decomposition of ideals into products of prime ideals .... 496 4 The approximation theorem for Dedekind domains . . . . . 497 5 The Krull-Akizuki Theorem .... 499 . . . . Fj 3 Factorial domains .... 1 Definition of factorial domains .... 2 Characterizations of factorial domains .... 3. Decomposition into extremal elements .... 4 Rings of fractions of a factorial domain .... 5 Polynomial rings over a factorial domain .... 6 Factorial domains and Zariski rings .... 7 Preliminaries on automorphisms of rings of formal power series .... 8 The preparation theorem .... 9 Factoriality of rings of formal power series .... 502 502 502 504 505 505 506 3 4. Modules over integrally closed Noetherian domains .... 512 512 517 521 523 527 529 531 535 54.0 543 . . . . 1 Lattices .... 2 Duality; reflexive modules .... 3 Local construction of reflexive modules .... 4 Pseudo-isomorphisms .... 5 Divisors attached to torsion modules .... 6. Relative invariant of two lattices .... 7. Divisor classes attached to finitely generated modules .... a. Properties relative to finite extensions of the ring of scalars 9. A reduction theorem .... 10 Modules over Dedekind domains .... Exercises for 3 1 Exercisesfor52 .... 506 507 511 545 556 .... Exercises for 34 .... Historical note (Chapters I to VII) .... Bibliography .... Index of notation .... Index of terminology .... Table of implications .... Table of invariances - 1.................................. Table of invariances -11 .... 563 .... 625 Exercises for 3 3 Invariances under completion 571 579 603 607 610 621 622 624 INTRODUCTION The questions treated in this Book arose during the development of the theory of algebraic numbers and (later) algebraic geometry (cf. the Historical Note). From the 19th century onwards these two theories began to show remarkable analogies; the attempt to solve the problems they posed led to the isolation of a number of general ideas whose field of application is not limited to rings of algebraic numbers or algebraic functions; and, as always, it is advantageous to consider these in their most general form in order to see their true significance and the repercussions of one study on another. The concepts treated in this Book can be applied in principle to all commutative rings and modules over such rings; it must however be pointed out that substantial results are often obtained only under certain hypotheses of jniteness (which always hold in the classical cases), for example by assuming the modules to be finitely generated or the rings to be Noetherian. The chief notions central to the first chapters are the following: 1. Localization and globalization. Let us begin for example with a system of Diophantine equations : (*> Pi(Xl,. . .)x,) =0 (1 < i < n) where the Pi are polynomials with integer coefficients and solutions (xi) are sought consisting of rational integers. It is possible to start approaching the problem by looking for solutions consisting of rational numbers, which involves l o o k g at the same problem with the coefficientsof the P, considered as elements of thefild of fractions Q of Z and the solutions sought with values in Q. A second step consists of seeing whether, given a prime number p , there exist rational solutions whose denominators are not divisible by p (integer solutions this condition) ;this amounts, in this case, to lying in the subring %I) of Qconsisting of the rational numbers of this form, called the local ring of Comesponding to the prime number p. Clearly the passage from Z to Q and xxi INTRODUCTION that from Z to Z, are of the same form: in the two cases, the only denominators allowed do not belong to a certain prime ideal (the ideal (0) and the ideal (p) respectively). The same name “local ring” arises in algebraic geometry, where this notion appears in a more natural way: for example for the ring C[X] of polynomials in one variable with complex coefficients, the local ring corresponding to the prime ideal (X - a)is the ring of rational fractions “regular” at the point a (that is, without a pole at that point). Every Diophantine problem and more generally every problem on Amodules (A a commutative ring) can be decomposed into two subsidiary problems: its solution is sought in the local rings A, corresponding to the different prime ideals p of A (“localization”), then the question is asked whether it is possible to conclude from the existence for all p of a solution to the “localized” problem that a solution exists to the problem posed initially (“passage from the local to the global”). Chapter I1 is devoted to the study of this double process and it is also seen that “localization” is not related only to prime ideals, but has a wider range. 11. Completion of local rings. A local ring A shares with fields the property of having only one maximal ideal m. This fact is used to transform, to a certain extent, a problem on A-modules into an analogous problem on vector spaces by passing to the quotient ring A/m, as this latter is a field. If we return for example to the Diophantine system (*) this idea is none other than the principle of “reduction modulo k”, transforming the equations into congruences mod. p, which occurred naturally beginning with the very first works in the theory of numbers. This being so, we clearly cannot hope in this way to obtain complete results for the original problem and it was quickly realized that to obtain more precise information it was necessary to consider, not only congruences modulo m, but also “higher” congruences modulo mn, for arbitrary integers n > 0. I t is thus found that, the larger n, the closer in some way the original problem is C< approached” (in the case A = Z for example, the reason is that an integer # 0 cannot be divisible by all the powers p” of a given prime number p ; this number will therefore make its presence felt in the reduction mod. pn provided n is taken large enough). The mathematical translation of this idea consists of considering on A a ring topology (cf. General Topology, Chapter 111, tj 6) in which the mnform a fundamental system of neighbourhoods of 0. But when we have for example, solved the system of congruences (1 < i < n) (**) P,(x,,. . ., x,) I 0 (mod.pk) for every integer k > 0, it still does not follow that the system (*) has a solution in the local ring Z,,,; the above hypothesis can be interpreted as saying that (*) admits a solution in the completion Zcp)of the topological ring Z(p). The original problem, thus weakened, is finally transformed into the analogous problem for local rings of the type A/mn, which are also nearer to fields I xxii INTRODUCTION than general rings, since they have a nilpotent radical; in classical algebraic geometry this corresponds to a “differential” study of the problem in the neighbourhood of a given point. Chapter I11 deals in a general way with these applications of topological ‘notions to the theory of local rings. In Chapter VI a special aspect of this is studied, adapted on the one hand to more detailed studies of algebraic geometry, and above all to the arithmetic of algebraic number fields, where the 1-1 rings encountered (such as Z(pJ belong to a particularly simple class, that 0f“valuation rings”, where divisibility is a total ordering (cf. Algebra, Chapter VI, 3 1) of the set of principal ideals. The study of the passage from a ring A to a local ring A, or to a completion A brings to light a feature common to these two operations, the property of JWS ofthe A-modules A, and A, which allows amongst other things the use of tensor products of such A-modules with arbitrary A-modules somewhat similar to that of tensor products of vector spaces, that is, without all the precautions surrounding their use in the general case. The properties associated with this notion, which are also applicable to modules over non-commutative rings, are the object of study in Chapter I. 111. Integers and decomposition ideals. The study of divisibility in algebraic number fields necessitated from the start the introduction of the notion of integer in such a field K, generalizing the notion of rational integer in the field Q. The general theory of this notion of “algebraic integer”, linked, as will be seen, to very strict conditions of finiteness, is developed in Chapter V; it can be applied to all commutative rings and is of great interest not only in arithmetic, but in algebraic geometry and even in the modern theory of “analytic spaces” over the field C. One of the major obstacles to the extension of classical arithmetic to rings of algebraic integers has long been that the classical decomposition of a rational integer into prime factors does not extend in general to these rings. The creation of the theory of ideals was necessary to surmount this difficulty: the unique decompositionsoughtis thenestablished for ideals, thenotion of primeideal being substituted for that of prime number. Moreover this result can be considered as a typical case where the “passage from the local to the global” is performed satisfactorily: the knowledge, for x E K, of the values at x of all the “valuations” On K determines x up to multiplication by an invertible integer. In less simple rings than rings of algebraic integers (and even for example in of polynomials in several indeterminates) this result is no longer valid. However it is possible to associate in a canonical way with every ideal a welldekrmined set of prime ideals :in algebraic geometry, if we consider for example inKn(Km y commutative field) a subvariety defined by a system of polynomial Wations Pa = 0, the irreducible components of this subvariety comespond bismtively with the minimal elements of the set of prime ideals thus asso&ted with the ideal generated by the Pa. It is moreover possible (ifwe restrict ~ xxiii INTRODUCTION ourselves to Noetherian rings) to give for every ideal a “decomposition” less precise than a decomposition as a product of prime ideals :here the product is in fact replaced by the intersection and the powers of prime ideals by “primary” ideals connected with the prime ideals associated with the ideal in question (but which are not direct generalizations of powers of prime ideals). The introduction of prime ideals associated with an ideal and the study of their properties is the subject of Chapter IV; here also the existence and certain uniqueness properties of the “primary decompositions” to which we have just alluded are proved; but it seems at present that these decompositions usually only play an accessory role in applications, the essential notion being that of prime ideal associated with an ideal. I n Chapter VII we examine in more detail rings whose properties most nearly approach those of rings of algebraic integers as far as decomposition as a product of prime ideals is concerned; amongst other things it is possible to introduce into these rings the notion of “divisor”, which is the geometric aspect of this decomposition and plays an important role in algebraic geometry. Finally Chapters V I I I et seq. will deal with notions of more interest in algebraic geometry than in arithmetic (where they become trivial) and notably the concept of dimension. With these notions we come to the frontier of algebraic geometry proper, a frontier which is ever moving and difficult to trace. For, if commutative algebra is an essential tool for the development of algebraic geometry in all its generality, conversely (as has already been seen above) the language of geometry proves very convenient for expressing the theorems of commutative algebra and suggesting a certain intuition naturally enough absent from abstract algebra; with the tendency to enlarge more and more the limits of algebraic geometry, algebraic and geometric language tend more than ever to merge. CHAPTER I(*) Flat Modules u&s otherwise stated, all the rings considered in this chapter are assumed to have a unit e b t ; all the ring homomorphisms are assumed to map unit element to unit element. A subring of a ring A m a n s a subring containing the unit element o f A. IfAis a ring, M a left A-module and U (resp. V) an additive subgroup ofA (resp. M) , recall that UV or U .V is used to denote the additive subgroup ofM generated by the products uv, where u E U , v E V (Algebra, Chapter VIII, $ 6, no. 1). If a is an i&d ofA, we write ao = A. For any set E, 1, (or 1 fi no confusion arises) is used to denote the identity mapping o f E to itself. Recall that the axiomsf o r a module imply that fi E is a lejit (resp. right) module over a ring A and 1 denotes the unit element o f A, then 1 . x = x (resp. x . 1 = x) for dl x E E (Algebra, Chapter 11, $1, no. 1). I f E and F are two lejl. (resp. right) A-mddes, recall that Hom,(E, F) (or simply Hom(E, F)) is used to denote the didive group of homomorphisms o f E to F (loc. cit., $ 1, no. 2). B y an abuse o f notation 0 will often be used to denote a module reduced to its identity element. 1. DIAGRAMS AND EXACT SEQUENCES 1. DIAGRAMS Let, for example, A, B, C , D, E be five sets and letf be a mapping from A to B, g a mapping from B to C, h a mapping from D to E, u a mapping from B to D and v a mapping from C to E. To summarize such a situation we often make use diagrams; for example, the above situation is summarized by the following Of (*) With the exception of Q 4, the results of this chapter depend only on Books I to VI. xxiv 1 8 1.3 EXACT SEQUENCES FLAT MODULES I For the diagram (2) to be commutative it is necessary and sufficient that the relations diagram (Set Theory, Chapter 11, €j3, no. 4) A-BLC 1’ (3) 4 JV DTE f In such a diagram the group of symbols A + B expresses schematically the fact thatf is a mapping from A to B. Where there is no ambiguity about5 we suppress the letter f and write simply A + B. When A , B, C, D, E are groups (resp. commutative groups) andf, g , h, u, v group homomorphisms, diagram (1) is called, by way of abbreviation, a diagram of groups (resp. commutative groups). In principle, a diagram is not a mathematical object, but only ajigure designed to facilitate reading an argument. In practice, diagrams are often used as abbreviatoy symbols to avoid naming all the sets and mappings under consideration; we therefore say “Consider the diagram (1)” instead of saying “Let A, B, C, D, E be five sets . and v a mapping from C to E”; see for example the statement of Proposition 2 in no. 4. .. f’oa = b of , g’ob=cog, h’of=doh; hold; in other words, it is necessary and sufficient that the three square diagrams contained in (2) be commutative. For the relations (3) imply c o g o f = g ‘ o b o f since c o g = g ‘ o b , and g ‘ o b o f = g ‘ o f ‘ o a since b of =f’ o a ; thus the three paths beginning at A and ending at C’ give the m e mapping. I t can be similarly verified that the four paths beginning at A and ending at D’ (resp. the three paths beginning at B and ending at D’) give fie same mapping. The relations (3) signify that the two paths beginning at A (resp. B, C) and ending at B’ (resp. C’, D’) give the same mapping. None of the other pairs of vertices of (2) can be joined by more than one path and the diagram (2) is therefore commutative. In what follows we shall leave the reader to verify analogous results for other types of diagrams. 3. EXACT SEQUENCES Recall the following definition (Algebra, Chapter 11, 9 1, no. 4) : 2. COMMUTATIVE DIAGRAMS DEFINITION 1. Let A be a ring, F, G , H three right (resp. left) A-modules, f a homom07fihi.m offF to G and g a homomorphism ofG to H. The orderedpair (f,g) is called an exact sequence i f 2’ (0) = f (F), that is i f the kernel o f g is equal to the image off. Consider, for example, the following diagram: f A’ --3 B’ -+ C’ f’ P’ h - A-+-B&C-D h’ The diagram D’ To every path composed of a certain number of segments of the diagram traversed in the direction shown by the arrows corresponds a mapping of the set represented by the beginning of the first segment to the set represented by the end of the last segment, namely the composition of the mappings represented by the various segments traversed. For each vertex of the diagram, for example B, by way of convention there is a path reduced to B, to which corresponds the identity mapping 1,. In (2) there are for example three paths beginning at A and ending at C’; the corresponding mappings are c o g of, g’ b f and g’ of’ a. A diagram is said to be commutative if, for every pair of paths in the diagram with the same beginning and end, the two corresponding mappings are equal; in particular if the beginning and end of a path coincide the corresponding mapping must be the identity. 0 2 0 I F-GLH (4) 0 is also called an exact sequence. Consider similarly a diagram consisting of four modules and three homomor- phisms: (5) f h E +FB’G+H. This diagram is said to be exact at F if the diagram E & F 5 G is an exact sequence; it is said to be exact at G if F f G 3 H is an exact sequence. If (5) is a c t at F and G, it is said to be exact or also an exact sequence. Exact sequences 6th any number of terms are similarly defined. Recall the following results (loc. cit.), where E, F, G denote right (resp. left) 3 1 3 1.4 THE SNAKE DIAGRAM FLAT MODULES A-modules, the arrows represent homomorphisms and 0 denotes a module reduced to its identity element: Suppose that the two rows of (10) are exact. Then: (i) I f c is injective, we have f (a) To say that 0 -+ E -+ F is an exact sequence is equivalent to saying that f is injective. f (b) To say that E -+ F -+ 0 is an exact sequence is equivalent to saying that f is surjective. f (c) To say that 0 4 E -+ F -+ 0 is an exact sequence is equivalent to saying that f is bijective, that is that f is an isomorphism of E onto F. (d) I f F is a submodule of E and i denotes the canonical injection of F into E and p the canonical surjection of E onto E/F, the diagram P (6) O-F>E+EE/F~O is an exact sequence. (e) Iff: E 4 F is a homomorphism, the diagram Im(b) n Im(u’) = Im(u’ o a) (11) (ii) I f a is surjective, we have (12) Im(u’0 a) to be an exact sequence, it is necessary and sufficient that there exist modules S, T and homomorphisms a : E -+ S, 6 : S -+F, c: F --f T and d : T -+ G such that f = b o a, g = d o c and the three sequences = Im(b 0 u) c Im(b) n Im(u’). Conversely, let x E Im(b) n Im(u’). There exists y E B such that x = b (y) . As 0, we have 0 = v’(x) = v’(b(y)) = c(v(y)),whence v(y) = 0 since cis injective. As (u, v) is an exact sequence, there exists z E A such that y = u (z) , whence x = b (u (t)) . 0 Ker(b) u = 0 and v’ u’ = 0, it is clear that 0 + Im(u) c Ker(v’ LEMMA 1. Consider a commutative diagram of commutative groups: A-LB 1) O+S-+FAT-O A’ -U’3 B’ d be exact. Recall finally that iff: E -+ F is an A-module homomorphism, we set -1 Ker(f) = f (0), Im(f) =f(E), Coim(f) = E/fiO) and Coker(f) = F/f(E). With this notation it is possible to take, in (9), S = Im(f)= Ker(g) and T = Im(g) (canonically isomorphic to Coker(f)). 4. Then there exists one and only one homomorphism u l : Ker(a) --f Ker(6) and one and only one homomorphism u p : Coker(a) 4 Coker(b) such that the diagrams Ker(a) -% Ker(b) = f(b) (14) - A - THE SNAKE DIAGRAM PROPOSITION 1. Consider a commutative diagram of commutative groups : A L B A U’ B’ crnd A’ C - bl .1C’ A --+ 4 6) = Ker(c o v). 0 b 0-T+G o Conversely, let x E Ker(v’). Then b(x) E Ker(v’) and there exists y E A’ such that u’(y’) = b(x), since the sequence (u’, v’) is exact. As a is surjective, there exists y E A such that a(y) = y’, whence b(x) = u’ (a (y)) = b (u (y)) ;it follows that x - u (y) E Ker(b), which completes the proof. EAS-0 (9) b) = Ker(c o v). v’ o u’ = -1 (where i is the canonical injection off (0) into E and p the canonical projection of F/f (E)) is an exact sequence. (f) For the diagram (8) E - -f+ F ~ ’ G 0 Im(6 o u) . Let us prove (i). Clearly -1 f o-~(o)-LE+FLF~(E)---+o Let us prove (ii). As u (7) + Im(u) = Ker(v’ Ker(6) = V (15) Coker(a) d uo B B’ 1p Coker(b) 5 I 5 1.4 THE SNAKE DIAGRAM FLAT MODULES are commutative, i a n d j denoting the canonical injections and p and q the canonical surjections. k t US prove (i). As u1 and u1 have the same graphs as the restrictions of u and to Ker(a) and Ker(b) respectively, we have u1 0 u1 = 0. Then Ker(ul) = Ker(6) n Ker(u) = Ker(6) n Im(u) = Im(j) n Im(u). If x E Ker(a), then a (x) = 0 and b (u (x)) = u ‘ (a (x)) = 0, hence u (x) E Ker(b), and the existence and uniqueness of u1 are then immediate. Similarly, we have u’(a(A))= b(u(A)c b(B), then by taking quotients u’ gives a homomorphism u2: Coker(a) -+ Coker(b), which is the only homomorphism for which (15) is commutative. But, by Proposition 1, (i), Ker(u,) = I m (j 0 ul) = Im(ul) if u’ is injective. Let us prove (ii). As u2 and u, are obtained from u and u by taking quotients, it is clear that u2 0 u2 = 0. Suppose that u is surjective; as q andp are surjective, it follows from the hypotheses and Proposition 1, (ii) that Let us now start with the commutative diagram (10) of commutative groups; there corresponds to it by Lemma 1 a diagram Ker(v,) = q(Ker(u2 0 q)) = q(Ker(u’) Im(b)) = Im(q o u’) = Im(u, o p) = Im(u,). + = dKer(u’)) = q(Im(u’>> Finally let us prove (iii). For x E Ker(c) there existsy E B such that u(y) = k (x) since u is surjective; moreover u’(b(y)) = c (k (x)) = 0 and consequently there &sb a unique t’ E A‘ such that u’(t’) = b (y) ,since u’ is injective. We now show that the element p (t ’) E Coker(a) is ina’ependent of the element y E B such that ~ (y) = k (x) . For if ~ ’ E is B another element such that u (y ’) = k (x) , then y’ = y + ~ (z)where , z E A; we show that if t” E A‘ is such that u’(t”) = b(y’) then t” = t ‘ a (z) ; for + U’(t’ I .L 4 i--+Coker(a) ~p + Coker(6) .L Coker(c) where i, j, k are the canonical injections, p , q, r the canonical surjections and ul, u, (resp. ul, u,) the homomorphisms canonically associated with u, u‘ (resp. u, u’) by Lemma 1. I t is immediately verified that this diagram is commutative. PROPOSITION 2. Suppose that in the commutative diagram (10) the sequences (u, v) and (u’, v’) are exact. Then: (i) u1 0 u1 = 0 ; ifu’ is injective, the sequence (ul, ul) is exact. (ii) u2 0 u2 = 0 ; ifu is surjective, the sequence (uz, u2) is exact. (iii) Suppose that uf is injective and v is surjective. Then there exists one and only one homomorphism d : Ker(c) --f Coker(a) with the following property: if x E Ker(c), y ~ B a n d t ’ ~ A ’ s a t i s r t h e r e l a t i o n s u (y=) k (x) andu’(t’) = b(y),thend(x)= p (t ’) . Moreover the sequence d (*) Ker(a) -% Ker(b) -% Ker(c) --f Coker(a) 5 Coker(b) is exact. 6 Coker(c) + a (z)) = u ‘ (t ’) + u ‘ (a (2)) = b (y) + b (u (z)) = b (y + U (2)) = b(y’). Finally, it follows that p (t ”) = p (t ’) + /I(.(.) = p (t ’) . Then it is possible to set d (x) = p(t’) and the mapping d : Ker(c) -+ Coker(a) has thus been defined. If now xl, x, are elements of Ker(c) and x = x1 + x,, we take elements yl,y, of B such that u(yl) = k (x l) and v(y,) = k(x2) and choose for y E B the element y, y,; it is then immediate that d (x) = d(x,) and d(x,), and hence d is a homomorphism. Suppose that x = ul(x’) for some x‘ E Ker(b) ; then take y E B to be the elementj(x’). As b (j (x ’)) = 0, it follows that d (x) = 0, hence d o vl = 0. Conversely, suppose that d (x) = 0. In the above notation we then have t’ = a(s), where S E A . In this case we have b(y) = u’(t’) = u’(a(s)) = b(u(s)), or b(y u(s)) = 0. The element y - u(s) is therefore of the form j (n) , where nEKer(b), and we have k (x) = u(y) = u(u(s) j (n)) = u (j (n)) = k(v,(n)); as k is injective, x = vl(n), which proves that the sequence (*) is exact at Ker(c) Finally, we have (always in the same notation) + - + + . uz(d(x)) = uz(P(t’)) = q(u’(t’)) = q (b (y)) = 0 and hence u, o d = 0. Conversely, suppose that an element w = p (t ’) of &kerb) is such that u,(w) = u,(p(t’)) = 0 (where t’ E A) . Then q(u’(t’)) = 0 and consequently u ’ (t ’) = b (y) for some y E B; as u’(u’(t’)) = 0, we have D’(b(!/))= 0, hence c(v(y)) = 0, in other words u (y) = k(x) for some x E Ker(c), and by definition w = d (x) , which shows that the sequence (*) is exact at 7 I 3 2.1 FLAT LIODULES REVISION OF TENSOR PRODUCTS Coker(a). It has been seen in (i) that it is exact at Ker(b) and in (ii) it is exact a t Coker(b), which completes the proof of (iii). v(B) and w and w’ have respectively the same graphs as v and v’; this diagram is commutative and its rows exact. Moreover w is surjective and by hypothesis u’ is injective; then by Proposition 2, (iii) we have an exact sequence Remark. If the groups of the diagram (10) are all (for example, right) modules over a ring A and the homomorphisms are A-module homomorphisms, it is soon verified that the homomorphism d defined in Proposition 2, (iii) is also a A-module homomorphism: if x E Ker(c) and a E A, and y E B is such that v(y) = k (x j , it is sufficient to note that v (y a) = k(xa). 0 = d Ker(c’) -+ Coker(a) - Coker(b) = 0 since b is surjective and c’ is injective; whence Coker (a) = 0. COROLLARY 1. Suppose that the diagram (10) is commutative and the two rows are exact. Then : (i) I f u ’ , a and c are injectizie, b is injective. (ii) If v, a and c are surjective, b is surjective. 1. REVISION OF TENSOR PRODUCTS Assertion (i) is a consequence of assertion (i) of Proposition 2: for Ker(a) = 0 and Ker(c) = 0, hence Ker(b) = 0. Assertion (ii) is a consequence of assertion (ii) of Proposition 2: for Coker(a) = 0 and Coker(c) = 0, hence Coker(b) = 0. Let A be a ring, E a right A-module and M a left A-module. In Algebra, Chapter 11,3 3, no. 1 we defined the tensorproduct E B A M ,which is a Z-module. If E’ (resp. M’) is a right (resp. left) A-module and u : E -+ E’ (resp. v : M --f M’) a homomorphism, we also defined (Zoc. cit, no. 2) a Z-homomorphism COROLLARY 2. Suppose that the diagram (10) is commutative and the two rows are exact. Under these conditions: u @ U : E @AM + E’ @AM’. (i) I f b is injective and i f a and v are surjective, then c is injective. (ii) I f b is surjective and ifc and u’ are injective, then a is surjective. 2. FLAT MODULES(*) LEMMA 1. Let M’ -$ M % M” --f 0 be an exact sequence of lt$t A-modules and E a right A-module. Then the sequence To prove (i) consider the diagram E .(A) L B A C where a’ is the mapping with the same graph as the restriction of b to u(A) and w and w’ are the canonical injections; clearly this diagram is commutative and its rows are exact. Moreover w’ is injective and by hypothesis v is surjective; then by Proposition 2, (iii) we have an exact sequence 0 = since b is injective and a’ is surjective; whence Ker(c) = 0. To prove (ii) consider the diagram - A A a‘i A’ W’ B v(B) b l d i B’ y v’(B’) 0 where this time c’ is the mapping with the same graph as the restriction of c to 8 @A M” ----+0 This is the Corollary to Proposition 5 of Algebra, Chapter 11, fj 3, no. 6. u ’ (A) IJ B‘ --.--f C’ w ‘U 0 = Ker(b) -----f Ker(c) -----f Coker(a’) M’ + 1Qu E @A M + 1 c3w E U an exact sequence of commutative groups. a’l bi 4 d @A I t follows that, for any left A-module homomorphism u : M --f N, E @A (Coker u) is canonically identified with Coker(1. @ u) , as Lemma 1 shows when applied to the exact sequence M & N -+ Coker u --f 0. In the notation of Lemma 1, we know (106. cit.) that if v is injective, that is if the sequence 0 -+ M’ 5 M -% M” --f 0 is exact, it does not necessarily follow that 1, ‘80 is injective and so E @A M’ cannot in general be identified with a (*) We inform readers already familiar with Homological Algebra that they find other characterizations of flat modules in 5 4. 9 I $2.2 FLAT MODULES M-FLAT MODULES subgroup of E B A M .Recall however (Algebra, Chapter 11, 5 3, no. 7, Corollary 5 to Proposition 7) the following result: as the restriction of P to M', r the identity mapping of R to R, m the canonical injection M' +- M and n the canonical injection N' + N. The diagram I - P' i' LEMMA 2. If v : M' --f M is injective and v(M') is a directfactor of M, the homomorphism 1, @ v is injective and its image is a directf a t o r of E @A M. 0 2. M-FLAT MODULES O - - + R y + I th DEFINITION 1. Let A be a ring, E a right A-module and M a l$t A-module. E is said to befrat for M (or M-Jat) f,for every l$t A-module M' and every injective homomorphism u: M' --f Mythe homomorphism 1, @ v : E @A M' -+ E @A M is injective. For any right A-module N, the notion of an N-j?at l&t module is defined similarly. To say that a right A-module E is flat for a left A-module M is equivalent to saying that E, considered as a left Ao-module (recall that Ao denotes the opposite ring to A) , is flat for the right Ao-moduleM. LEMMA 3. For a tight A-module E to be M-Jat, it is necessary and sujicient that f o r every jinitely generated submodule M' of M the canonical homomorphism 1, @ j : E @A M' --f E @A M (j bkng the canonical injection M' -+M) be injective. Suppose that this condition holds and let N be any submodule of M. Suppose that the canonical image in E @A M of an element Z = Z i~ , @ Y , E E @ A N (X , E E , y t E N) is zero and let M' be the finitely generated submodule of N generated by they,; as by hypothesis the composite mapping E @A M' -+ E @A N -+E @A M is 7 R --+ M' --+ T(R) T(i') T(N') --+ 0 T(M') is commutative and its rows are exact by Lemma 1 of no. 1. Moreover, since E is M-flat, the homomorphism T (m) is injective. As T(r) and T(p')are surjective, it follows from 5 1, no. 4, Corollary 2 to Proposition 2 that T (n) is injective, which proves the lemma. LEMMA 5. Let (MJLE1 be a family and E a righ A-module. If,for all of left A-modules, M I E I, E isfrat for . 9 = M, their direct sum M,, then E isflat f o r M . (a) Suppose first that I = (1, 21, and let M' be a submodule of M = MI @ M,, M, and M, being canonically identified with submodules of M. Denote by Mi the intersection M' n M, and by ML the image of M' in M, under the canonical projection p of M onto M,. We have a diagram LEMMA 4. Let E be a right A-module and M a l$t A-module such that E is M-j?at. If N is either a submodule or a quotient module of M, then E is N-Jat. O-M,-M Mi P' i' ----j v.1 M ' - + Mk --3 0 u.1 --+M,-O P I Where 01, V , u,, i, i' are the canonical injections andp' is the mapping with the m e graph as the restriction of p to M', which is surjective. It is immediately verified that this diagram is commutative and that its rows are exact. With T(Q>and T(v)used in the same sense as in the proof of Lemma 4, we have a diagram is injective, hence so is E @A N' + E @A N. Suppose then that N is a quotient module of M, that is there exists an exact sequence 0 -+ R M 5 N --f 0. T(M;) Let N' be a submodule of N and M' = >'(N'). Let i' denote the mapping of R to M' with the same graph as i, p' the surjection M + N' with the same graph T(M1) 10 -0 To simplify the writing, we set T(Q) = E @A Q for every left A-module Q and T (v) = l E @ v for every left A-module homomorphism u. The diagram 0 '@AM -I$ P is commutative and its rows are exact. considered as an element of E @A M', is injective, the sum z' = x, By,, zero. As z is the image of z', we have also z = 0, whence the lemma. The case in which N is a submodule is easy, as, if N' is a submodule of N, the composite homomorphism N' --+ 0 aT(M) --+ T(M;) W') T(~d1 Tb)] 3T(M) T(us)] T(p)- T (M 2) 11 I By Lemma 1 of no. 1 the two rows of this diagram are exact; as E is flat for M, and M,, T(v,) and T(v,) are injective; moreover, by Lemma 2 of no. 1, T(i) is injective. Corollary 2 to Proposition 2 of 3 1, no. 4 then shows that T(v) is injective and consequently E is M-flat. (b) If I is a finite set with n elements, the lemma follows by induction on n using (a). (c) In the general case let M' be ajnitely generated submodule of M. Then there exists a finite subsetJ of the indexing set I such that M' is contained in the direct sum M, = M,. By (b) E is flat for MJ; the canonical homomorphism E @A M' -+ E @A M, is therefore injective. On the other hand, as MJ is a direct factor of M, the canonical homomorphism E @A MJ --f E @A M is injective (no. 1, Lemma 2). Taking the composition, it follows that E @A M, -+ E @AM is injective and E is flat for M by Lemma 3. fj2.3 FLAT MODULES FLAT MODULES If M" is an exact sequence of left A-modules and fi E is an M"-Jat right A-module, the sequence LEMMA 6. is exact. We use the notation T(Q)and T(v)in the same sense as in the proof of Lemma 4 ofno. 2. We write M'; = w(M) and let i: M; --f M" be the canonical injection and p the mapping of M to MY with the same graph as w. The sequence M' -$ M -% MI + 0 is exact and it follows from Lemma 1 of no. 1 that the sequence T(M') 2T(M) T(p! T(M;) -+o is exact. Moreover, as E is M"-flat, the mapping T(i) : T(M;) injective, and as T(i) T(p) = T(w), the sequence --f T(M") is 0 3. FLAT MODULES PROPOSITION 1. Let E be a right A-module. Thefollowing three properties are equivalent : (a) E isflatfor A, (in other wordr,f o r every lejt ideal a ofA, the canonical homomorphism E @A a -+E @A A, = E is injective). (b) E is M-Jat for every lejt A-module M. (c) For every exact sequence of l ~A-modules t and homomorphism DEPINI~ON 2. A right A-module E is calledjat fi it has the equivalent properties of Proposition 1. M~D-MGM" Remarks (1) By Lemma 3 of no. 2, for a right A-module E to be flat, it is necessary and sufficient that, for everyjnitely generated left ideal a of A, the canonical mapping E @A a -+ E (Proposition 1) with image Ea be injective. (2) Let E be a flat right A-module. If M' is a submodule of a left A-module M, the canonical injection E M allows us to identify E @A M' @A M' -+E with a Subgroup of E @A M. This being so, let N be a left A-module, u : M -+ N a homomorphism, K = Keru, and I = Imu. By considering the exact Wquence the seqwnce 1QW '" is exact. I t is immediate that (b) implies (a). Conversely, suppose that (a) holds; by Lemma 5 of no. 2, E is flat for every free left A-module; as every left A-module is isomorphic to a quotient of a free module (Algebra, Chapter 11, 5 1, no. 11, Proposition 20), it follows from Lemma 4 of no. 2 that E is flat for M. We show that (c) implies (b). If v: M' -+ M is an injective homomorphism, M is exact; by (c) the sequence the sequence 0 + M' ' is exact; this means that 1 @ u is injective, in other words, E is M-flat. Finally, the implication (b) + (c) is a consequence of the following more precise lemma: 12 Flat left A-modules are defined similarly. To say that a right A-module E is flat equivalent to saying that E, considered as a left Ao-module, is flat. O-K-MU-N it is w i l y seen (Proposition 1) that E @A (Ker u) is identijed with Ker(1, @ u). the other hand, writing u' for the surjective homomorphism M 3 I with e p h as U, and i for the canonical injection I -+ N, 1, @ u' is surj M V C (no. 1, Lemma 1) and 1, @ i is injective since E is flat. As ' E '8 A (Im u) 8 = is i&nt$ed with Im(1, @ i, (lE @ u'), 8 u). 13 FLATNESS OF QUOTIENT MODULES FLAT MODULES I PROPOSITION 2. (i) Let (EL),,, be afamily ofright A-modules. For E = Jut, it is necessary and sujicient that each ofthe El bejlat. 0,ELto be (ii) Let I be an ordered set and (E,, f J a)a direct system of right A-modules (Algebra, Chapter 11, 3 6, no. 2). Ifeach of the E, isjlat, then E = lim E, isjlat. > - Let M' -+ M be an injective left A-module homomorphism. (i) For the direct sum homomorphism L E I (E @A @ ~ M') 9 M, to be exact, it is necessary and sufficient that each of the homomorphisms ELQ A M ' - + A M be so (Algebra, Chapter 11, 1, no. 6, Corollary 1 of Proposition 7), which proves (i) since (El @A M) is canonically identified with E @A M (Algebra, Chapter 11, 3 3, no. 7, Proposition 7). (ii) By hypothesis each of the sequences 0 -+ E, @A M' + E, @A M is exact; so then is the sequence 0 + E @A M'-+ E @A M since taking the direct limit commutes with tensor products (Algebra, Chapter 11, 6, no. 3, Proposition 7) and preserves exactness (ibid., fj 6 , no. 2, Proposition 3). --f (EL @A 9 4. EXAMPLES OF FLAT MODULES (1) For any ring A, A, is clearly a flat A-module (Algebra, Chapter 11, no. 4, Proposition 4). Then it follows from Proposition 2, (i) of no. 3 that every free right A-module, and more generally every projective right Amodule (Algebra, Chapter 11, § 2, no. 2), is a flat A-module. (2) If A is a semisimple ring (Algebra, Chapter VIII, 3 5, no. 1, Definition 1) every right A-module E is semisimple and hence a direct sum of simple modules; as each of these latter is isomorphic to a direct factor of A, (ibid., 3 5, no. 1, Proposition 6) , E is projective and therefore flat by (1) (cf. Exercise 16). * (3) In Chapters I1 and I11 we shall study in detail two important examples of flat A-modules: rings of fractions S-IA and Hausdorff completions A of A for 3-adic topologies.* 3 3, PROPOSITION 3. Let A be a ring and E a right A-module. (i) Suppose that E isjlat. For every element a of A which is not a right divisor of O(*), the relations x E E, xu = 0 imply x = 0. (*) Recall that a right (resp. left) divisor of 0 in a ring A is an element 6 E A such that the mapping x Hxb (resp. x H bx) is not injective. 14 2.5 (ii) suppose that A is an integral domain in which every finitely generated ideal is ps;ncip"l(for example aprincipal ideal domain (Algebra, Chapter VII, fj 1, no. 1)). T bfor E to bejlat it is necessary and that E be torsion-fee. We prove (i). Let v: A, -+ A, be the left A-module homomorphism t F+ ta; the h p t h e s i s implies that v is injective. As E is flat, the homomorphism lE 8 v: E @A A, -+ E @A A, is also injective. When E @A A, is canonically identified with E, 1, @ v becomes the endomorphism x H xu of E. Thus the xu = 0 implies x = 0. we prove (ii). By (i), if E is flat, E is torsion-free. Conversely, let E be a torsion-free A-module; we verify that, for every finitely generated ideal a of A, the canonical homomorphism E @A a -+ E is injective (no. 3, Remark 1). This assertion is obvious if a = (0); otherwise, by hypothesis a = A a for some a E A, a # 0, and t t+ ta is then an isomorphism v of A onto a; using i to denote the canonical injection a -+A, i 0 v is the homothety with ratio a on E and is injective since E is assumed to be torsion-free. Then 1, @ (i o v) = (1, @ i) o (l E @ 0) ; as 1, @ v is an isomorphism, 1, @ i is injective, which completes the proof. Example. Applying Proposition 3 to the ring Z, it is seen that Q is a flat Zmodule, but that Z/nZ (for n > 2) is not a flat Z-module. 5. FLATNESS OF QUOTIENT MODULES ~ ~ ~ P ~ S I T 4. I Let O NE be u right A-module. The threefollowing proterties are equiua- I&: (a) E isfit. (b) For every exact sequence o f right A-modules o f the form (1) O-G-~.H>E---+O and merY lgt A-module F, the sequence is exact. (c) T h e exists an exact sequence (I), where H isjlat, such that the sequence (2) is exact for every lgt A-module F o f the form A&, where a is a finitely generated idcor ofA. we Show first that (a) implies (b). The left A-module F is isomorphic to a quotimt of a free module (Algebra, Chapter 11,s 1, no. 11, Proposition 20) ; in 0 t h words, ~ we have an exact sequence O---,R-L-F-Oi P 15 I FLAT MODULES 5 2.6 INTERSECTION PROPERTIES where L is free. Consider the diagram % . E @R in"@ u is injective; moreover, Proposition 4 proves that v @ 1,) and v @ 1, are injective. This being SO, if E is flat, 1, @ u is injective, hence also (lE @)' (v @ lF') = (u @ IF) (lE' @ u) ; it follows that 1:, @ u is injective and consequently E' is flat. Conversely, if E' is flat, l,, @ u is injective; then it follows from 3 1, no. 4, Corollary 1 to Proposition 2 that 1, @ u is injective and so E is flat. (3) I t follows immediately that this diagram is commutative, and its rows and columns are exact by Lemma 1 of no. 1 ; moreover, as 1, @ p and 1, @ p are surjective (no. 1, Lemma l), we have G @ F = Coker(1, @ i) , H @F = Coker(1, @ i) ; Rmrarks (1) It is possible for E and E' to be flat without E" being so, as the example of the Zmodules E = Z, E' = nZ, E" = Z/nZ (n 2 2), shows. (2) A submodule of a flat module is not necessarily a flat module (Exercise 3). 6. INTERSECTION PROPERTIES w @ 1, is surjective (no. 1, Lemma 1); finally, as L is free and hence flat, v @ 1, is injective. Thus the snake diagram (5 1, no. 4, Proposition 2, (iii)) can be applied to prove the existence of an exact sequence LEMMA 7 . Let E be a right A-module, F a l g t A-module and F', F" two submodules of (4) Consider the diagram K e r (l , @ i) - K e r (l , @ i) - G @d F ~ H H F . This being so, if E is flat, 1, @ i is injective, in other words Ker(1, @ i) = 0, and the exact sequence (4)shows that v @ 1, is injective, hence the sequence (2) is exact (taking account of Lemma 1 of no. 1). As (b) obviously implies (c), it remains to prove that (c) implies (a). Consider the diagram (3) in the case R = a, L = A,, F = AJa and apply the exact sequence (4). By hypothesis v @ 1, is injective, hence Im(d) = 0; moreover, as H is flat, we have Ker(l, @ i) = 0; the exactness of the sequence (4) then implies Ker(1, @ i) = 0, in other words, 1, @ i is injective and this proves that E is flat (no. 3, Remark 1). PROPOSITION 5. Let O + E ' & E E" -+O be an exact sequence of right Amodules. Suppose E" isflat. Then,f o r E to beflat it is necessary and sujicient that E' be flat. Let u : F' -+ F be an injective homomorphism of left A-modules. Consider the diagram IF' / E'@F   IF +E"@F 1 IF It is commutative and its rows are exact (no. 1, Lemma 1). Since E" is flat, 16 0 -+ F' n F" --f F' -+ F'/(F' n F") -+0 where the unspecified arrows are the canonical injections and surjections a n d j the canonical isomorphism defined in Algebra, Chapter I, 5 6, no. 13, Theorem 6. This diagram is commutative and its rows are exact. We derive (since F = F' F") a commutative diagram + E @ (F' n F") ----f E @ F' -+ E @ (F'/(F' n F")) 1 1E,j.1 E @ F" F E @FF E @ (F/F") , The rows of this diagram are exact (no. 1, Lemma 1) and 1 @ jis an isomorp h . Our assertion is then a special case of 5 1, no. 4,Proposition 1, (i) (cf. Exercise 5). I F . E' @ F' +E @I F' +E" @ F' lE'@U F such that F = F' + F". Then the intersection ofthe canonical images of E @ F' and E @I F" in E @ F is equal to the canonical image of E @ (F' n F"). PROPOWON 6. Let E be a right A-module and F a left A-module such that E is F-Jat. For 9dmodule F' ofF, we denote by +(F') the image ofE @ F' under the canonical g* ofE @ F' to E @ F (which is injective by D&nition 1 ofno. 2). Then, ifF', F"arc two submodules of F, we have +(F' n F") = +(F') n +(F"). 17 I A s E is E-flat, +(F’ + F”) is identified with E @ (F’ + F“), and the submodules +(F’), +(F”) and +(F’ n F”) are identified with the canonical images of E @ F’, E @ F” and E @ (F’ n F”) in E @ (F’ + F”) respectively. Proposition 6 then follows from Lemma 7. 7. m S O R PRODUCTS OF FLAT MODULES k t A, B be two rings, E a right A-module and F an (A,B)-bimodule (Algebra, Chapter 11, 3 1, no. 14).Recall (Algebra, Chapter 11, fj 3, no. 4) that E @A F has a canonical right B-module structure, for which (X Remark 1. With the hypotheses of Proposition 6, E @ F’ is usually identified with +(F’)for every submodule F’ of F, which gives the formula E @A 3 2.7 TENSOR PRODUCTS OF FLAT MODULES FLAT MODULES @y)b = x @ (yb) for X E E , ~ E F ,b E B . PROPOS~~ON 8. Let A, B be two rings, E a right A-module and F an (A,B)-bimodule. Suppose that E isjlat and that F isflat as a B-module. Then the B-module E @A F is (F’ n F”) = (E @A F’) n (E @A F”). flat. PROPOSITION 7. Let E be a right A-module, E’ a submodule of E, F a l$t A-module and F‘ a submodule of F. Suppose that E/E’ or F/F’ isflat. Then the canonical image of E’ @ F’ in E @ F is the intersection ofthe canonical images of E’ @ F and E @ F’ in E @F. k t G be a left B-module and G’ a submodule of G. Since F is flat as a right &module, the canonical homomorphism F Since E is flat, the canonical homomorphism E @a (F @B G’) E @A (F @B G) is injective. ASE @A (F QBG’) and E @A (F BBG) are canonically identified with (E @A F) BBG’ and (E @A F) BBG respectively (Algebra, Chapter 11, 8 3, no. 8, Proposition 8), the canonical homomorphism -+ Suppose for example that E/E’ is flat and consider the diagram E’ @ F’ +E @ F’ --+ (E/E’) @ F’ i i E’ @ F -+ E @ F mBG’ -+ F BBG is injective. (E/E’) @ F (E @A F) @BG’-+() @BG is hjective, which proves that E @A F is a flat B-module. where the arrows are the canonical homomorphisms. This diagram is commutative and its rows are exact (no. 1,Lemma 1). As E/E’ is flat, u is injective. Then our assertion is a special case of tj I, no. 4, Proposition 1, (i). COROLLARY 1. Let C be a commutative ring, E, F twojlat C-modules. Then E goF is aflat C-module. COROLLARY. Let E be a right A-module and E’ a submodule of E. Then E is a (C, C)-bimodule and it is sufficient to apply Proposition 8 with B = A = C. (i) that E/E’ isjlat. Then,for every lgt ideal a of A, E’a = E’ n Ea. (5) (ii) Conversely, su)bose that E i s j u t and, for everyjnitely generated l g t ideal a of A, relation (5) holdr. Then E/E’ isflat. COROLLARY 2. Let p be a homomorphism of a ring A to a ring B. If E is a Jlat right A-module, the right B-module p* (E) = Eo, obtained by extending the ring ofscalars to B (Algebra, Chapter 11, 3 5, no. 1) isflat. (i) It is sufficient to apply Proposition to the case F = A,, F’ = a. (ii) TO prove that E/E’ is flat, apply criterion (c) of Proposition 4 of no. 5; it is then necessary to establish that the sequence By definition E,, = E @A B, where B is considered as an (A,B)-bimodule bY means of p. As the right B-module B, is flat, it is sufficient to apply 0 -+ E‘/E’a -+ E/Ea -+ E/(E’ + Ea) += b p d t i o n 8. 0 COROLLARY 3. Let R, S be two rings and +: R -+ S a ring homomorphism. IfM is a aflat right R- is exact at E’/E’a for every finitely generated left ideal a of A. NOW this is precisely what relation (5) expresses. flat right S-module and +*(Sd) is aflat right R-module, then +,(M) Remark 2. The conclusion of Proposition 7 remains true if we assume only that E/E’ is F-flat or that F/F’ is E-flat. $: M and all r E R (Algebra, Chapter 11, 5 1, no. 13). Then apply Propo- 18 module. that +,(M) is the right R-module defined by x.r . ahon 8 with A = S, B = R, E = M and F = x . + (r) for all S, S having the structure 19 I of a (S, R)-bimodule defined by +; the right R-module M precisely * (M). + BSS is then PROPOSITION 9. Let (A,, foa) be a direct system of rings, A = lim A, its direct -+ limit, (E,, fpa) a direct system o f right A,-modules with the same indexing set and E = lim E, its direct limit, which is a right A-module (Algebra, Chapter 11, 5 6, . 3 no. 2). If each of the E, is afrat &-module, E is afrat A-module. Let Ek = E, where A is considered as a left &-module by means of the canonical homomorphism A, -+ A; we know that the right A-module E is canonically isomorphic to lim EL (loc. cit., Corollary 2 to Proposition 7). . 3 I t follows from Corollary 2 to Proposition 8 that E&is a flat right A-module for all a,hence E is a flat A-module by Proposition 2 of no. 3. 8. FINITELY PRESENTED MODULES Let A be a ring. An exact sequence (6) 3 follows from fj 1, no. 4, Corollary 2, (ii) to Proposition 2 that vE is surjective, and as we have just seen that vE is injective, it is bijective. LO. EXTENSION OF SCALARS: CASE OF COMMUTATIVE RINGS Now let A be a commutative ring, B a ring and p :A -+ B a ring homomorphism such that p(A) is contained in the centre of B; in other words, p defines on B an 22 2.10 &algebra structure. For every A-module E, the right B-module E(B) = E 8, B is then identified with B 8, E, the A-module structures of p,(B,) and p,(B,) being identical by hypothesis. Recall that for every ordered pair (E, F) of Amod&s, we have defined a canonical B-homomorphism a: (Horn,(% F))(B) Ho~B(E(B), F(BJ (10) such that for all u E Hom,(E, F), w (u @ 1) = u @ 1, (Algebra, Chapter 11, 8 5, no. 3). + P~oposInONI 1. Let A be a commutative ring, B a ring, p a homomorphism of A to the cmtre of B, and E and F two A-modules. Suppose that B is a j u t A-module and E is Jinitely generated (resp. jiniteb presented). Then the canonical homomorphism (10) is injective (resp. bijective). 0 is composed of the canonical isomorphism F) and the canonical homomorphism (8) HomA(E, B V: @A + HomB(E(B),F d B @A Hom,(E, F) -+ HOmA(E, B @A F) (loc. dt.), the proposition is a consequence of Proposition 10 of no. 9. Suppose now that A and B are commutative and consider three A-modules El, E,, E, and an A-bilinear mapping5 El x E, -+E,. Then there exists one and only one B-bilinear mappingf,: Ei(B) x E2(B,--+ E3(,) such that fB(l @ x19 @ x2> = @f(Xl> '2) for all x1 E El, x2 E E, (Algebra, Chapter IX, 3 1, no. 4,Proposition 1). In the statement which follows we shall suppose that B is a flat A-module and, for every submodule E' of E, (i = 1,2, 3), we shall canonically identify E;B) W i t h its image in E,(B) (no. 3, Remark 2). RE POSITION 12. Let A , B be commutative rings, p a homomorphism ofA to B, El, E,, Ea three A-modules,f: El x E, fB: -+ E, an A-bilinear mapping and E2(B) --f E3(B) itsextension. Consider a submodule F, of E,, a submodule F, of E,, and denote by T the submodule of El consisting of those x1 E El such t h a t f (x , , x,) E F, for all x2 E F,. su&ose that B is a j a t A-module and that F, isjinitely generated. Then T,, is the set of E El,,) such thatfB(x',, X L) E F3(,)fOr all X L E F,(B,. k t P be the canonical surjection E, -+ E3/F3;with each x1 E E, we associate A-hear mapping x, t+p(f (x 1 , x z)) of F, to E,/F,, which we denote 23 I 82.11 FLAT MODULES INTERPRETATION OF FLATNESS IN TERMS OF RELATIONS by g (x l) ; then g is an A-homomorphism of El to Hom,(F,, E3/F3) and the kernel of g is precisely T. Since B is a flat A-module, we have the exact sequence In the particular case when the E, are equal to the ring A, f is multiplication a d the F, ideals a,, we obtain the transporter formula -T(B) E3/F3))(B) B(a,: a), = Ba,: Ba, (12) valid when B is a flat A-module and a, is a finitely generated ideal. (no. 3, Proposition 1). By Proposition 11 the canonical homomorphism 0: (E3/F3)(B)) -+ HomB(F2(B), E3/F3))(B) is injective. On the other hand, as B is a flat A-module, (E3/F,)(B)is canonically taking the composition of o with 1 @ g, we obtain identified with E3(B)/F3(B); a homomorphism u for which the sequence 1 -----f T(B) - 11. INTERPRETATION OF FLATNESS IN TERMS OF RELATIONS (*) Throughout this no. A denotes a ring, E a right A-module and F a left Amodule. Every element of E 8, F can be written in at least one way in the form z = HomB(FZ(B), El(B) E3(B)/F3(B)) 2 e, @A where e, E E andA E F. The following lemma gives a condition I=I under which this sum is zero : is exact. I t follows immediately from the definitions that u (x ;) , where = @ E1(B), is the linear mapping which maps each x; E F,,,, to the class mod. F3(B)of f B (x ; , x;) ;by linearity this is also true for all x; E El(B);since the kernel of u is TCB), the proposition is proved. LEMMA 10. Let (f h) h o L be a family of generators of F and (e h) h E La family of elements o f E ofjinite support. For eh 8f h = 0, it is necessary and that A€L t h e exist ajnite set J, afamily (x j) ofelements ofE and afamily (ajh)(j E J, A E L) of elements of A with thefollowing properties: 2 (1) thefamily (ajh) harjnite support; COROLLARY 1. Let A, B be two commutative rings, p: A -+ B a homomorphism such that B is a frat A-module and E a j n i t e h presented A-module. For every Jinitely generated submodule F o f E, the submodule ofthe dual ofEo, orthogonal to F(B)is equal to (F')(B),where F' is the submodule ofthe dual E* o f E orthogonal to F. 2ajhf h 0for all j J; (3) eh = 2 xja,,for all A L. (2) = E A€L E IeJ By Proposition 11 (E*)(,, is canonically isomorphic to the dual (E(B))*(cf. Then it suffices to apply Proposition 12 with E, = E*, E, = E, E, = A, F, = F, F, = {0}, and f the canonical bilinear form on E* x E. COROLLARY 2. Let A, B be two commutative rings, p: A --f B a homomorphism such that B is aflat A-module and E an A-module. Then,for everyjinitely generated submodule F o f E, the annihilator ofFo) is the ideal aB ofB, where a is the annihilator ofF in A. Loosely speaking, the system of eh must be a linear combination with coefficients in E of systems of elements of A which are “relations between the K'. Consider the free A-module A$L),its canonical basis (uh) and the homomorphism g : AiL)-+ F such that g(uh) = f h for all A E L ; denoting by R the kernel of g, we have (since the f Agenerate F) an exact sequence I t suffices to apply Proposition 12 with El = A, E, = E, = E, F, = F, F, = (0). R -AA - ~A F -o Remark. If there is no ambiguity over the modules E, nor the bilinear mapping Where i denotes the canonical injection. By Lemma 1 of no. 1 we derive the exact sequence f, F,: F, is sometimes used to denote the module denoted by T in Proposition (13) 12 and it is called the transporter of F, to F,. The conclusion of Proposition 12 then reads (11) 24 F3(B): FZ(B) = (F3: F2)D 0 + E' @s F(s)+ E" @s FW -+ E" @S ! ! ,! F(s)+ 0 (2) 0 = Tor?(.(p*(L),F)*Toe(p*(E),F) -+ p*(H) But as F,,, is flat, the homomorphism H @, F,,, is identified with the homomorphism p*(H) @R --f Then it follows from (2) that To*(p,(E), p*(L) --f @R @ItF+ p*(L) i Jd ! E' --+ C' A' which proves that Fo, is flat. Conversely, if (b) holds, we have first of all, for every free right S-module L = SY), Tory(p,(L), F) = (Tor?(p,(S,), F))") = 0. Every right S-module E can be written in the form E = L/H for a suitable free S-module L ; then we have the exact sequence A" ----f B" --+ I)' -z C" I A"' ---f B"' @RF' U"' in which the rows and columns are assumed to be exact, d and u" injective and a' surjective. Show that under these conditions u'" is injective. Generalize this L @, F,,) is injective and rwult. F' 4. Consider a commutative diagram of commutative groups F) = 0. A--+B---tC---+D Remark. Proposition 2 also follows from the existence of the exact sequence I E @s TOrT(p*(Sd),F) Tor?(P*(E), F) Tor?'(E, Sd @R F) 0 arising from the spectral sequence of the "associativity" of the Tor functors. I 38 --f --f --f . - A' .--f B' -----f C' wherethe two rows are assumed to be exact. D' 39 EXERCISES EXERCISES (a) Show that, if a is surjective and b and d injective, then c is injective. (b) Show that, if d is injective and a and c surjective, then b is surjective. §2 5. Suppose that an exact sequence A 4A -% A" -+ 0 and two surjective homomorphisms B' -$A', B" 5A" are given, where A, A', A , B', B" are modules over the same ring. Show that, if B" is a projectiue module, then there exists a surjective homomorphism a : B f @ B" A such that the diagram -LB~ BB"-%B~ B' A'If, A L A " is commutative (i and p being the canonical mappings). 6. Suppose that an exact sequence 0 + A % A -% A" and two injective homomorphisms A' % C', A" % C" are given, where A, A', A", C', C" are modules over the same ring. Show that, if C' is an injectiue module (Algebra, Chapter 11, 9 2, Exercise 1 l) , there exists an injective homomorphism a : A ---f C' @ C" such that the diagram A'If, a,! C' A @ 2. Let M, N be two submodules of an A-module E such that M + N is flat. For M and N to be flat, it is necessary and sufficient that M n N be flat. 3. Let A be the ring K[X, Y] of polynomials in two indeterminates over a field K. (a) Consider in A the principal ideals b = (X), c = (Y) ,which are free Amodules and whose intersection b n c = (XU) is also free. Show that a = b + c is not a flat A-module, although a is torsion-free (cf. Algebra, Chapter 111, 0 2, Exercise 4). (b) In the A-module A2, let R be the submodule consisting of the elements (x, - x) where x E a. I n the A-module A2/R, let M, N be the submodules which are the images of the factor submodules of A2; show that M and N are isomorphic to A, but that M n N is not a flat A-module. 4. (a) Give an example of an exact sequence L A " a 1 -L C' 1. Give an example of an exact sequence 0 -+ N' -+ N -+ N" -+ 0 of left &modules and a right A-module E such that E is "-flat and N"-flat, but not &flat (take for example N' = N" = 2/22). 0 -+ E'+ E --f E" -+ 0 a-1 which does not split and all of whose terms are flat modules (cf. Algebra, Chapter VII, 3 3, Exercise 8 (b)). (b) From (a) deduce an example of an exact sequence C" --L C" are commutative (i and p being the canonical mappings). 7. Let U, V, W be three commutative groups and f:U -+ V, g: V -+ W homomorphisms. (a) Consider the diagram 0 -+ E ' - + E -+E" -+ 0 which does not split and whose terms are right A-modules which are notJat, such that for every left A-module F the sequence O + E ' @ F + E @ F + E " @ F-tO B o ~ u ~ u x v + v + - o f.1 O+V--+W h1 ,-4 is exact (use Lemma 2 of no. 11. 5. Give an example of a right A-module E, a left A-module F and two subflodules F" of F suchofthat canonical imageofof EE 66F'(F'and n F") in F" E 6b(cf. F not theF',intersection thethe canonical image; x V-W-+O 6 - wherex(u) = (u , f (u)) , N u , u) = v - f (u) , y(u) = (g(u) , u) , a(m,u) = w -g(u), h(u, v) = (g (f (u)) , v). Show that this diagram is commutative and that its rows are exact. (b) Deduce from (a) and Proposition 2 of no. 4 an exact sequence Exercise 3 (a)1. 0 -+ Ker(f) + Ker(g o f) where L, is a free left A-module (0 < i < n) , is called a presentation of M o f 4 t h n or an n-presentation of M. The presentation is called finite if all the L, are finitely generated free modules. --f Ker(g) -+ Coker(f) Give a direct definition of this exact sequence. 40 -+ Coker(g o f) -+ Coker(g) -+ 0. fl6. Let A be a ring and M a left A-module. An exact sequence L, -+ L n - l -+. . *-+ L, -+ Lo -+ M -+ 0 41 EXERCISES EXERCISES If M is a finitely generated left A-module, we denote by A(M) the least upper bound (finite or +CO) of the integers n 2 0 such that M has a finite npresentation. If M is not finitely generated, we set A(M) - 1. (a) Let 0 -+ P -+ N -+ M -+0 be an exact sequence of left A-modules. Then A(N) 2 inf(A(P), h (M)) . (Starting with two n-presentations of P and M respectively, derive one for N using Exercise 5 of 9 1.) (b) If a is a left ideal of a ring A which is not finitely generated, AJa is a monogenous A-module which does not admit a finite presentation, in other words A(A,/a) = 0 (no. 8, Lemma 9). (c) Give an example of a monogenous left ideal a of a ring A such that A,/a (which has a finite presentation) admits a dual which is not a finitely generated right A-module. (d) Let K be a commutative field, E the vector space KCN), (en) the canonical of E and T the tensor algebra of E, which therefore has a basis consisting of fie finite products el,eiz. . .elk (k 2 0, i, E N for all j) . For a given integer n, let b be the two-sided ideal of T generated by the products =I (b) Let M, 2 M,- +. . .-+ M, 2 M + 0 be a finite n-presentation of M; show that, if h (M) > n, Ker(u,) is a finitely generated A-module. (Let L,+, % L , ~ . .-+ . 1'0 u1 L, --%L, -+ L, --+ M -0 be a finite (n + 1)-presentation of M and let P = Ker(u,) be such that there is an n-presentation of P: L,,, = L, -----f.. .--f L, "2, L, u1 --f @ L,,, w''-'. . .-% 5 Lo -+ 0 0 -+ Ker(v,+,) -+ Ker(w,) -+ Ker(u,) -+ 0 (5 1, M,-, 0 L, M, @ L, and exact sequences no. 4, Proposition 2). Observe finally that Ker(w,) is a direct factor of M, @ L,,,. (c) Show that with the hypotheses of (a) A(M) 2 inf(A(N), A(P) + 1). (If n < inf(A(N), A(P) + l), show by induction on n that A(M) 2 n, arguing as in (a) and using (b).) (d) Show that with the hypotheses of (a) A(N) = = A(P) + 1. inf(A(M), A(P)). In particular, for N to admit a finite presentation it is necessary and sufficient that M and P do so too. (f) Let N,, N, be two submodules of an A-module M. Suppose that N1 and N, admit finite presentations. For N1 + N2 to admit a finite presentation it is necessary and sufficient that N, n N, be finitely generated. 7. (a) With the notation of Exercise 6, show that, if M is a projective module, then h(M) = - 1 or A(M) = + CO. IfA is a left Noetherian ring, then, for every A-module M, A(M) = - 1 or A(M) = +a. 42 J enen - I and e,+ke, for all k 2 1 ;let A be the quotient ring T / b , and for every integer m, let a,,, be the canonical image of em in A. Show that, if M = A,/Aa,, then X(M) = n (observe that, for m < n - 1, the left annihilator of a, is Aa,, and use Exercise 6(b)). 8. Let C be a commutative ring and E, F two C-modules. Show that X(E B0F) 2 inf(A(E), A(F)). 9. Let E be a finitely presented left A-module. (a) Show that for every family (FJLEIof right A-modules, the canonical F,) -+ (E 8, F,) (Algebra, Chapter 11, 9 3, homomorphism E 8, (n n 1El LEI no. 7) is bijective. (b) Let (G,, (bPa) be a direct system of left A-modules; show that the Canonical homomorphism lim Hom,(E, G,) + Hom,(E, lim G,) is bijective. A(P) 2 inf(A(N), A(M) - 1). (Same method as in (c).) Deduce that, if A(N) = + CO, then A(M) (e) Deduce from (a), (c) and (d) that, if N = M @ P, then ... , P d 0. Applying the method of (a) to the exact sequence 0 -+ P -+ Lo + M -+ 0 we obtain an exact sequence M, e1e0, --+ --+ 10. (a) Let A be a ring, I a set and R a submodule of L = AT). Let 6 be (J,S), where J is a finite subset of I and S a finitely generated submodule of A; n R. 6 is ordered by the relation '7 c J' and sty';show that 6 is directed with respect to this order relation, that the family (&/S) is a direct system of right A-modules with 6 as indexing set and there exists an isomorphism of L/R onto lim_ (A#). *e Set of ordered pairs (J,S) E6 (b) Deduce from (a) that every A-module is a direct limit of finitelypresented A-modUles. 11. Let E be a right A-module. E is called pseudo-coherent if every finitely , Bcnerated submodule of E is finitely presented; every submodule of a pseudo-herent module is pseudo-coherent. E is called coherent if it is pseudo-coherent mcl finitely generated (and therefore finitely presented). 43 EXERCISES EXERCISES (a) Let 0 -+ E' -+ E -+ E" -+ 0 be an exact sequence of right A-modules. Show that, if E is pseudo-coherent (resp. coherent) and E' is finitely generated E" is pseudo-coherent (resp. coherent). Show that, if E' and E" are pseudocoherent (resp. coherent), so is E. Show that, if E and E" are coherent, so is E' (use Exercise 6 and Lemma 9 of no. 8). (b) Let E be a coherent A-module and E' a pseudo-coherent (resp. coherent) A-module. Show that, for every homomorphism u: E -+E', Im(u) and Ker(u) are coherent and that Coker(u) is pseudo-coherent (resp. coherent) (use (a)). (c) Show that every direct sum (resp. every finite direct sum) of pseudocoherent (resp. coherent) modules is a pseudo-coherent (resp. coherent) module. (d) If E is a pseudo-coherent module and M, N are coherent submodules of E, show that M + N and M n N are coherent (use (a) and (c)). (e) Suppose that A is commutative. Show that, if E is a coherent A-module and F a coherent (resp. pseudo-coherent) A-module, Hom,(E, F) is a coherent (resp. pseudo-coherent) A-module. (Reduce it to the case where F is coherent and consider a finite presentation of E, then use (b).) (f) Deduce from (e) that every polynomial ring (in any finite or infinite set of indeterminates) over a Noetherian commutative ring is coherent. Deduce from this that a quotient ring of a coherent ring is not necessarily coherent.* (g) For A to be left coherent, it is necessary and sufficient that the left annihilator of every element of A be finitely generated and that the intersection of two finitely generated left ideals of A be finitely generated (use Exercise 6(f)). T[12. (a) Let A be a ring. Show that the following four properties are equivalent: $ 7 13. Let A, B be two rings, F an (A, B)-bimodule and G a right B-module. Show that, if G is injective (Algebra Chapter 11, $ 2, Exercise 11) and F is a flat left A-module, the right A-module Hom,(F, G) is injective. (Use the isomorphism Hom,(E, Hom,(F, G)) -+Hom,(E for a right A-module E (Algebra, Chapter 11, $ 4, no. l).) fi 14. Let A, B be two rings, E a left A-module, F an (A, B)-bimodule and G a right B-module; consider the canonical homomorphism (Algebra, Chapter 11, 6 4, Exercise 5) IS: (a) The right A-module A, is coherent (Exercise 11). (p) Every finitely presented right A-module is coherent. Hom,(F, G) such that (IS( x)) (v) defined similarly. (b) Show that every right Noetherian ring is right coherent. Give an example of a right Artinian ring which is not left coherent (cf. Algebra, Chapter VIII, $ 2, Exercise 4). * (c) The ring of a non-discretevaluation of height 1 (ChapterVI) is coherent but contains ideals which are not coherent and admits (monogenous) quotient modules which are not pseudo-coherent. * (d) Show that, if A is a right coherent ring, then, for every right A-module E, A(E) = - 1 or A(E) = 0 or A(E) = +co (Exercise 6). (e) Let (A,, +o,) be a direct system of rings whose indexing set is directed and let A = lim A,. Suppose that, for a < p, A, is a flat right A,-module. + Show that, if the A, are right coherent, so is A. (Observe that A is a flat A,module for all a and that, if E is a finitely generated submodule of A,, there exists an index a and a finitely generated submodule E, of (&)d such that A is isomorphic to E.) E, 4'4 @A E -+Hom,(Hom,(E, F), G) = u (v (x)) for (y) Every A-module A: (I an arbitrary set) is flat. (6) Every product of flat left A-modules is flat. (TO prove that (a) implies (p), use Exercise ll(b). To see that (y) implies (a) , use Proposition 13 of no. 11 and argue by reductio ad absurdurn. To show that (a) implies (8),use Exercises 9.) Such a ring is called right coherent and the concept of a left coherent ring is 8, F, G) v all x E E, u E Hom,(F, G), E Hom,(E, F). Show that, if G is an injective B-module (Algebra, Chapter 11, $ 2, Exercise 11) and E finitely presented, IS is bijective. (Consider first the case where E is free and finitely generated.) 7 15. Let A be a ring. Show that every left A-module E which is flat and finitely presented is projective. (Given a surjective left A-module homomorphism I: F + F", let u' be the homomorphism Hom(l,, u) : Hom,(E, F) -+ Hom,(E, F") and the homomorphism HOm(U', lc) : Hom,(Hom,(E, F"), G) -+ Hom,(Hom,(E, F,) G) , where G is a divisible Z-module. Using Exercise 14 first, prove that ii is injective; then, with a suitable choice for G (Algebra, Chapter 11, $2, Exercise 14)3 Show that u' is surjective.) 16. Let A be a ring and a an element of A. Show that the following properties equivalent. (a) aEaAa. (p) aA is a direct factor of the module Ad. 45 EXERCISES EXERCISES (y) A,/aA is a flat right A-module. (6) For every left ideal b of A, aA n b = ab. (Use the Corollary to Proposition 7 of no. 6 to prove the equivalence of (y) and (6) and show directly that (6) implies (a) and (a) implies (p), by proving the existence of an idempotent element e E aA such that eA = aA.) 17. Let A be a ring. Show that the following properties are equivalent: (a) Every element a E A satisfies the equivalent properties of Exercise 16. (p) Every finitely generated right ideal of A is a direct factor of A,. (y) Every left A-module is flat. (8) Every right A-module is flat. Then A is called an absolutelyJlat ring (*). (To see that (a)implies (p), use Exercise 15(b) ofdlgebra, Chapter VIII, 3 6.) 7 18. Let A be an absolutely flat ring (Exercise 17). (a) Let P be a projective right A-module. Show that every finitely generated submodule E of P is a direct factor of P. (Reduce it to the case where P is free and finitely generated. Then note that P/E is finitely presented and use Exercises 15.) (b) Show that every projective right A-module P is the direct sum of monogenous submodules isomorphic to monogenous right ideals of A. (Use Kaplansky's Theorem (Algebra, Chapter 11, 3 2, Exercises 3) to reduce the problem to the case where P is generated by a countable family of elements, then use (a).) (c) Give an example of an absolutely flat ring A and a non-projective finitely generated A-module (consider a quotient of A by an ideal which is not finitely generated; cf. Algebra, Chapter VIII, 3 6, Exercise 15(f) and Commutative Algebra, Chapter 11, 9 4, Exercise 17). 19. Let A be a ring. Show that the following properties are equivalent: (a) A is semisimple. (p) Every right ideal of A is an injective A-module. (y) Every right A-module is projective. (6) Every right A-module is injective. 20. Let A be an integral domain, B an A-algebra which is a flat A-module and M a torsion-free A-module. Show that, if t E B is not a divisor of zero, the relation t. z = 0 for z E B @A M implies z = 0. (Reduce this to the case where M is finitely generated and, by embedding M in a finitely generated free Amodule, to the case where M = A.) 21. Let S be a commutative ring, R a commutative S-algebra, B an Salgebra (commutative or otherwise) and B(R, the R-algebra obtained from B by extension of scalars. Suppose that R is a flat S-module and that B is a finitely generated S-module. If Z is the centre of B, show that the canonical homomorphism of Z,,) = Z BSR to B(R) is an isomorphism of Z,,, onto the centre of B(R). (Use the exact sequence e 0 +Z -+ B -+ Homs(B, B) where O(x) (y) = xy - yx, and Proposition 11 of no. 10.) T[22. Let E be a left A-module. For every right ideal a of A and every element a E A, denote by a: a the set of x E A such that ax E a and by aE: a the set of y E E such that ay E aE. Then clearly (a: a)E c aE: a. Show that, for E to be flat, it is necessary and sufficient that, for every right ideal a of A and every element a E A, (a: a)E = aE: a. (To see that the condition is necessary, 6 A,/a, consider the exact sequence of right A-modules 0 -+ (a: .)/a -+ A,/a + + J where is the canonical injection and the mapping obtained by taking quotients under left multiplication by a. To see that the condition is sufficient apply the criterion of Corollary 1 to Proposition 13 of no. 11 : starting with a n 2 0, where a, = 2atA and the element relation a,x, = a, E A, x, E E, apply the hypothesis to the ideal t=1 n t=a a, and argue by induction on n.) 23. (a) Let 0 -+ R + L -+ E -+ 0 be an exact sequence of left A-modules, where L is a free A-module; let (e,) be a basis of L. Show that the following conditions are equivalent: (a) E is flat. (p) For all x E R, if a, is the right ideal generated by the components of with respect to the basis (e,), then x E Ra,. (y) For all x E R, there exists a homomorphism u,: L -+ R such that %(X) = x. (8) For every finite sequence of elements of R, there exists a homomorphism u : L --f R such that u(x,) = xi for 1 < i < n. (Use the Corolto Proposition 7 of no. 6.) (b) Let a be a left ideal of A such that A/a is a flat A-module. Show that, for finitely generated left ideal b c a, there exists x E A such that * k' b c k u c a (*) This is a modification of the terminology “regular ring” introduced in Algebra, Chapter VIII, 3 6 , Exercise 15, as this has a completely different meaning in Commutative Algebra. 46 (use condition (8) of (a)). (c) Derive from (a) a new proof of the result of Exercise 15. 47 EXERCISES EXERCISES (d) Let r be the Jacobson radical of A and 0 + R -+ L + E + 0 an exact sequence of left A-modules such that L is free. Suppose that E is flat and R is contained in rL. Show that R = 0 (in the notation of (a) observe that a, is a finitely generated ideal and that a, = a%r). (e) Let E be a finitely generated flat A-module; suppose that there exists a two-sided ideal b ofA contained in the Jacobson radical of A such that E/bE is a free (A/b)-module. Show that E is then a free A-module relation b' = S-lA is equivalent to the relation b n S # 0 , the latter expressing the fact that b' contains invertible elements of S-lA. I t followsfromno. 4, Proposition 10 (iii) that 6' H b = (i:)-l(b') isan isomorphism (with respect to inclusion) of the set of ideals of S-IA distinct from S-lA onto the set 5 ofideals ofA not meeting Sand satisfying condition (MS) of Proposition 10. If b' is maximal (resp. prime), clearly 6' is maximal in 5 (resp. prime) and conversely (by (i)). On the other hand, if t is an ideal of A disjoint from S, its saturation tl with respect to S is an ideal of A containing t and dis70 where 2. Let A be a ring and S a multiplicative subset o f A. For every ideal a o f A not meeting S t h e exists a prime ideal containing a and not meeting S. COROUARY s-'! -g ~ ~ # S-IA (Remark) and hence there exists a maximal ideal of S-lA conS-la (Algebra, Chapter I, § 8, no. 7, Theorem 2) and the corollary O from W S Proposition 11 (ii). cOROLLAR~ &ad ..ii:* 3. Let A, B be two rings, p a homomorphismfrom A to B and p a prime $A. For there to exist a prime ideal p' ofB such that pl(p') = p, it is necessary that pl(Bp(p)) = p. 71 $2.6 NILRADICAL AND MINIMAL PRIME IDEALS LOCALIZATION I1 If there exists an ideal p' of B such that pl(p') = p, then p(p) c p', whence 6. NILRADICAL AND MINIMAL PRIME IDEALS Bp(p) c p' and >'(Bp(p)) c pl(p') c p; as the converse inclusion is obvious, In a (commutative) ring A the set of nilpotent elements is an ideal, for if x, y are elements of A such that xm = y" = 0, then (x y),+, = 0 by the binomial theorem. ol(Bp(p)) = p. Conversely, suppose that pl(Bp(p)) = p and consider the multiplicative subset S = p(A p) of B; the hypothesis shows that - S n Bp(p) = 0; by Corollary 2 there exists a prime ideal p' of B containing Bp(p) and not meeting S; then pl(p') contains p and cannot contain any element of A and hence is equal to p. -p COROLLARY 4. Let A, B be two rings and p a homomorphismfrom A to B. (i) Suppose that there exists a B-module E such that p,(E) is a faithfullyJlat Amodule. Then,for every prime ideal p of A, there exists a prime ideal p' of B such that P1(Pf) = P. (ii) Conversely, suppose that B is ajlat A-module. Then, ;f,for every prime ideal p of A, there exists an ideal p' ofB such that ;'(PI) = p, B is afaithjiullyj7at A-module. (i) The hypothesis implies that, for every ideal a of A, i1(Bp(a)) = a (Chapter I, 3 3, no. 5, Proposition 8 (ii)) and it is sufficient to apply Corollary 3. (ii) It is sufficient to show that, for every maximal ideal rn of A, there exists a maximal ideal rn' of B such that D'(rn') = rn (Chapter I, 5 2, no. 5, Proposi- tion 9 (e)). Now there exists by hypothesis an ideal q ofB such that i l (q) = rn; as q # B, there exists a maximal ideal rn' of B containing q and consequently -1 p (m') 3 rn; but, as -1 i1(rn')cannot contain 1, p (rn') = rn. COROLLARY 5. Let A be a ring, S a multiplicative subset ofA and B a ring such that if(A) B c S - I A . Let q be aprime ideal ofB such that theprime ideal p = (iz) (9) ofA does not meet S and let p' be the prime ideal S-lp o f S- lA. Then p' n B = q. Let S' = i z (S) ; a canonical isomorphism has been defined from S'-'B to S - l A (no. 1, Corollary 4 to Proposition 2) ;we identify these two rings by means of this isomorphism. As q n S' = @, q' = S'-lq is the unique prime ideal of S - I A = S'-lB such that q' n B = (i:)-l(q') = q (Proposition 11 (ii)), whence (iz)-l(q') = p; consequently q' = p' (Proposition 11 (ii)). I n the notation of Corollary 5 , there are canonical isomorphisms of A, and B, onto (S- 'A),. (Proposition 11 (iii)) and hence a canonical isomorphism A, --f B,. 72 + DEFINITION 4. The ideal of nilpotent elements of a (commutative) ring A is called the nilradical o f A. If a is an ideal of A, the inverse image, under the canonical mapping A -+ A/a, of the nilradical of A l a is called the radical of a. We often denote by r(a) the radical of an ideal a of A. To say that an element x E A belongs to the radical of a means therefore that there exists an integer n > 0 such that xn E a. Iff is a homomorphism from A -1 to a ring B and b is an ideal of B, the radical off (b) is the inverse image under f of -1 the radical of 6, for to say that xn Ef (b) means that (f (x))" E 6. The nilradical of a ring A is contained in its Jacobson radical (Algebra, Chapter VIII, 3 6, no. 3, Corollary 3 to Theorem 1) but may be distinct from it; it is always equal to it if A is Artinian (Algebra, Chapter VIII, 3 6, no. 4, Theorem 3). We say that a prime ideal p of a ring A is a minimal prime ideal if it is minimal the set of prime ideals of A ordered by inclusion. PRoPosmoN 12. Let p be a minimal prime ideal o f a ring A. For all x s E A p and an integer k > 0 such that sxk = 0. - E p, there exists - The set S of elements of the form sxk (k an integer > 0, s E A p) is a multiplicative subset of A. If 0 4 S, there would exist a prime ideal p' not meeth g S (no. 5, Corollary 2 to Proposition 11). Then p' = p and p' # p since # p', contrary to the hypothesis that p is minimal. ~ O P O S I T I O N 13. The nilradical o f a ring A is the intersection of all the prime ideals of A and it is also the intersection o f the minimal prime ideals o f A. clearly, if x E A is nilpotent, it is contained in every prime ideal of A (5 1, no. 1, Definition 1). Conversely, let x be a non-nilpotent element of A; the set s (k an integer 2 0) is then a multiplicative subset of A not containing 0 a c l hence there exists a prime ideal p of A not meeting S (no. 5, Corollary 2 to %&tion 11) and afortiori x $ p; this establishes the first assertion. To prove second, it is sufficient to prove h2. Every prime ideal o f a ring A contains a minimal prime ideal o f A. 73 I1 3 2.7 LOCALIZATION MODULES OF FRACTIONS OF TENSOR PRODUCTS I t is sufficient, by Zorn's Lemma, to show that the set P of prime ideals, ordered by the relation 3 , is inductive. Now, if G is a non-empty totally ordered subset of P, the intersection po of the ideals p E G is also a prime ideal: for if x 4 po and y 6 po, there exists an ideal p E G such that x 6 p and y 6 p, whence xy 6 p and a fortiori xy 6 po. w e write S = A p; then the ring A, = S - l A is identified with a subring of S-IB (no. 1, Proposition 2) and on the other hand A, has only a single prime ideal p' since p is minimal (no. 5, Proposition 11). As S-IB is not reduced to 0 (since it contains A,), it has at least one prime ideal r' and therefore c' n A, = p'; if -1 j = :i and we write t = j (t ') , then Remark. In 3 4, no. 3, Corollary 3 to Proposition 14, we shall show that in a Noetherian ring the set of minimal prime ideals isfinite; moreover we shall see later that every decreasing sequence of prime ideals in a Noetherian ring is stationary. COROLLARY 1. The radical o f an ideal a in a ring A is the intersection of the prime ideals containing a and it is also the intersection o f the minimal elements of this set of prime ideals. COROLLARY 2. For an ideal a of a ring A we denote by r(a) the radical ofa. Then,for two ideals of a, b of A, r(a n 6) = r(ab) = r(a) n r(b); in particular, ifa c 6, then r(a) c r(b). For a prime ideal to contain a n b (or [illegible] ideal of A and k = A/m the residue field; the hypothesis implies that B @A k = B/mB # 0; since the tensor product is associative, (E @A B) @A k is isomorphic to E @A (B @A k), hence also to E @A (k @k (B @A k)) and finally to (E @A k) @k (B @A k) ; by § 3, no. 2, Proposition 4, E @A k # 0, since E is finitely generated and E # 0 (Algebra, Chapter 11, § 3, no. 7) and a fortiori E @A B # 0. LEMMA 3. Let B be a local ring and E and E' two finitely generated B-modules. If E' # 0 and E" # 0, then E @B E" # 0. --O P T I O N 20. Let A be a ring and M a finitely generated A-module. For every @'-ideal p E Supp(M), there exists a non-zero h-homomorphism w : M + Alp. Supp(M @A M') (10) = Supp(M) n Supp(M'). Let k be the residue field of A, = @, h : A,/p.A, (Chapter 1, § 3, no. 7). Since M, is finitely generated and M, # 0, (k @B E') # 0; then we deduce that Let p E Supp(M). As M is finitely generated and M, # 0, (k @B E") # 0 (Algebra, Chapter 11, § 3, no. 7). But, since the tensor product is associative (loc. cit. § 3, no. 8), Proposition 4). Let K = A/pA, be the field of fractions of the integral domain A/p; since M,/pM, is a vector space over K, which is not reduced to 0, there exists a non-zero linear form u : M,/pM, -+ K. If (x)l 1. Since E m, there 8 exists a family (ah,€ of elements A of finite support such that y = a,xh and we may assume that each of the ah is homogeneous of degree i - deg(k,) (by replacing it if need be by its homogeneous component of that degree) ; as deg(x,) > 0, the induction hypothesis shows that ah E# for all Ahl, whence y E A' and A c A', which proves that (a) implies (b). ,2A, be a graded commutative ring with positive degrees and m the graded ideal ,)% A,. COROLLARY. Let A = (i) The following conditions are equivalent: (a) The ideal m is afinitely generated A-module. (b) The ring A is a finitely generated graded A,-algebra. (ii) Suppose that the conditions of (i) hold. Let (f,) (i E I,) be a family of homogeneous elements of A in a system of generators of the A-module (b) , and (iii) Let (x,),, be a system of homogeneous elements (respectively generators) of the A,-module A), so is the family consisting of the homogeneous components of the y n = the equivalence of conditions (a) and (b) then follows from Proposition 1. (ii) We may suppose that As (a) and generated (as an A,-algebra) by the family consisting of the homogeneous components of (1 < i < n) of a finite system of generators of A and let m, (1 < i < n) of the A,-module A is generated (as an A,-module) by homogeneous elements y, (1 < j < s) (of h, = deg(A,), = deg(x,) then the formula in the statement). In the set of m, for i ≠ j, Let n, be the integers > 0 satisfying the relation 2 nthi = n; for each n there is a finite number of families (,ii,) 1 of integers satisfying these conditions, since h, 2 1 for all i; we conclude that M, is a finitely generated A,-module and moreover clearly M, = {0} when R < inf(h,). i) xp '. PROPERTIES OF THE RING A(d) 6 A = € Z A, be an integral domain. Let A be a graded ring of type N, A = (4),, and M = (M,)n a graded A-module; such that each of the Mand ideals of A an integer > 0 and 0 set r < d. Clearly Ad(0) is a graded submodule of M, Ad(0) = Ad(0)-module; We call M(d) is the A(d)-module, as a graded sub-A(d)-module of M, h(d,k). We shall write M(d)instead of M(d,0) (0 < k < d - 1). PROPOSITION 2. Let A = ,0 r,2n, be a graded commutative ring with positive degrees and m = ,0 A, be a graded A-module. Suppose that A is a finitely generated graded A,-algebra. Then, for every ordered pair (d, k) of integers such that d 1 and 0 < k < d - 1: (i) A(d) is a finitely generated graded A,-algebra and M a finitely generated graded A-module; (ii) M(d,k) is a finitely generated A(d)-module. Let us show that A is afinitely generated A(d)-module. Let (x,) be a system of generators of the A,-algebra A consisting of homogeneous elements. The elements of A (finite in number) of the form ayk2 . . .x,a such that 0 < a, < d for 1 < i < n constitute a system of generators of the Ad)-module;A for every homogeneous element y of A is a linear combination with coefficients in A, of elements of the form x; . . . x,", where the n, are positive integers. This being so, write n, = q,d + r, with q, E, for i 1 < i < n, the integers q,, < d (1 < i < s) ; then aye a, - (a, . . .a, - (a,' . . a,, :a:) (loc. cit. a:) which proves our assertion, for every homogeneous element y of degree nd + k E A satisfies xd E A(d).Then, if M is a finitely generated A-module, it is also finitely generated A(d)-module, which proves (ii). Let US apply the above to the graded A-module rn = @ A,, which is finitely 12.1 generated by the hypothesis (a) of 8, which shows that M, is jointly generated A(d)-module; therefore (no. 2, Corollary to Proposition 1) A(d) is a finitely generated A(d)-algebra. LEMMA 1. Let A be a graded commutative ring with positive degrees such that A = Ao[Al]. M a graded A-module and (y)As a system of homogeneous generators of M such that deg(y,) 0 for all m 0 A € L. Then,for all n > no and all k 3 0; M,,,, = A, M,. Let M be the sub-module of M generated by x and E M, Since the generated by the M, since the n > no and x E M,. Since the family of (ah)hPL of elements of a finite support and that each of the a, is homogeneous of degree n + 1 - deg(yh) (replacing it if need be by its homogeneous component of that degree). As 158 § 1.3 PROPERTIES OF THE RING A = Ao[Al] and deg(y,) > 0, each ah is a sum of elements of the form bh' where b E A, b' E A, whence E A,M, Then M, = AlM, whence, n, = AkM, by induction on k. LEMMA 2. Let A be a graded commutative ring with positive degrees and M a graded A-module. Let S be a graded commutative A-algebra with positive degrees, which is a jointly generated A,-module. The proof then consists in then (i) For n 2 no and k 2 s, n + k < n + s.k. S n + Rk) Lemma 1 there exists an integer no >0 such that: (i) For n 2 no and k 2 0, Sn) = S0[d]; (ii) M, E, n = A, E, whence a fortiori S,,, = S, S,, which establishes (i). Then, for d 3 no and m 3 0, Smd + (S,)msa Suppose that n + no is an integer. Let no be such that M is generated by the Mi; (iii) Let N be the smallest integer such that Iki i 1 to n by induction on m applying (i); this establishes (ii) go PROPOSITION 3. Let R = R, be a graded commutative ring with positive degrees, A = R(d) and n is a graded R-module. Suppose that R is a finitely generated R,-algebra. Then there exists an integer e 2 1 such that R(me)= R,[R,,] and R(m) = R for all integers m 2 0. There exists an integer m > 0 such that M is generated by a finite number of Let n = A,B, = A, whence m 3 n. Let E, = A E, Let b the elements x y are then all deg(x), h E x, and that the sub-Ro-algebra of R generated by the elements x, y, z is a graded subalgebra of R, and R, = 0 if i is a multiple of d. Let A (resp. S) be the graded ring whose underlying ring is R (resp. R(d))and whose graduation consists of the A, = R, (resp. S, = R,). Then A = A,[A,] by definition of B. Consider the elements of R (finite in number) of the form " ~ x, T x, ~ where 0 Gcj < q, and all k + . + eahs = 0 (mod. q) ; let us show that they generate the B-module R(d) l t is sufficient to prove that every element of R(') of the form x(') x; . x; is a B-linear combination of the above elements. Now, there exist positive integers k,, r, such that nj = k(q, r) where r - 3 z rjhj = 0 (mod. q) ; as the S is a finitely generated A-module, Lemma 2 can be applied; there exists no such that for d 3 no, s'd) = So[S] and hence R(Qd) = R,[R(qd) for n 2 no. The proposition follows with e = qn for q = 0 (mod. q), whence n E q-a Q by hypothesis and the S. and by definition, this proves our assertion. As 159 GRADUATIONS, FILTRATIONS AND TOPOLOGIES 111 § 1. GRADED PRIME IDEALS .2A, be a graded commutative ring with positive degrees and m the graded ideal ,% A,. Let p be a prime ideal of A. We suppose that A is a graded commutative ring with a prime ideal p which is a domain and we write A = A/p, the integral domain A, with the statement is obviously necessary. If A, = A, for all n 2 no, the proposition is a solution to the problem; then any element of A of degree n with this property, however, any two of these elements are obviously equivalent. Suppose then that there exists an element x of A, with (x)A is an integral domain (Algebra, Chapter 11, § 11, no. 4, Proposition 1). .9 $a, be a graded commutative ring with positive degrees and m the graded ideal ,% A, and let m be an integer > 0. To show that for Let p be the set of elements such that x,y E p we define conditions under which r,x E p : 0, p, such that x, y E p, hence x,y E p, then PROPOSITION 5. Let A be a sufficient that, for all x E A,, the element E A : x,y E p. Let x E A,... and by induction on n; if x,y is a prime ideal of A, and x 0, y E p, then p is a graded prime ideal of A, the prime ideal satisfying the above conditions is unique. The condition of the statement is obviously necessary. If p, = A, for all n 2 no and x, x, y y = x, x, we can assume x, y 0. Conversely, if p is a prime ideal... and (with x, y not in p) E, then p is a graded prime ideal of A and suppose A, is graded ideal of A, and that x, y, z E p. If there exists an integer l such that x 5 p and hence y p E A. To prove that p is prime, it is sufficient to show that, if x E A,, y E A,, and x, y E p, then x E p or y E p. (Proposition 4). Then A, = ah,, x e A, and y = p, - ah,. a.x E p, whence the assertion. The integer n being chosen so that n + a... p, then x p - An, p, x p, then p n p (Proposition 4) by the condition... an element y of A, and there exists a prime ideal p of A, p = 2. (i) For every graded prime ideal p of A, there exists a unique (necessarily essential) gradedprime ideal p of A such that p n A(d)= p'. (ii) If a E A, does not belong to pty and does not belong to Pkd and hence p n A(,) is essential. (iii) For all 2 0, the set p n A, must be equal to the set a, of x E A, such that xd E p". It is then clear that a = is a graded prime ideal; as a, = pk > 0 when is a multiple of d. Let us prove a is a prime ideal. By hypothesis, let x, y be elements of A such that x, y E A and xy E a, then x, y are homogeneous of degree i and j with x, y E, we have xy E a, x E p, y E p Let us first show that, if x ~ y, p' E p': then x d E p or y d E p is a prime ideal of A and hence a is a graded prime ideal of A. Finally, the relation (xy) ~ E, E p' implies x,y E p and p' E p' ; since p is a graded prime ideal of A whose intersection with A(d) is pw d is that which is essential. PROPOSITION 6. Let A be a graded commutative ring with positive degrees and p a prime ideal of A. The set S of homogeneous elements of A not belonging to p is multiplicative and the ring of fractions S-IA is therefore graded commutatively (Chapter 11, § 2, no. 9) (note that there will in general be homogeneous elements # 0 of negative degree in S-'A). (i) Let p' be the ideal S-'p of S-IA consisting of the homogeneous elements of degree 0 ; in other words (with the set of fractions x/s, where s and x are homogeneous of the same degree in A and s E p. Similarly, for every graded A-module M, S-IM is graded canonically (loc. cit.) and we shall denote by M(,,,the subgroup of homogeneous elements of degree 0, which is obviously an A(,, -module. 7. Let p be a gradedprime ideal of A, (a) A(,) of A(,); for every prime ideal p' of A(,) there exist ... let p' be such that ... pA = p. Then every element of ... MCd) = M is bijective. PROPOSITION 6 It is the set of homogeneous elements of A not belonging to p and so = S n A(,). We conclude that xay a, x, x =... homomorphism x - S'-IMcd) +S-IM is a homo- s am+nZt we conclude that axy a,+,+, since xy p. Finally, if n 2 no and x E A,, the conditions x E a and x,+, are equivalent; by induction on n. Finally, if n 2 no and x E A,, the conditions x E a and a,,+, are equivalent by the ...x E A, and x = c e, for n 2 no, then x g p, and the ideal ... 160 3 1.4 GRADED PRIME IDEALS generated some primes 1 ... which completes the proof of the existence of the graded prime ideal p which solves the problem. If also p' is another graded prime ideal of A such that p' n A(d) = p and if x E A, then xd E p' ; hence x is an element of a and a' = p ; hence a = p. Let x be a homogeneous element of degree with x E p. Since p = p' by hypothesis and therefore + 160 3 1.4 GRADED PRIME IDEALS generous homomorphism of degree 0 of A is injective, for if x E M,, satisfies 0 E S,, s E p, then since sdx = 0 and sd E p,x = 0 ; there is also hence also the unique ring a canonical homomorphism of degree 0 of A(d)(= A,,,). it follows from i ; n, (S1)m PROPOSITION 8. Let m 2 1 be a set of numbers... ker A : ... , then ... if x E p... 1 ... 1,2 FILTERED RINGS AND MODULES 1. FILTERED RINGS AND MODULES DEFINITION 1. Let G be a group. A filtration on G is a family of subsets of G such that a decreasing filtration of G such that (i) G, c G, for m = p.; A,, = (G,) filtration, if the family of the G, be a subgroup of G ... an increasing ... filtration if the family of the subgroups (G,) ... filtration on G, we shall call filtered group and denote by (G, G,) ... the filtrations we shall use are decreasing filtrations and we shall say filtration instead of decreasing filtration. Let G be a group, A(G),... other words, the filtered group G (resp. G with a filtration)... 162 ... if G = G,. If G is filtered and its filtration ... Let G be a group with a filtration (G,) and ... Let H be a subgroup of G. Then the family of subgroups (H n G,) is a filtration on H called the induced filtration; if G is filtered group and H a normal subgroup, the image of (G,) in G/H is a filtration called the quotient filtration; G/H is then called a filtered quotient group of G. Let (G,) be a filtered group, E a set, f : E -+ G, then (f-'(G,)) ... is a filtration on E, the inverse image filtration. Let A be a ring; a filtration (A,) on A is called compatible with its ring structure if A,A, c A,+, for all m, n; A is then called a filtered ring. Let M be an A-module; a filtration (M,) on M is called compatible with the module structure (with the filtration on A) if A,M, c M,+, for all m, n; M is then called a filtered A-module. Let A be a filtered ring and M a filtered A-module ... Example 1) Let A be a ring, m an ideal of A. The family (m^n) n E Z, with m^n = A for n < 0, is a filtration on A compatible with its ring structure, called the m-adic filtration on A. If M is an A-module, the family (m^n M) is a filtration on M compatible with its module structure, called the m-adic filtration on M. ... Let A be a filtered ring, M a filtered A-module, N a submodule of M; the induced filtration on N and the quotient filtration on M/N are compatible with the module structures. 2) ... Let A be a ring and u : E -+ F a homomorphism of filtered A-modules ... compatible with the filtrations if u(E,) c F, for all n. ... 3) ... Example 4) Let g be a Lie algebra over a commutative ring K and U its enveloping algebra ... the increasing filtration (U,) ... 5) ... Let G be a group with a filtration (G,) compatible with its group structure. When is it exhaustive if G = U G,, separated if n G, = {e}, ... THE GRADED MODULE ASSOCIATED WITH A FILTERED MODULE 2. ... Let G be a commutative group with a filtration (G,). For all n E Z, we write gr,(G) = G,/G,+1; the group gr(G) = @ gr,(G) is called the graded group associated with the filtered group G. ... Let A be a filtered ring, (A,) its filtration; the bilinear mappings (x, y) -+ xy of A, x A, into A,+, define by passing to the quotients mappings gr,(A) x gr,(A) -+ gr,+,(A), whence a multiplication on gr(A) making gr(A) a graded ring, called the graded ring associated with the filtered ring A. Similarly, if M is a filtered A-module, gr(M) is a graded gr(A)-module, called the graded module associated with the filtered module M. ... Example 1) Let A be a ring with the m-adic filtration; gr(A) = @ m^n/m^(n+1); ... Let k be a field and A = k[X1, ..., Xn] ... Example 2) ... Let A be a filtered ring, M, N filtered A-modules and u : M -+ N a homomorphism compatible with the filtrations. Then u(M,) c N, and by passing to quotients we obtain homomorphisms gr,(u) : gr,(M) -+ gr,(N) and hence a homomorphism gr(u) : gr(M) -+ gr(N) of graded gr(A)-modules, called the homomorphism associated with u. ... PROPOSITION 1. Let A be a filtered ring, E a filtered A-module, F a submodule of E with the induced filtration and E/F with the quotient filtration; then the sequence 0 -+ gr(F) -+ gr(E) -+ gr(E/F) -+ 0 is exact. ... strict morphism ... A homomorphism u : E -+ F of filtered modules is called strict if u(E,) = u(E) n F, for all n ... PROPOSITION 2. Let E -+ F -+ G be an exact sequence of strict morphisms; then gr(E) -+ gr(F) -+ gr(G) is exact. ... 3. THE TOPOLOGY DEFINED BY A FILTRATION Let G be a group with a filtration (G,) consisting of subgroups... There is a unique topology on G compatible with its group structure for which the G, form a fundamental system of neighbourhoods of e; it is called the topology defined by the filtration (G,). ... This topology is Hausdorff if and only if the filtration is separated ... The closure of a subgroup H is n HG, ... PROPOSITION 3. Let A be a filtered ring and E a filtered A-module ... the topology on E defined by the filtration is compatible with the module structure ... a topological ring ... m-adic topology ... the m-adic topology ... 4. ... Let A be a ring, m an ideal of A ... PROPOSITION 4. ... Let G be a filtered group; the topology defined by its filtration is discrete if and only if there is an n with G, = {e}; ... Cauchy sequence ... complete ... 5. THE TOPOLOGY DEFINED BY A FILTRATION ... LEMMA ... Let G be a topological group whose filtration (G,) consists of normal subgroups, and suppose that G is complete and Hausdorff ... PROPOSITION 5. ... the mapping ... PROPOSITION 6. ... PROPOSITION 7. Let A be a ring, m an ideal of A, E an A-module ... Artin–Rees ... E an A-module whose m-adic filtration ...

is sufficient then to take x, to be an element of W;,, and the construction of (x,) can PEN then be performed by induction. + n PROPOSITION 8. Suppose that A and E satisfu the hypotkeses ofProposition 7. Let (F,) be a decreasing sequence o f closed submodules o f E such that F, = 0. Then,for every neighbourhood V of0 in E, there existsp such that F, c V (in other words, the base of the filter (F,) converges to 0). n We may assume that V is one of the En,in which case E/V is Artinian. Let US write F; = (F, V)/V; as the F; form a decreasing sequence of submodules of E/V, there exists an integerj such that FL = F; for all p > j. We shall see that F; = {0}, which will complete the proof. Let x E F; and let W, be the set of elements of F, whose image in E/V is x (p 2 j) ; by definition of j, the W, are non-empty closed affine subsets of E and obviously W,+l c W,; + 176 THE LIFT OF HOMOMORPHISMS OF ASSOCIATED GRADED MODULES 3 2.8 then it follows from Proposition 7 that there exists an element y belonging to all the W,. As W, c F, and F, = {0}, y = 0 ; since x is the canonical image ofy in E/V, x = 0 (cf. Exercises 15 to 21). ,cN 8. THE LIFT OF HOMOMORPHISMS OF ASSOCIATED GRADED MODULES THEOREM 1. Let X, Y be twojltered groups whosejltrations (X,), (Y,) consist of normal subgroups; let u : X 4 Y be a homomorphism compatible with thejiltrations. (i) Suppose that thejltration (X,) is exhaustive. For gr(u) to be injective, it is necessary and that-ul(Y,) = X,for all n E Z. (ii) Suppose that one of the following hypotheses holds: (u) X is complete and Y Hausdorff; (p) Y is discrete. Then, f o r gr (u) to be surjective, it is necessary and su$cient that Y, = u(X,) for all n E Z. (i) To say that the mapping gr,(u) is injective means that Xn n-i (yn+ 1) c This is obviously the case of;' xn + 1' (Y,+l) = X,,,. Conversely, if for all n, we deduce by induction on k that Xn-k n i l (Y n + 'c) x,+1for all n E Z and all k 0. As the filtration (X,) is exhaustive, we see that, for all n, X is the union of the Xn-, (k 2 0), hence-u'(Y,+,) c X,+, for all n and there- ' fore X,+ c i'(Y, + 1) , which completes the proof. (ii) To say that the mapping gr,(u) is surjective means that Yn = u (Xn)Yn + P This is obviously the case if Y, = u(X,). Conversely, suppose that y,,= U(X,)Y,+~for all n E Z. Let n be a n integer and y an element of Y,; we shall define a sequence (x,),,, of elements of X, such that x k E &, x k + l = x, (mod. X,,,) and u(x,) = y (mod. Yn+,) for all k 2 0. We shall take xo equal to the identity element of X, which certainly gives u(x0) = y (mod. Y,). Suppose that a n x, E X, has been constructed such that u (x k) EZ y (mod. Yn+k);then (u(x,))-'y E Yn+,; the hypothesis implies that there exists tEx+k such that u (t) = (u(x,))-'y (mod. Y,+k+,) and hence u(xkt) = y (mod. Y,+k+l) ; it is sufficient to take x , + ~= x,t to carry out the induction. This being so, if Y is discrete, there exists k 2 0 such that Y,+k= {e'} (the identity element of Y), whence u(x,) = y and hence in this case it has been Proved that u(X,) = Y, for all n. Suppose now that X is complete and Y Hausdorff. As x i lxk E X, + for h 2 k > 0, (xk) is a Cauchy sequence in X; as 177 111 GRADUATIONS, FILTRATIONS AND TOPOLOGIES X, is closed in X and hence complete, this sequence has a t least one limit x in X,. By virtue of the continuity of u, u (x) is the unique limit of the sequence (u (x k)) in Y, Y being Hausdorff. But the relations u (x J = y (mod. Y,,,,,) show that y is also a limit of this sequence, whence u (x) = y and it has also been proved that u(X,) = Y,. COROLLARY 1. Suppose that X is Hausdorff and its jiltration exhaustive. Then, fi ~ (u is) injective, u is injective. Let e, e' be the identity elements of X and Y respectively. Then LIFT OF FAMILIES OF ELEMENTS OF AN ASSOCIATED GRADED MODULE is commutative. As gro(A) = A/m is a field, the hypothesis implies that 1 @ gro(u) is injective; as by hypothesis yMis injective, so is yM (1 @ gro(u)). This implies first that yN is injective and hence bijective and therefore that 0 gr(u) is injective. The formula >l(rnnM) = mnN is then a consequence of Theorem 1 (i). Also, let us write N' = u(N) and letj: N' --f M be the canonical injection. I f p : M --f P = M/N' is the canonical homomorphism, then in the commutative diagram g m COROLLARY 2. Suppose that one o f the following hypotheses holds : (a) X is complete, Y is Hausdorfand itsjiltration is exhaustive; (p) Y is discrete and itsjiltration is exhaustive. Then, ifgr(u) is surjective, u is surjective. In this case Y = Y, = u(X,) c u (X) . v v @ gro(") 163 gro(i) ------+ g w @ gr,(M) 1 8 FO(P) _ _ _ f YN.1 by hypothesis, whence the corollary. COROLLARY 3. Suppose that X and Y are Hausdorf, thejltrations of X and Y exhaustive and X complete. Then, ifgr(u) is bijective, u is bijective. Let A be a local ring, rn its maximal ideal and M an A-module; let A and M be given the m-adic filtrations and let gr(A) and gr(M) be the graded ring and the graded gr(A)-module associated with A and M. We have seen (no. 3, Example 3) that the canonical mapping (1 1) is always surjective; we are going to consider the following property of M: (GR) The canonical mapping 9 2.9 g V) gr(i) d P) gr(A) @ g r o w -+ 0 -i - gr(P) 0 the lower row is exact (no. 4,Proposition 2) and so is the upper row by virtue of Proposition 2 of no. 4 and the fact that gr,(A) is a field. Moreover, g r (j) is injective (no. 4, Proposition 2) and hence gr,(j) is injective, The first part of the argument applied to j shows that yNris bijective; as yMis also bijective by hypothesis, we conclude that yp is bijective (Chapter I, 4 1, no. 4,Corollary 2 to Proposition 2). COROLLARY. Under the hypotheses of Proposition 9, ;f we assume also that N is Hausdorf with the m-adicjiltration, then u is injective. This follows from the fact that gr(u) is injective (Corollary 1 to Theorem 1). PROPOSITION 9. Let A be a local ring, m its maximal ideal, M, N two A-modules and * Remark. Suppose that the hypotheses of Proposition 9 hold and also one of the following conditions : (1) rn is nilpotent; (2) A is Noetherian and P is ideally Hausdorff (cf. 9 5 , no. 1) ; then P is aflat A-module. This follows from the fact that y p is bijective and 9 5 , no. 2, Theorem 1 (iv), since A/m is a field. * u : N -+ M an A-homomorphism. M and N are given the rn-adicjiltrations and suppose that: (1) M sathjiesproperty (GR) ; (2) gr,(u) : gr,(N) --f gr,(M) is injective. Then 9. THE LIFT OF FAMILIES OF ELEMENTS OF AN ASSOCIATED GRADED YM: is bijective. gr(A) @gro(A) grO(M) --f gr(M) gr(u) : gr(N) --f gr(M) is injective, N and P = Coker(u) sathfiproperty (GR) and m"N = -h'(rnnM) for every integer n > 0. I t is immediately verified that the diagram gr(A) @gro(A) grO(N) 1Q g d u) _ _ _ f gr(A) @pro(A) grO(M) I 178 MODULE Let A be a filtered commutative ring, (A,Jnez its filtration and C a subring of A, such that C n A, = (0). The restriction to C of the canonical mapping A. +Ao/A, = gro(A) is then injective, which allows us to identify C with a nubmodule of gro(A); this is what we shall usually do in similar cases. If Al # A, and K is any subjield of A,, then K n A, = (0) since K n A, is an ideal of K not containing 1; then K may be identified with a subfield of gro (A). ~ O P O S I T I O N10. Let A be ajltered commutative ring and (A,) itsjltration; suppose 179 I11 LIFT OF FAMILIES OF ELEMENTS OF AN ASSOCIATED GRADED MODULE GRADUATIONS, FILTRATIONS AND TOPOLOGIES 3 2.9 is dense in A"; moreover the homomorphism u defined in the proof of Proposition 10 is continuous on A' and can be extended uniquely to a continuous homomorphism v: A +-A, since A is Hausdorff and complete (General Topology, Chapter 111, fj 3, no. 3, Proposition 5), which proves (i); also, gr(A") = gr(A') and gr(v) = gr(u); (ii) and (iii) then follow respectively from Corollaries 1 and 2 to Theorem 1 of no. 8 in view of the hypotheses on A. that there exists a subring C of& such that C n A, = (0) and C is identijied with a subring ofgr,(A). Let (x i) ,be ajnitefamily ofelements $A; suppose that xi E A,, for 1 < i < q and let 5, be the class o f xi in gr,,(A) for 1 < i < q. (i) I f t h e family (ti)of elements of gr(A) is algebraically free over C , the family (xI) is algebraically free over C. (ii) Ifthejiltration on A is exhaustive and discrete and (t i)is a system o f generators o f the C-algebra gr(A), then (xi) is a system ofgenerators ofthe C-algebra A. , The conclusion of (ii) (resp. (iii)) of the proposition is sometimes expressed by saying that the family (x,) is formally free over C (resp. a formal system of generators of A). Let A' be the polynomial algebra C[X,, . . ., X,] over C; let A' be given the graduation (A;) of type Z where A, is the set of C-linear combinations of P 2 the monomials X?l'. . such that ,=I nts(i) = n. Let u be the homomorphismf ++f (q, . . .,x,) from the C-algebra A' to the C-algebra A; by definition, u(&) c A,, for all n E Z and hence u is compatible with the filtrations (A' being given its filtered ring structure associated with its graded ring structure, cf. no. 1, Example 1). This being so, the hypothesis of (i) means that PROPOSITION 12. Let A be ajiltered ring, E ajiltered A-module and (A,,) and (E n) I gr(u) : A' = gr(A') + gr(A) In the A-module L = A', let L, denote the set (ai) such that a, E A,-,,(,) for all i E I ; q are the least and greatest of the n (i) , then A:-, 2 L, 2 A:-p and the topology defined on L by the definition (L,,) is the same as the product topology; hence L is a complete filtered A-module. As L is free, there exists an is injective; as the filtration on A' is exhaustive and separated, Corollary 1 to Theorem 1 of no. 8 may be applied and u is injective, which proves the conclusion of (i). Similarly, the hypothesis (ii) on the (&) means that gr(u) is surjective; as A is discrete and its filtration is exhaustive, Corollary 2 to Theorem 1 of no. 8 may be applied and u is surjective, which proves the conclusion of (ii) 2 . PROPOSITION 1 1. Let A be a complete Hausdorffjltered commutative ring, C a subring of A, such that C n A, = 0 and ajnite family of elements of A such that X I E A,, where n, > 0for 1 < i < q; let El be the class ofx, in gr,,(A) for 1 < i < q. (i) There exists a unique C-homomorphism v from the algebra of formal power series A" = C[[X,, . . ., X,]] to A such that v(X,) = x, f o r 1 < i < q. (ii) I f t h efamily (El) is algebraically free over C , the homomorphism v is injective. (iii) If thejltration on A is exhaustive and thefamily (ti)is a system of generators of the C-algebra gr(A), the homomorphism v is surjective. 5 2 < 5 As ni 2 1 for all i, , = 1 njs(i) 2 e i= 1 s (i) for every monomial X;(". . .Xp' and on the other hand nis(i) r . i = 1 s (i) if r is the greatest of the n,. If A: denotes the set of formal power series whose non-zero terms aJC;('). . .X:(@ 5 satisfy nis(i) 2 n, it follows from no. 6, Corollary to Proposition 6 that A" i=l is Hausdorff and complete with the exhaustive filtration (A;) and that A' = C[X,, 180 . . ., X,] the respectivejltrations on A and E. Suppose that A is complete and the Jiltration (En) is exhaustive and separated. Let (xi)1EIbe ajnite family o f elements o f E and for i E I let n (i) be an integer such that xi E Eno);jinallylet ti be the class of xi in gr,,(,)(E).Then, fi (E,) is a system of generators oj' the gr (A)-module gr (E) , (x l) is a system ofgenerators of the A-module E. I a,x, and it is obviously A-linear mapping u : L + E such that u ((a i)) = compatible with the filtrations; we must prove that u is surjective and for this it is sufficient, by virtue of Corollary 2 to Theorem 1, no. 8, to show that gr(u) :gr(L) -+ gr(E) is surjective or also that, for all XEE,, there exist a family (a,) such that 2 a, E for all i E I and x = (€1 aixi (mod. En+,). Let t be the class of x in gr,(E); since the 4, generate the gr(A)-module gr(E), there exist ai E gr(A) c such that t = at& and we may assume that xi E gr,-ncr,(A)by replacing if ,€I need be ai by its homogeneous component of degree n - n (i) . Then a,is the image of an element a, E A,,-ncr,and the family (a,) has the required property. COROLLARY 1. Let A be a complete filtered ring and E a jiltered A-module whose Jltration is exhaustive and separated. If gr(E) is a jnitely generated (resp. Noetherian) e (A) -module, then E is a jinitely generated (resp. Noetherian) A-module. If gr(E) is finitely generated, there is a finite system of homogeneous generators and Proposition 12 shows that E is finitely generated. Suppose now that @(E) is Noetherian and let F be a submodule of E ; the filtration induced on F by that on E is exhaustive and separated and gr(F) is identified with a 181 APPLICATION GRADUATIONS, FILTRATIONS AND TOPOLOGIES 111 sub-gr(A)-module of gr(E) (no. 4, Proposition 2) and hence is finitely generated by hypothesis; we conclude that F is a finitely generated A-module and hence E is Noetherian. COROLLARY 2. Let A be a complete Hausdorffjltered ring whosejltration is exhaustive. Ifgr(A) is a lejit Noetherian ring, so is A. I t is sufficient to apply Corollary 1 with E = A,. COROLLARY 3. Let A be a completejltered ring, (A,) its filtration, E a Hausdorff filtered A-module, (En) its filtration and F ajnitely generated siibmodule of E ; suppose that A, = A and E, = E. (i) f o r all k > 0, E, = Ek+l AkF, then F = E. (ii) I f i t isfurther supposed that thefiltration on E is deriuedfrom that on A (no. 1, Example 2), the relation E = El F implies F = E. u, + + Let Ei (1 < i < n) be the classes mod. El of a finite system of generators of F. I t follows from the given hypothesis that for all k > 0 every element of gr,(E) 2 can be expressed in the form i= aIE,, where xi E gr(A) ; the ti therefore generate the gr(A)-module gr(E), which proves (i) by virtue of Proposition 12. If the filtration on E is derived from that on A, the relation E = El + F implies E, = AkE = AkE, + AkF = AkA,E + AkF C A,L+lE+ A,F = Ek+, + A,F c E,L, whence (ii). PROPOSITION 13. Let A be a ring, m a two-sided ideal ofA contained in the Jacobson radical of A and E an A-module. Let A and E be given the m-adicjltrations (no. 1, Example 3). Suppose that one of the following conditions holdr : (a) E is afinitely generated A-module and A is Hausdorf; (b) m is nilpotent. For E to be afree A-module, it is necessary and su8cient that E/mE be a free (Aim)module and that E satisjy property (GR) (no. 8). If E is a free A-module and (eh) a basis of E, mkE is the direct sum of the submodules mkeh of E for all k > 0 (Algebra, Chapter 11, § 3, no. 7, Remark); then mkE/mk IE is identified with the direct sum of the mkeh/mk leh (Algebra, Chapter 11, 3 1, no. 6, Proposition 7). We deduce first (for k = 0) that the E form a basis of the (Aim)classes 1 @ eh of the eh in E/mE = (A/m) module E/mE, since the canonical mapping + + (mk/mk+I) @A (E/mE) -+ mkE/mk+lE is bijective for all k 2 0; hence yE is bijective. Note that this part of the proof uses neither condition (a) nor condition (b). 182 : EXAMPLES OF NOETHERIAN RINGS 8 2.10 Suppose conversely that the conditions of the statement hold and let a family of elements of E whose classes mod. mE form a basis of (jJLEI its canonical the (A/m)-module E/mE; let L be the free A-module basis and u : L -+ E the A-linear mapping such that u (j J = x, for all t E I. The hypotheses already imply that u is surjective (Chapter 11, 9 3, no. 2, Corollary 1 to Proposition 4) and it remains to prove that u is injective. Now, each of the hypotheses (a) and (b) implies that A is Hausdorff and hence so is L with the m-adic filtration, since mkL = (mk)(I) (Algebra, Chapter 11, 9 3, no. (L/mL) from the first part 7, Remark) and gr(L) is identified with gr(A) of the proof; the homomorphism u is compatible with the filtrations and it is possible to write gr(u) = yE u where u is the bijection of gr(L) onto (X J , ~be ~ 0 gr(A) @Ah (E/mE) mapping the class off, mod. mM onto 1 @ ?Z,, where ?Z, is the class of x, mod. mE. The hypothesis then implies that gr(u) is injective and the conclusion follows with the aid of Corollary 1 to Theorem 1, no. 8. 10. APPLICATION: EXAMPLES OF NOETHERIAN RINGS LEMMA 1. Let A be a graded r i y of type Z, whose gradualion (A,) is such that A, = 0 for all n < 0 or A, = 0 for all n > 0. Let M be a graded A-module of type Z. For M to be a Noetherian A-module, it is necessary and suficient that every graded submodule of M be finitely .Cenerated. As n H -n is an automorphism of the group Z, we may restrict our attention to the case A, = 0 for all n > 0. Let A' and M' denote the ring A and the module M with the filtrations associated with their respective graduations (no. 1, Example l), which are exhaustive and separated; the hypothesis on A implies that A' is discrete and hence complete. If E is a sub-A-module of M, the filtered A-module E' obtained by giving E the induced filtration is Hausdorff and its filtration is exhaustive; moreover gr(E') is identified with a graded sub-A-module of M = gr(M') and hence is finitely generated by hypothesis. The conclusion then follows from Corollary 1 to Proposition 12 of no. 9. THEOREM 2. Let A be a graded ring of type N,M a graded A-module o f type N and (4)and (M,) their reqkctiue graduations. Suppose that there exists an element a E A, that A, = AOanand M, = anMO f o r all n > 0. Then, fi M, is a Noetherian A,-module, M is a Noetherian A-module. By virtue of Lemma 1 it is sufficient to prove that every graded submodule N of M is finitely generated. For all r 2 0, let N, = N n M, and let L, be the set of m E M, such that arm E N,. As aTA, c A, = Aoar, a'A,L, c A,a'L, c A,N, c N, 183 I11 COMPLETE TII-ADIC RINGS AND INVERSE LIMITS GRADUATIONS, FILTRATIONS AND TOPOLOGIES the ring gr(A) is Noetherian by Corollary 3. From this we deduce that A itself is Noetherian (no. 9, Corollary 2 to Proposition 12). and hence the L, are sub-A,-modules of M,; moreover, aN, c N n a M , = N n M,+, = N,+, and hence the sequence (L,),20 is increasing. The hypothesis implies that there exists an integer n 0 such that L, = L, for r 2 n. For each r < n, let (m,,s)l cs 0, the ring of formal power series C[[X,, . . .,X,]] is Noetherian. This follows from Corollary 5 and no. 6, Corollary to Proposition 6, for if m is the ideal of A = C[[X,, . . .,X,]] consisting of the formal power series with no constant term, A/m is isomorphic to C and m/m2 to the C-module C". Remarks (1) Corollaries 2, 3 and 6 apply in particular if C is a commutativefield. ki c Jl Aoarmrs, * (2) Let g be a Lie algebra over a commutative Noetherian ring C and suppose that g is a finitely generated C-module. Let the enveloping algebra U ofg be given the increasing filtration (U,) defined in no. 3, Example 4. With the corresponding topology, U is discrete and hence Hausdorff and complete; the associated graded ring gr(U) is a finitely generated C-algebra, being a quotient of the symmetric algebra S(g), hence gr(U) is a Noetherian ring (Corollary 3) and we deduce that U is a left and right Noetherian ring (no. 9, Corollary 2 to Proposition 12). * ,zl zl en kn Aoarm,,, C A,ar-". (anm,,,) which completes the proof (cf. Exercise 10). COROLLARY 1 (Hilbert's Theorem). For every commutative Noetherian ring C, the polynomial ring C[X] is Noetherian (cf. Exercise 10). 11. COMPLETE m-ADIC RINGS AND INVERSE LIMITS COROLLARY 2. For every commutative Noetherian ring C and every integer n > 0, the polynomial ring C[X,, . . ., X,,] is Noetherian. This follows from Corollary 1 by induction on n. , I COROLLARY 3. If C is a commutative Noetherian ring, every jinitely generated commutative C-algebra is a Noetherian ring. We have seen in no. 6 that, if A is a commutative ring and m an ideal of A such that A is Hausdorff and complete with the m-adic topology, then the topological ring A is canonically identified with the inverse limit of the discrete rings A, = A / m i f l (i E N) with respect to the canonical mappings h,j:A/mj+l-tA/mi+l (i G j) ; Such an algebra is isomorphic to a quotient of a polynomial algebra C[X,, . . ., X,,] (§ 1, no. 1). note that hi, is surjective and that, if nu is its kernel, then nu = m'+l/mf+' = (m/ml+l11+1 = COROLLARY 4. Let A be a graded commutative ring of type N and let (A,,) be its graduation. For A to be Noetherian, it is necessary and suj'icient that A, be Noetherian and that A be ajinitely generated A,-algebra. in particular (n,,)jj+l = 0. Conversely: The condition is sufficient by Corollary 3. Conversely, suppose A is Noethe- 2 rian; m = n a 1 A,, which is an ideal of A, is then finitely generated; then A is a finitely generated A,-algebra (3 1, no. 2, Corollary to Proposition 1); on the other hand A,, which is isomorphic to A/m, is a Noetherian ring. COROLLARY 5. Let A be a commutative ring and m an ideal ofA such that A/m is Noetherian, m/m2 is a jinitely generated (A/m)-module and A is Hausdorff and complete with the m-adic topology. Then gr(A) and A are Noetherian. gr(A) is an (A/m)-module generated by m/m2 (no. 3, Example 3) and hence 184 fj 2.1 1 I I PROPOSITION 14. Let (A,,hi,) be an inverse system of discrete commutative rings, whose indexing set is N and let (Mi, u,,) be an inverse system of modules over the inverse system ofrings (4,h,,). Let n, denote the kernel ofh,, : A, -+ A, and set A = lim A,, c. M = lim M,. Suttose that c (a) for all i E N,h, is the identity mapping on A, and, for i < j , hi, and u,, are surjective; (b) f i r i < j , the kernels ofh,, and uu are n;" and n:+lM, respectively. Then: 1 I (i) A is a complete Hausdorff topological ring, M is a complete Hausdorff topological A-module and the canonical mappings h, : A -+A,, u, : M --f Mi are surjective. (5) If M, is ajinitely generated A,-module, M is a finitely generated A-module; 185 111 GRADUATIONS, FILTRATIONS AND TOPOLOGIES to be precise, every jnite subset S of M such that u,(S) generates M, is a system of generators o f M. Nic m,M' Ni= m,M' The assertions in (i) follow from General Topology, Chapter 11, 3 3, no. 5, Corollary to Proposition 10 and Corollary 1 to Theorem 1. For all i E N, let us write m,+, = Ker(h,), Nt+l = Ker(u,); then sition 12 of no. 9 that M' = M, which completes the proof. -1 c k30 and N,+ = lim n: 1:Mi +k ; t as hi + k and u, k are surjective, We preserve the notation of the proof of Proposition 14; the hypotheses here allow us to assume that the ideal a isjnitely generated. Let i 2 0 be any integer; for a l l j B 0, by (17), N,+,= a'(aiM) N,+,+l c m,(a'M) N,+,tl; conversely, m,(aiM) c m p , M c m,,,M c Ni+,, whence Nit, = m,(a'M) 1(m,N,)= h, +,-1(mt)u1+,- "1 N, = atM' + N,,, + Nl+,+l* As a and M are finitely generated A-modules, so is a'M. Applying Corollary 3 to Proposition 12 of no. 9 to the module N,with the filtration defined by Ni, = N, if j < 0, N,,= N,+,if j 2 0, we obtain N, = aiM, whence N, c m:M. But also m:M c m,M c N,,whence N, = miM. Applying this to the case where M , = A,, u,, = hi,, we obtain m, = m:. Moreover, m, = a + m: by (17), which proves the last assertion of the corollary. is equal to n~+,-l(n~+,-lM,+,-l) = 0, as, for all k 2 0, n:", which is the kernel of hkk,is equal to 0. We see similarly that m,m; c m,,,. If for i < 0 we set m, = A and N, = M, (mt),ez is a filtration of A and (NJtGz a filtration of M compatible with the filtration on A; the topologies on A and M are obviously those defined by these filtrations. This being so, let a be an ideal of A such that hl(a) = n1 and M' the submodule of M generated by S; we are going to prove that (17) + + Let us show that m,N,c N,+,for i 2 1 and j 2 1, which amounts to proving that U,+,-~(~,N,) = 0; now ui +,- + N,+l;on the other hand obviously m,M c N, and hence + Ni+l for all i 2 0; then it follows from Corollary 3 to Propo- COROLLARY 1. With the notation and hypotheses o f Proposition 14 suppose further that M, is ajnitely generated A,-module and that the ideal n1 of A, isjnitely generated. Let rn, be the kernel of h,; the topologies on A and M are then the m,-adic topologies on this ring and this module respectively; to be precise,for all i 2 0, the kernels of h, and ui are m? and m y 'M respectively; further ml/m: is ajnitely generated A-module. m,+, = limhl,,+k(0)= l i m n ,f++ ,k c 4 2.12 T H E HAUSDORFF COMPLETION OF A FILTERED MODULE COROLLARY 2. Under the hypotheses of Corollary 1, f o r A to be Noetherian, it is necessary and suficient that A, be so, for i 2 0. The condition is necessary since A, is isomorphic to a quotient of A; it is sufficient by virtue of no. 10, Corollary 5 to Theorem 2. Let us write a, = h,(a), MI = u,(M'); it is sufficient to show that u,(N,)= M;. 12. THE HAUSDORFF COMPLETION OF A FILTERED MODULE This is true if i = 0, for No = M and M & = M, by hypothesis. If i 2 1, then u,(N,)= n:M, by (16). As h,, is surjective and h,, = h,, hlr, h,, maps the Let G be a filtered group whose filtration (G,) consists of normal subgroups of G ; we have already recalled (no. 6) that the Hausdog completion of the topological group G is canonically identified with the inverse limit lim G/Gn c 0 -1 kernel n, of h,, onto the kernel n1 of h,, and n, = h,,(n,) ;then t h,,(a,) = h,(a) = n1 = M n ,) and, as the kernel of h,, is n f , n, c a, + np and a, c n,, whence nr = a, nf. Moreover u,,(M:) = uO(M')= M, = uot(Mi) and, as Ker(u,,) = n,M,, M, = MI + n,M,; whence + n:M, = (a, + nf)'(MI + ",Mi). -1 Moreover m, = h,(n,), whence a c m, and therefore at c 186 n I Now, a:n:+'-' c n:+' = 0 for 0 < k < i; then it certainly follows that u,(N,) = n,M, = a:M:, which proves (17). mi c mi, whence of the discrete groups G/G,, the canonical homomorphism i: G -+G having image the Hausdorff group associated with G (everywhere dense in G) and of the subkernel the closure G, of (0) in G. The Hausdorff completion SOUP G, of G is identified with the closure of i(G,) in G (General Topology, Chapter 11, 5 3, no. 9, Corollary 1 to Proposition 18) and, since G, is closed in en G, -1 I G, = i -1 (en) = i (en ni(G)). Moreover, the G, form a fundamental system of neighbourhoods of 0 in 6 (G m a l Topology, Chapter 111, $ 3 , no. 4, Proposition 7) and are therefore 187 I11 GRADUATIONS, FILTRATIONS AND TOPOLOGIES normal open subgroups of G (General Topology, Chapter 111, 3 2, no. 3, Proposition 8); the topology on G is defined by the filtration (G,,), which is always separated by definition. As i (G) is dense in G and G,, is open, G = i(G).Gn (19) and similarly (20) = i(Gn-l).G,. (en) We deduce from (18) and (19) that the filtration is exhaustive if and only if (G,) is. The second isomorphism theorem (Algebra, Chapter I, 3 6, no. 13, Theorem 6 (d)) and equations (18), (19) and (20) show that the canonical homomorphisms THE HAUSDORFF COMPLETION OF A FILTERED MODULE Chapter 11, $ 3, no. 7, Proposition 12). Recall also that, for every uniformly continuous mapping$ X --f Y, J' denotes the uniformly continuous mapping from 2 to P such thatJ'oj, = j , 0 f (loc. cit., Proposition 15) ;if X is a uniform subspace of Y andf the canonical injection, 2 is identified with a uniform subspace of P andfis the canonical injection of X into P (loc. cit., no. 9. Corollary 1 to Proposition 18). LEMMA 2. Let X Y 5 Z be an exact sequence o f strict morphisms o f topological groups (Algebra, Chapter 11, $ 1, no. 4, Remark). Suppose that X, Y, Z admit Hausdorf completion groups and that the identity elements o f X, Y,Z admit countable fundamental systems o f neighbourhoods. Then 2 --f i 9f . 2 is an exact sequence of strict morphisms. Let N,, N, be the respective kernels off and g ; let us write Gn - 1/Gn+ Gn - 1 / G n , G/Gn + G/Gn, (21) are bijective and hence so is the canonical homomorphism (22) gr(G) gr(G). Now let A be a filtered ring, E a filtered A-module and (A,) and (En)the respective filtrations of A and E; we shall assume that these filtrations are exhaustive so that for the corresponding topologies A is a topological ring and E a topological A-module (no. 5, Proposition 3). Then we have defined ral Topology, Chapter 111, $6, nos. 5 and 6) A as a topological ring and topological &module. If i: A --f A is the canonical homomorphism, then i(A,,,)i(A,,) c i(Am+,),whence by the continuity of multiplication in A, + A,A, c A,+, since A,, is the closure of i (A,) in A. It can be similarly shown that (23) (24) in other words: Amfin c Ern+,; PROPOSITION 15. Let A be a jltered ring and E a jltered A-module, the respective filtrations (A,), (En)o f A and E being exhaustive. Then (A,) is a filtration compatible with the ring structure on A and (I?,) ajltration compatible with the module structure on over thefiltered ring A; moreover thesejiltrations are exhaustive and define respectively the topologies on A and Finally, the canonical mappings gr(A) -+ gr(A) and gr(E)--f gr(I?) of graded Z-modules are respectively a graded ring isomorphism and a graded gr(A)-module isomorphism. e e. I n what follows, for every uniform space X, jx will denote the canonical mapping from X to its Hausdorff completion fi and X, = jx(X) the uniform subspace of s, which is the HausdorE space associated with X. Recall that the topology on X is the inverse image under jxof that on Xo(General Topolosy, 188 3 2.12 f =f 3 o f 2 o f i where flis the canonical mapping X -+ X/N,, f2is an isomorphism of X/N, onto N, and f3is the canonical injection N, -+ Y. We already know that f2 is an isomorphism of (X/N,) onto N, and we have just recalled that f3 is an injective strict morphism of N, to 9 ;if we show thatfl is a surjective strict morphism, it will follow that! is a strict morphism (General Topology, Chapter 111, 5 2, no. 8, Remark 2). Let g1 be the canonical mapping Y -+ Y/N,; if we show that i1 is a surjective strict morphism of the kernel A,, we shall see as 2 will be exact. above that is a strict morphism and the sequence Thus we have reduced the problem to proving that, if Y = X/N (where N is a normal subgroup of X) a n d 3 X --f Y is the canonical mapping,fis a surjective strict morphism with kernel R. Letf,: X, -+ Yo be the mapping which coincides withfon X,; as& (resp. j,) is a surjective strict morphism of X onto X, (resp. Y onto Y o) , f ois a surjective strict morphism (General Topology, Chapter 111, 3 2, no. 8, Remark 3). NOWX, and Y o are metrizable (General Topology, Chapter IX, $ 3, no. 1, Proposition 1); then it follows from General Topology, Chapter IX, 4 3, no. 1, Corollary 1 to Proposition 4 and Lemma 1, thatfo = f i s a surjective strict morphism and has kernel the closure f i b in X of the kernel Nb of fo.Then it will be sufficient for us to prove that f i b = &. Now Nb obviously contains NO= jx(N); it will be sufficient to show that Nb is contained in the closure NOof No in X. Now, u = jx(xo - N,>= x -~JN,) -1 is an open set in X which does not meet N ; asf is a surjective strict morphism, v =f(U) is an open set in Y not containing the identity element e' of Y and hence not meeting the closure of e'; thenj,(V) does not contain the identity 189 111 THE HAUSDORFF COMPLETION OF A FILTERED MODULE GRADUATIONS, FILTRATIONS AND TOPOLOGIES element of Yo. But j,(V) = fo(Xo plete the proof of Lemma 2. - No) and hence Nb c No, which com- PROPOSITION 16. Let A be afiltered ring, (A,) itsfiltration, E an A-module and (En) thejiltration on E derivedfrom that on A consisting ofthe En = A,E. Suppose that the filtration (A,) is exhaustive and the module E isfinitely generated. I f ; : E -+ fi is the canonical mapping, then,for all n E Z, (25) 8, = A,8 = &i(E) and fi = A.i(E). In particular fi is a finitely generated &module. The equation A,E = En implies, by virtue of the continuity of the external law on the A-module 8, A,$ c 8, and obviously A,,8 3 A,; (E) .By hypothesis there exists a surjective homomorphism u : L --f E , where L = Af, I being a finite set; let L be given the product filtration, consisting of the L, = A:, which define on L the product topology; then f, = A: and L ,= A; (General Topology, Chapter 11,s 3, no. 9, Corollary 2 to Proposition 18).Letj: L --f f, be the canonical mapping and (e ,) , , , the canonical basis of L ; for an element 2 aij(e,) (where a, (€1 E A for all i E I) to belong to en,it is necessary and suffi- cient that a, E An for all i ; then f,,, = &.j(L). This being so, by definition u(Ln) = AnE = En and hence u is a strict morphism of L onto E (General To ology, Chapter 111, $ 2, no. 8, Proposition 24). Lemma 2 then shows that li: -+ I? is a surjective strict morphism. As f,, is an open subgroup off,, d(f,,) is an open (and therefore closed) subgroup of E; but ti(f&) = &ti(j(L)) = A,i(E) and, as i (E n) c A,i(E) c & i (E) , finally 8, c A,i(E) c An& c fin and therefore = A n i (E) ;setting n = 0, we obtain the second formula of (25). = k en COROLLARY 1. Under the conditions ofProPosition 16, ifA is complete, so is E. AS the canonical mapping A -+ A is then surjective (no. 6, Proposition 5), fi = i (E) by (25) and the conclusion follows by Proposition 5 of no. 6. COROLLARY 2. Let A be a commutative ring, m afinitely generated ideal ofA and A the A Hausdorffcompletion ofA with respect to the m-adic topology. Then mn = (m)" for every integer n > 0 and the topology on A is the th-adic topology. = mn.A Let us write A, = mn, which is a finitely generated ideal of A. The formula mpA, = m n + pshows that the topology induced on A, by the m-adic topology coincides with the m-adic topology on the A-module A, (no. 1, Example 3). A By Proposition 16 applied to E = A,, A, = A. A,, in other words mn = mn .A. I n particular m = m.A, whence (m)" = (cf. Exercise 12). 190 m".A = A.A, 4 2.12 Examples of Hausdorf completions ojjltered rings (1) Let A be a graded ring of type N and let (A,),aobe its graduation; let it be given the associated filtration which is separated and exhaustive (no. 1, Example 1). The additive group A is canonically identified with a subgroup of B n = A,; if B is given the topology the product of the discrete topologies, the neN topology induced on A is the topology defined by the filtration on A ; also B is a complete topological group and A is dense in B (General Topology, Chapter 111, $ 2 , no. 9, Proposition 25). The additive topological group B is then identified with the completion A of the Hausdorff additive group A and it follows from Proposition 15 that it has a unique ring structure which makes it the completion of the topological ring A. To define multiplication in this ring, 2 note that, if we write A; = l > n A,, the closure in B of the two-sided ideal A; is the set B, of x = (x,) E B such that x, = 0 for i 6 n. Then let x = (xi), y = (y,) be two elements of B and z = (2 ,) their product. Then, for all n > 0, x = x; (mod. B,), y = yk (mod. B,), where xk = (xi)0G14n, yk = (Y ,) ~ ~ ~whence ~,,, z = xkyk (mod. B,). But x i and y i belong to A and it is therefore seen that, for all n E N, In particular, we again obtain the Corollary to Proposition 6 of no. 6 : if C is . . . ,X ,] , with the filtration associated with its usual graduation (by total degree) is canonically identified with the ring of formal power series c[[xl,. . ., X,]] (cf. Algebra, Chapter IV, $ 5, no. 10). * (2) Let K be a complete commutative field with a valuation. The completion of the ring of convergent series in r variables over K is canonically identified with the ring of formal power series K[[X,, . . . , X ,]] . * (3) Let a be a non-zero non-invertible element of a principal ideal domain; the (a)-adic topology on A is also called the a-adic topology; it is Hausdor- for the intersection of the ideals (an) reduces to 0 (Algebra, Chapter VII, 5 1, no. 3). Note that the completion of A with respect to this topology is not necessarily an integral domain (cf. no. 13, Remark 3). The associated graded ring m(A) = gr(A) is canonically isomorphic to (A / a) [X](no.

prime field F,. If Z, is the ring ofp-adic integers (5 2, no. 12, Example 3), the application of Corollary 1 to the polynomial X2 - n shows that n is a square in Z,; for example 7 is a square in Z,. (2) Let A = K[[Y]] be the ring of formal power series in one indeterminate with coefficients in a commutative field K ; with the (Y)-adic topology, the ring A is Hausdorff and complete (8 2, no. 6 , Corollary to Proposition 6) and the mapping f(Y) wf (0) defines by passing to the quotient ring an isomorphism of A/(Y) onto the field K. By Corollary 1, if F(Y, X) is a polynomial in X with coefficientsin A and a is a simple root of F(0, X) in K, there exists a unique formal power seriesf (Y) such that f (0) = a and F(Y,f(Y)) = 0. COROLLARY 2. Let A be a ring and m an ideal of A such that the orderedpair (A, m) satisJies Hensel's conditions. Let r, n be integers such that 0 < r < n and f = (Atl,...,f,) is a system o f n - r elements ofA{X,, . . ., X,}; let Jp-r(X) denote the minor o f M , (X) consisting ofthe columns ofindex jsuch that r + 1< j < n. Let a E An be such that Jp-,(a) is invertible in A and f(a) = 0 (mod. m(n-r)). Then there exists a unique x = (xl, . . .,x,) E An such that x k = a, for 1 < k < r, x = a (mod. mxn) and f(x) = 0. Substituting a, for X, for 1 < k < r in the& (no. 2, Remark 3), we see immediately that we may restrict our attention to the case where r = 0 to prove the corollary. Theorem 1 and Proposition 7 show then that fdefines a bijection of a + m x n onto f(a) + m x n = m x n ; the corollary follows from the fact that 0 E mxn. 224 § 4.6 APPLICATION TO DECOMPOSITIONS OF RINGS COROLLARY 3. With the notation of Corollary 2, let a E An; let us write v = JF-'(a) (not necessarily invertible in A) and suppose that f(a) = 0 (mod. ezmx(n-r)).Then there exist n - r formal power series without constant term (r + 1 < i < n) in A[[X,, . . ., X,]] such that,for all t = (tl, . . .,t,) E m r, + (25) 6(a1 + e2t1, f o r r + 1 < i < n. ., a + e2tr, art1 + e+r+1(t),. . J an + e+n(t)) = 0 (2 6) Let tE m r, let&(X) = X, - a, and let u = (f l , . . .,f,); then JU(a)= and Theorem 2 applied to the system u. With the notation of Theorem 2 it follows from the above definitions that gi(X) = X, for 1 < i < r, whence h,(X) = X, for 1 < i < r ; moreover, if M'EM,(A) is such that M,,(a).M' = el,, M' is of the form For t Replacing y by M ' . z (where z we obtain (26) A (a l = (zl., . .,z,) E m "") in formula (20), + e2z1, . . . , a , + e2z,, a,+, + e h r + l (M ' . z) , . . . , a n +ehn(M'.z)) = e2z1 for 1 < i < n. hj are for r + 1 < j < n. For t E m r whose transform (25) is X (X1 , . . ., X r ,- b r +1,...,* b -bn) for r + 1 < j < n, for r + 1 < i < n (2 6), we obtain relations (25) for all t E m 'f. 6. APPLICATION TO DECOMPOSITIONS OF RINGS Let A be a ring and m an ideal ofA such that the ordered pair (A, m) Sa%tes Hensel's conditions. Let B be the quotient ring A/m and x : A -+ B the canonical homomorphism. For every idempotent c o f B there exists a unique idempotent e of A such that x(e) = c. - M M 2. Let a be such that x (a) = c ; Corollary 1 to Theorem 2 of no. 5 may be applied to the polynomial f(X) = X2 - X in A[X] and the element a E A. Then ? (a) = 2a - 1 and, as x (2 a - 1) = 2c - 1 and (2c - 1)2 = 1 in B, 2c - 1 invertible in B and hence 2a - 1 is invertible in A (8 2, no. 13, Lemma 3). Asf(a) E m, Corollary 1 to Theorem 2 of no. 5 immediately gives the existence and uniqueness of e. PROPOSITION 8. Let A be a ring and m an ideal ofA such that the ordered pair (A, m) Sa%$es Hensel's conditions. Let B be the quotient ring A/m and x : A -+B the canonical homomorphism. 225 STATEMENT OF THE FLATNESS CRITERION Ill (2) Every direct sum of ideally Hausdorff modules is an ideally Hausdorff module, by virtue of the relations homomorphism. If B is the direct composition o f a finite family (b,) I o f ideals, there exists a uniquefamily (a) of ideals of A such that x(a,) = b,for all I E I and A is the direct composition of thefamily (a,). (3) If a is an ideal of A, the subspace N of M induced by the topology on M. If A is Noetherian and 3 an ideal of A contained in the Jacobson radical (b) of A, every finitely generated A-module M is ideally Hausdorff with the 3-adic topology on a @A M isJner than the topology induced on a @A M by the 3-adic topology on M, which is Hausdorff by hypothesis. Let I = c, where c, E B, for all i; the c, are idempotents of B such that c,c, = 0 for i # j . By Lemma 2 there therefore exist idempotents e, of A (i E I) such that x(e,) = c, for all i; as e,e, is an idempotent such that x(e,e,) = cicj = for i # j , e,e, = 0 for i # j (Lemma 2) ; as I - T 3 0 2. STATEMENT OF THE FLATNESS CRITERION Let A be a ring, 3 a two-sided ideal of A, M a left-module and gr(A) and gr(M) the graded ring and graded gr (A)-module associated respectively with the ring A and with the module M with the 3-adic filtrations (9 2, no. 3). We have seen (loc. cit.) that for every integer n 2 0 there is a surjective Zmodule homomorphism Y,,: (3"/3"+')@A,3 (M/3M) + 3"M/3"+lM and a graded homomorphism of degree 0 of graded gr(A)-modules e, is an idempotent such that 1el) = 1 c, = 0, similarly 1 = e;. It follows that A is the direct composition of the ideals a, = e,A and that x(a) = x(e,)B = 6, It remains to show the uniqueness of such a decomposition. Now, suppol ideals such poses that A is the direct composition of another family of ?(xiel) = Ae, = b, for all i; then 1 = el where el E a;, whence, in B , 1 = where x(e') E b,, which implies x(ei) = c,; as ei and e, are idempotents, necessarily ei = e,, (Lemma 2), which completes the proof. gr(A) @gr(A) grO(M) -+ gr(M) whose restriction to gr,(A) @gro(A) gro(M)is yn for all n and which is therefore surjective. YM: Remark. Proposition 8 again gives the structure of a semi-local ring on A which is Hausdorff and complete with the c-adic topology (c the Jacobson radical of A), which has already been obtained as a consequence of 9 2, no. 13, Corollary to Proposition 19. THEOREM 1. Let A be a commutative ring, 3 an ideal of A and M an A-module. Consider thefollowing properties: (i) M is aflat A-module. (ii) Tor:(N, M) = 0for every A-module N annihilated by 3. (iii) M / 3 M is a flat (A/3)-module and the canonical mapping 3 M -+ 3 M is bijective (the latter condition being equivalent to Tort(A/3, M) = 0 by virtue of the relation Tor;(A, M) = 0 and the exact sequence Tor:(A, M) -+ Tor:(A/3, M) -+ 3 @A M -+ M). (iv) M/3M is aJlat (A/3)-module and the canonical homomorphism 5. FLATNESS PROPERTIES OF FILTERED MODULES 1. IDEALLY HAUSDORFF MODULES YM: gr(A) grO(M) -+gr(M) is bijective (property (GR) of 3 2, no. 8). (v) For all n 2 1, M/SnM is aflat (A/3")-module. Then (i) * (ii) o (iii) * (iv) o (v). Iffurther 3 is nilpotent or $A is Noetherian and M is ideally Hausdorff, properties (i), (ii), (iii), (iv) and (v) are equivalent. Remark. If A / 3 is a field (as often happens in applications) the condition "M/BM is a flat (A/3)-module" holds automatically for every A-module M, which simplifies the statement of properties (iii) and (iv) ; moreover, in this case, property (v) is equivalent to saying that M/B"M is a free (A/3")-module for every integer n 2 1 (Chapter 11, $ 3, no. 2, Corollary 2 to Proposition 5). DEFINITION 1. Let A be a commutative ring and 3 an ideal of A. An A-module M is called ideally Hausdorff with respect to 3 (or simply ideally Hausdorff if there is no ambiguity) if, for every finitely generated ideal a o f A, the A-module a @A M is Hausdorff with the 3-adic topology. Putting a = A in this definition, we have already seen that M is necessarily Hausdorff with the 3-adic topology. Examples (1) If A is Noetherian and 3 is contained in the Jacobson radical of A (in other words if A is a Zariski ring with the 3-adic topology), everyjinitely generated A-module is ideally Hausdorff (3 3, no. 3, Proposition 6) . 226 5 5.2 GRADUATIONS, FILTRATIONS AND TOPOLOGIES 5 227 111 PROOF OF T H E FLATNESS CRITERION 5 5.2 GRADUATIONS, FILTRATIONS AND TOPOLOGIES 5 5.3 (A) The implications (i) 3 (ii) 0 (%) The implication (i) 3 (ii) 0 (ii) is immediate (Chapter I, $ 4) . The equivalence (ii) o (iii) is a special case of Chapter I, 3 4,Proposition 2 applied to R = A, s = A/B, F = M, E = N, taking account of the fact that being given an (A/B)-module structure on N is equivalent to being given an A-module structure under which N is annihilated by 3. where we note that (3"/3"+l)@A (M/SM) is canonically identified with (B"/3"+') (M/SM). This diagram is commutative by definition of yn and its rows are exact. If (b) holds, 0, and On+1 are bijective and so therefore is yn by definition of cokernel, hence (b) implies (c). Conversely, assuming that 3 is nilpotent, let us show that (c) implies (b) ;we shall argue by descending induction on n, since 3"@AM -+ 3"M = 0 for n sufficiently large. Suppose then that in diagram (8), y, and 8, are bijective; then so is 8, by virtue of Chapter I, $ 1, no. 4,Corollary 1 to Proposition 2. Remark (1). Condition (ii) is also equivalent to the following: (ii') Tor(N, M) = 0 for every A-module N annihilated by a power of 3. Clearly (ii') implies (ii) Conversely, if (ii) holds, then in particular Tort(8nN/3n+1N,M) = 0 for all n ; from the exact sequence O + 3 n + 1 N + 3 n N + 3"N/3"+lN+O (C) The implication (ii) 3 (iv) If (ii) holds, so does (ii') by Remark 1 ; Proposition 1 then shows that yMis an isomorphism. On the other hand, we already know that (ii) implies (iii) and hence that M/SM is a flat (A/3)-module, which completes the proof that (ii) implies (iv) we derive the exact sequence Remark (2) . Proposition 1 shows that, if 3 is nilpotent, (iv) implies (iii); taking account of Remark 1, we have therefore proved in this case that (i), (ii), (iii) and (iv) are equivalent. 3. PROOF OF THE FLATNESS CRITERION . . Torf(gn+lN, M) -+Tort(SnN, M) -+Tort(3nN/3n+1N,M) and, as there exists an integer n such that 9"N = 0, we deduce by descending induction on n that Tort(3"N, M) = 0for all n < m and in particular for n = 0. I t follows from this that if 9 is nilpotent, (ii) implies (i), for (ii') then means that Tor!(N, M) = 0 for every A-module N and hence that M is flat (Chapter I, $ 4). (E) Let us prove the following proposition: PROPOSITION 1. Let A be a commutative ring, 3 an ideal of A and M an A-module. Thefollowing conditions are equivalent: (a) For all n > 1, Tort(A/S", M) = 0. (b) For all n 3 1, the canonical homomorphism On: 3" @A M + 3"M is bijective. Moreover these conditions imply : (c) The canonical homomorphism yM: gr (A) @gr(A) gr,(M) -+ gr (M) is bijective. Conversely, ;f 8 is nilpotent, (c) implies (a) and (b). The equivalence of (a) and (b) follows from the exact sequence 0 = Tort(A, M) -+Tor:(A/Sn, M) + 8" @A M -+ M. (D) The equivalence (iv) o (v) For all n > 1, M / V M has a canonical (A/S")-module structure. If it is filtered by the (8/gn)-adicfiltration, it is immediate that grm(M/3"M)= grm(M)if m < n and gr,,,(M/BnM) = 0 if m 2 n. For all k 2 1, let A, = A/gk, 3, = 3 / g k M, = M/gkM; let (iv), (resp. (v),) denote the assertion derived from (iv) (resp. (v)) by replacing A, 3, M by A,, 3,, M,. It follows from what has just been said that (iv) is equivalent to "for all k 2 1, (iv)k" and obviously (v) is equivalent to "for all k 2 1, (v)-".Then it will sufficeto establish the equivalence (iv), o (v), for all k or also to show that (iv) o (v) when 3 is nilpotent. NOW(Remark 2) we have seen that in that case (iv) is equivalent to (i). As M/S"M is isomorphic to M @A (A/3"), (i) implies (v) (Chapter I, 2, no. 7, Corollary 2 to Proposition 8);moreover clearly (v) then implies (i). We have therefore shown the equivalence (iv) o (v) in all cases and also that of all the properties of the theorem in the case where 3 is nilpotent. I (E) The implication (v) G- (i) when A is Noetherian and M ideally Hausdorff It is sufficient to prove that for every ideal a of A the canonical mapping j : a @A M -+ M is injective (Chapter I, 3 2, no. 3, Proposition 1). Let x E Kerj; a @A M is Hausdorff with the 8-adic topology, it suffices to verify that, for every integer n > 0, x E 3"(a @PA M). Letf. 3"a-t a be the canonical injection; it suffices to show that x E Im(f @ lM); for if b E 3", a E a and m E M, the h g e underf @ 1, of the element (ba) @ m of (3%) @A M is the element (ba) @ m = b(a 8.2)of a @AM and hence I m (f @)1, C 3"(a @AM). BY virtue of Krull's Theorem (5 3, no. 2, Theorem 2), there exists an integer k Consider next the diagram 3"a+ @A+ 3" @AM +(3"/8"+')@A (M/3M)+ (1) o.+l -+Sn+lM--+ 228 -1 0 Yn 3"M gr,(M) -+ 0 I 229 to show that the canonical mappingf: 3B @, M -+ 3M is injective. Let fbe the canonical mapping 3 @AB -+ 3B and f a the canonical isomorphism 8 @ A M + 8 @A B @, M ; f 0 (f @1M)0f z is the canonical mapping f : 8 @A M -+ 3M, as is easily verified. Nowf ' is an isomorphism since B is flat over A; it is then an isomorphism. Let p : A / 3 -+ B/3B be the canonical homomorphism; the (A/3)-module structure on M/3M derived by means of p from its (B/3B)-module structure is isomorphic to that on M @A (A/3). Then it follows that, if M is a flat Amodule, M/3M is a flat (A/S)-module and hence also a flat (B/3B)-module if p is an isomorphism; we have thus proved that (c) 3 (b) in that case. such that a, = a n c 3%; if i : a, -+ a is the canonical injection, it will then be sufficient to show that x E Im(i @ lM).Now, denoting by p : a -+ a/ak and h : a/a, -+ A/Sk the canonical mappings, there is a commutative diagram. a, @A M -J1 - 18 :@ 1 M a @A M 0 Ug 1M -+ @A 1M (A/3k) @A M in which the first row is exact. It suffices to prove that x E Kerip @ lM)and, as x E K e r j by hypothesis, it will suffice to verify that the mapping h @ 1, is injective. Now, it may also be written (Algebra, Chapter 11, $ 3, no. 6, Corollary 3 to Proposition 6) 8 IM/3":W @A/Sk (M/SkM) -f COROLLARY. Let A be a commutative Noetherian ring, 3 an ideal ofA, A the Hausdorff completion of A with respect to the 3-adic topology and M an ideally Hausdorff module with respect to 3A. For M to be aJat A-module, it is necessary and sufficient that M be aflat Amodule A- M/3kM and, as h is injective and, by (v), M/SkM is aflat (A/3'")-module,this completes the proof. We know in fact that A is a Noetherian ring ($ 3, no. 4, Proposition 8) and a flat A-module ($ 3, no. 4,Theorem 3), that 3A = (5 2, no. 12, Proposition 16) and that the canonical homomorphism A / 3 -+A/& is bijective (3 2, no. 12, Proposition 15) ; Proposition 3 can therefore be applied. 4. APPLICATIONS PROPOSITION 2. Let A be a commutative ring, 3 an ideal of A and B a commutative Noetherian A-algebra such that B is contained in the Jacobson radical of B. Then every finitely generated B-module M is an ideally Hausdorff A-module with respect to 3. We shall see more generally that for every finitely generated A-module N, N B A M is Hausdorff with the 3-adic topology. For No, = N g A B is a finitely generated B-module and the B-module N @A M is canonically identified with N,,, 8, M by virtue of the associativity of the tensor product. Let 2 be the Jacobson radical of B; as 3B is contained in 2,the 3-adic topology on N @A M is therefore identified with a finer topology than the 2-adic topology on N(B)QPB M ; but this latter topology is Hausdorff since N,,, 8, M is a finitely generated B-module (no. 1, Example 1), whence the conclusion. PROPOSITION 3. Let A be a commutative ring, B a commutative A-algebra, 3 an ideal of A and M a B-module. Suppose that B is a Noetherian ring and aJat A-module and that M is ideally Hausdorffwith respect to 3B. Thefollowing conditions are equivalent: (a) M is aflat A-module. (b) M is aflat B-module. (c) M/3M = M/(3B)M is aJat (B/3B)-module. Ifurther the canonical homomorphism A/3 -+ B/SB is bijective, conditions (a) and (b) are also equivalent to: (c) M/3 M is a flat (A/3)-module. Condition (a) implies (b) by Chapter I, $ 2 , no. 7, Corollaries 2 and 3 to Proposition 8 and the fact that M/3M is isomorphic to M @, (B/3B). Suppose condition (b) holds; to show that M is a flat B-module, we shall apply Theorem I of no. 2 with A replaced by B and 3 by 3B. It will therefore be sufficient 230 5 5.4 APPLICATIONS GRADUATIONS, FILTRATIONS AND TOPOLOGIES I11 PROPOSITION 4. Let A and B be two commutative Noetherian rings, h : A -+ B a ring homomorphism, 3 an ideal ofA and 2 an ideal ofB containing 3B and contained in the Jacobson radical of B. Let A be the Hausdorff completion of A with respect to the 3-adic topology and 8 the Hausdorff completion ofB with respect to the 2-adic topology; h is continuous with these topologies and h :A -+ f3 therefore makes 8 into an &algebra. Let M be ajinitely generated B-module and fi its Hausdorff completion with respect to the 2-adic topology; thefollowing properties are equivalent: (a) M is aflat A-module. (b) fi is aflat A-module. (c) M is aflat &-module. (d) M is aflat &module. As B with the 2-adic topology is a Zariski ring, fi is a faithfully flat B-module (5 3, no. 5, Proposition 9) and M is canonically isomorphic to M @, 8 (5 3, no. 4, Theorem 3) ;it is immediately verified that this canonical isomorphism onto the A-module structure on M @, 8 derived from that on M. Applying Proposition 4 of Chapter IY 3 3, no. 2 with R replaced by B, S by A, E by B, F by M, we see that M to be a flat A-module, it is necessary and sufficient that fi be a flat A-module. Moreover, 8 is a finitely generated &module and 3B is contained in 2 = 2B a d hence in the Jacobson radical of fj (3 3, no. 4,Proposition 8); therefore fi is an ideally Hausdorff A-module with respect to 3A (Proposition 2). Conditions (b) and (c) are therefore equivalent by the Corollary to Proposition 3. is an isomorphism of the A-module structure on a a a 23 1 EXERCISES EXERCISES 6 1) In order that A!, = @A! (resp. A! = (A")") for n 2 no, it is necessary and sufficient that A,,, = AA, (resp. A = (A,)n) for n 3 no. 3. Let K be a field, B the polynomial ring K[X, Y] with the graduation defined by the total degree, C the graded subring of B generated by X and Y2and a the graded ideal of C generated by Y4.Show that, in the graded ring A = C/a, A,,, = A,A, for n 3 2 but A, # (A,), for n 2 6. 32 1. Let K be a field, A the polynomial ring K[X, Y] in two indeterminates and a, the principal ideal (XU") in A; the sequence (an)n2 forms with a, = A an exhaustive and separated filtration on A. Let b be the principal ideal (X) of A; show that the topology on b induced by that on A is strictly coarser than the topology defined by the filtration on b associated with that on A (and a fortiori this latter filtration is distinct from the filtration induced by that on A). . 31 1. Let A be a graded commutative ring of type Z and (A,) its graduation; "9, we set A+ = h>O A,, A< = A,; these are graded subrings of A. (a) For every homogeneous elementof A of degree d, the ring of fractions A, (corresponding to the multiplicative subset consisting of the f",where n 3 0) has a canonical graded ring structure (Algebra, Chapter 11, 3 11) ; we denote by A,,, the subring of A, consisting of elements of degree 0. Show that, ifd > 0, then (A"), = A,, A,,)isisomorphic toACd)/(f - l)A(d)and((A,)>),, is a graded ring isomorphic to A,. (b) Let the polynomial ring B = A[X] = A gZZ[X] be given the graduation the tensor product of those on A and Z[X], a graduation compatible with the ring structure on B. Show that, if d > 0, B,,) is isomorphic to (A,) and (A(d)),is a graded ring isomorphic to A,, Z[X, X-l]. (c) Let g be another homogeneous element of A of degree e. Show that, if d > 0 and e > 0, A(,,,, is isomorphic to (Au))gd,.e" (d) Suppose d > 0 and (f) = 0 for n < 0. Show that, if A is Noetherian, so is A,, (use 3 2, no. 10, Corollary 4 to Theorem 2). * aZ 2. Let A be a graded commutative ring of type Z such that A, = 0 for n < 0. For all n 2 0, let A[,,] denote the graded ideal mqnAmof A; the Algebra Ah = nTo A[,] is a ring graded by the (A[,, a=(,, for allfE A, (d > 0), letfh denote the element of Ah whose component are zero except for that of degree d, which is equal to (a) Show that, iff E Ad, where d > 0, the ring Ah is isomorphic to (A,) (notation of Exercise 1). (b) For Ah to be a finitely generated A-algebra, it is necessary and sufficient that A be a finitely generated Ao-algebra. 2. Let K be a commutative field of characteristic 2 2 and A the ring K[[X, y]] of formal power series in two indeterminates. (a) Show that in A the principal ideal p = (X2 - Y3) is prime. (If a productf(X, Y)g(X, Y) of two formal power series is divisible by X2 - Y3, note first that f(T3,T2) = 0 or g(T3, T2)= 0 in the ring of formal power series K[[T]]; assuming for examplef(T3, T2) = 0, show first thatf(X, Y) is divisible by X + Y3 and, by consideringf (-Y3 + X, Y2), prove finally thatf(X, Y2) is divisible by X2- Y6.) (b) Let m be the maximal ideal AX + AY of A. Show that p is closed with respect to the m-adic topology on A (with which A is Hausdorff and complete) but that in theringgr(A), gr(p) is not a prime ideal (p being given the filtration induced by that on A). 3. Let A be a filtered ring and E a finitely generated A-module. Show that, i f E is given the filtration induced by that on A, gr(E) is a finitely generated gr(A)-module (cf. Exercise 5 (c)). 4. Give an example of a bijective A-linear mapping u: E -+ F, where E and F are two filtered A-modules, such that u is compatible with the filtrations but gr(u) is neither injective nor surjective. (Take E filtration and u the identity mapping.) * 232 Qo = A, F = A with another 5. Let A be a filtered commutative ring with filtration = A. (a),,, such that (a) For the ring gr(A) to be generated by a family of elements whose degrees are bounded, it is necessary and sufficient that there exist an integer q such 233 III EXERCISES GRADUATIONS, FILTRATIONS AND TOPOLOGIES that,for all n, a,= a,+ + b, where 6, is the sum of the ideals aFa7. . :a of the indicesj and k appearing in the elements of R or S, consider the images of the two sides of (*) under the canonical homomorphism for all systems of integers a, 2 0 (1 < i < q) such that f = la, = n + k + 6, for all k > 0. (b) For gr(A) to be Noetherian, it is necessary and sufficient that A be Noetherian, that the condition of (a) hold and that for i < q the a,/a,+, be finitely generated (A/a,)-modules (use Corollary 4 to Theorem 2 of no. 10). (c) Let K be a commutative field and A the polynomial ring in two indeterminates K[X,Y]. A total ordering is defined on the set of monomials X*Yn by setting X?n<XPYq if m + n < p + q or if m + n = p + q and m < p . Let (M,) be the sequence of monomials in X, Y thus arranged in ascending order and let a, be the ideal of A generated by the Mk of index k 2 n. Show that (a,) is a filtration compatible with the ring structure on A; with this filtration gr(A) admits divisors of 0 and is not Noetherian, although A is a Noetherian integral domain (use the criterion in (b)); in particular, gr(A) (with the filtration induced on a, by that on A) is not a finitely generated gr(A)-module, although a, is a finitely generated A-module (cf. § 1, no. 2, Corollary to Proposition 1). 7 6. Let A be a commutative ring, E and F two A-modules and (En) (resp. (F,)) an exhaustive filtration on E (resp. F) consisting of sub-A-modules. On the tensor product G = E @A F, consider the exhaustive filtration consisting (E / E) Fq) and argue by induction on Card(R) (d) Deduce from (c) that the canonical homomorphism defined in (a) is then bijective. @A + 7. Let A be a commutative ring, E an A-module, F a submodule of E, B the exterior algebra A (E) and 3 the two-sided ideal of B generated by the canonical images in B of the elements of F. Let gr3(B) be the graded ring associated with the ring B filtered by the 3-adic filtration. (a) Define a surjective canonical (non-graded) A-algebra homomorphism A (E/F) 8 (A (E/F)) -+ gr3(B) (where we mean the skew tensor product of graded algebras (Algebra, Chapter 111). (b) Show that, if F admits a complement in E, the homomorphism defined in (a) is an isomorphism. (c) Take A = Z,E = 2/4Z, F = 22/4Z; show that the homomorphism defined in A is not injective in this case. 1 ~ c (FJ/Fj+l) + (Ei @AFj)/(Im (Et @AF,+,) + Im(Ei+1 @AF,)) (*I Hhk) I 10. Let A be a Hausdorff commutative ring and 0 an automorphism of A. Show that on the ring E defined in Algebra, Chapter IV, 3 5, Exercise 10 (b) is a (left or right) Noetherian ring. 11. Show that, if E is a vector space of dimension 2 over a commutative field, the tensor algebra of E is a ring which is neither left nor right Noetherian (if a, b are two linearly independent vectors in E, consider the left ideal (or right ideal) generated by the elements anbn for n 2 1). = Hsup(t.h),sup(f,k) where in the second sum (i,j, h, k) run through R x S. (If R and S are each reduced to a single element, use Chapter I, 5 2, no. 6 , Proposition 7. Ifp is the greatest of the indices i and h appearing in the elements of R or S, q the least 234 (b) I. ((;Rf(h2t; H,> of A x E to E is uniformly continuous with the topologies defined by the filtrations. 9. Give an example of two filtered rings A, B whose filtrations are exhaustive and separated and a non-surjective homomorphism u : A -f B compatible with the filtrations and such that gr(u) is bijective. From this deduce a counterexample to Corollary 1 to Proposition 12 when the ring A is not assumed to be complete and a counter-example to Proposition 13 when E is no longer assumed to be finitely generated (use Algebra, Chapter VIII, 3 7, Exercise 3 *Gt+j/Gf+j+l are the restrictions of a graded homomorphism of degree 0 (called canonical) gr(E) @A gr(F) -f gr(E @A F), which is surjective. (b) Show that, if gr(E) is a flat A-module, the A-modules Em/Enfor m < n and (E/En for n E Z are flat. (c) Suppose in the following that gr(E) is a flat A-module and that E is a flat A-module (the second hypothesis being a consequence of the first if (En) is a discrete filtration). Then the H,, = E, @A Fj are canonically identified with submodules of G = E @A F (Chapter I, 2, no. 5, Proposition 4). Show that, for any two finite subsets R, S of Z x Z, (E1 n F,) ... Let A be a filtered ring, (A,) its filtration, E a filtered A-module and E, = E, the mapping (a, x) H ax (this filtration. Show that, if the G, = + j = n Im(E, @A F,). (a) Show that the canonical homomorphisms (Et/E(+l)@A 4 + 112. Let K be a commutative field, A the polynomial ring K[X],],El in an arbitrary infinite family of indeterminates and m (the maximal) ideal of A generated by the X,. If we set 4 = A/mi+l,the A, and the canonical homomorphisms h,,: A/mj + A/mi for i < j satisfy the conditions of Proposition 235 GRADUATIONS, FILTRATIONS AND TOPOLOGIES 111 EXERCISES 14; the ring lim A, is the completion A of A with respect to the m-adic topol ogy and the kernel of the canonical homomorphism A --f A, is equal to (m1) fie closure of rn' in A. (a) Show that A is canonically identified with the ring of formal power series in the X,, each of which has only afinite number of terms of given degree (Algebra, Chapter IV, 3 5, Exercise 1). (b) From now on take I = N. Show that m # A.m (consider the formal A, W 21 XL power series (c) Suppose that K is a finite field. Show that (m)2 # (rn2)- (Show first the following result: for every integer k > 0, there exists an integer nk and for every integer n 2 nk a homogeneous polynomial F, of degree n in n2 indeterminates with coefficients in K such that F, cannot be the sum of the terms of .. . P K Q k , where the P, degree n in any polynomial of the form P,Q, and Qi are polynomials without constant term in the same indeterminates.) Deduce that A is not complete with respect to the m-adic topology. + + 13. Let K be a field, A = K[[X]] the ring of formal power series and rn its maximal ideal, so that A is Hausdorff and complete with the rn-adic topology (no. 6, Corollary to Proposition 6) . On the additive group A consider the filtration (En) such that E, = A and En is the intersection of rnn and the ring K[X] ; this filtration is exhaustive and separated, the topology 9 which it defines on A is compatible with the additive group structure on A and is finer than the rn-adic topology but it is not a complete group with the topology 9 (consider the sequence of polynomials (1 - Xn)/(l - X)). 14. Deduce from Exercise 12 an example of a ring A (not necessarily commutative) and a left A-module. A topology on E is called linear if it is invariant under translations and 0 admits a fundamental system of neighbourhoods which are submodules of E ; E is then said to be linearly topologized. A linear topology on E is compatible with the module structure if A is given the discrete topology. 0 n any A-module the discrete topology and the coarsest topology are linear topologies. (a) I f E is a linearly topologized module and F a submodule of E, the induced topology on F and the quotient topology of that on E by F are linear topologies. If @,,fa,) is an inverse system of linearly topologized A-modules, where the fap are continuous linear mappings, the topological A-module E = lim Ea t is linearly topologized. (b) Let E be a linearly topologized A-module. There exists a fundamental system (Vh)hpLof neighbourhoods of 0 in E consisting of open (and closed) submodules; if E/V, -+E/V, is the canonical mapping when V, 2 V,, is an inverse system of discrete A-modules; the topologie family (E/V, , gical A-module = lim E/V, is identified with the Hausdorff completion of E, +(, e 236 t which is therefore linearly topologized (General Topology, Chapter 111, 3 7, no. 3). (c) A Hausdorff linearly topologized A-module E is discrete if it is Artinian or if there exists a least element in the set of submodules # 0 of E. 15. (a) Let E be a Hausdorff linearly topologized A-module. For a filter base 23 on E consisting of linear varieties to admit a cluster point, it is necessary and sufficient that for every 23' 23 consisting of linear affine varieties. It is said to be linearly compact if it is Hausdorff and every filter base on E consisting of linear affine varieties admits a t least one cluster point. Every Artinian module is linearly compact with the discrete topology. Every linearly compact submodule of a Hausdorff linearly topologized module F is closed in F. (b) If E is a linearly compact A-module and u a continuous linear mapping of E to a Hausdorff linearly topologized A-module F, u(F) is a linearly compact submodule of F. (c) Let E be a Hausdorff linearly topologized A-module and F a closed submodule of E. For E to be linearly compact, it is necessary and sufficient that F and E/F be so. (d) Every product of linearly compact modules is linearly compact (consider a filter base which is maximal among the filter bases consisting of affine linear varieties and having a single cluster point ... such that the E/U, are linearly compact discrete A-modules (cf. 4 3, Exercise 5). (TOsee that (y) implies (d) consider a open submodule F of E and a filter base 23 on E/F consisting of affine linear varieties. If all V E 9, let M, be the 237 111 inverse image in E of the direction submodule of V in E/F; consider on E the linear topology in which the M, form a fundamental system of neighbourhoods of 0.) (b) Let E be a Hausdorff linearly topologized A-module and M a linearly compact submodule of E. Show that, for every closed submodule F of E, M + F is closed in E (consider the image of M in E/F). (c) Let E be a linearly compact A-module and F a Hausdorff linearly topologized A-module. Show that for every closed submodule M of E x F, the projection of M onto F is closed. Obtain the converse (cf. General Topology, Chapter I, 3 10, no. 2). (d) Let E be a linearly compact A-module and u a continuous linear mapping of E to a Hausdorff linearly topologized A-module F. Show that, for every filter base 8 on E consisting of affine linear varieties, the image under u of the set of cluster points of 8 is the set of cluster points of u (8) . In particular, for every closed submodule M of E, NQB (M + N) = M + N. NcB 17. A linear topology Fon an A-module E is called minimal if it is Hausdorff and there exists no Hausdorff linear topology strictly coarser than F. (a) For a Hausdorff linearly topologized A-module E to be minimal, it is necessary and sufficient that every filter base on E consisting of affine linear varieties and having a single cluster point, be convergent to this point. (To see that the condition is necessary, observe that, when M runs through 8 and V a fundamental system of neighbourhoods of 0 consisting of submodules, the M + V form a filter base with the same cluster points as 8. To see that the condition is sufficient, note that a filter base consisting of open submodules, whose intersection is reduced to 0, is a fundamental system of neighbourhoods of 0 in a Hausdorff linear topology coarser than 9.) (b) For a discrete topology on an A-module E to be minimal, it is necessary and sufficient that E be Artinian. (c) If Fis minimal, the topology induced by Fon any closed submodule of E is minimal. 7 18. In an A-module E, a submodule M # E is called sheltered if there exists a least element in the set of submodules # 0 in E/M. (a) Show that every submodule N # E of E is an intersection of sheltered submodules (for all x 6 N, consider a maximal element in the set of submodules of E containing N and not containing x) . (b) Let F be a Hausdorff linear topology on E and let F*be the linear topology with fundamental system of neighbourhoods of 0 the filter base generated by the submodules of E which are open under 9- and sheltered. Show that F*is Hausdorff and that every submodule which is closed under 9- is also closed under F*(note that every submodule which is closed under .T is an intersection of submodules which are open under F).Deduce that, if E is 238 EXERCISES GRADUATIONS, FILTRATIONS AND TOPOLOGIES complete with respect to F*,it is complete with respect to F (General Topology, Chapter 111, 3 3, no. 5, Proposition 9). (c) Suppose that F is linearly compact. Then show that F*is a minimal linear topology (Exercise 17). (Let 8 be a filter base consisting of submodules closed under F whose intersection is 0; show that, for every submodule U which is open under F and sheltered, there exists M E 8 such that M C U, using Exercise 16 (d)). (d) Let F be a Hausdorff linearly topologized A-module and Fl its topology; show that, if u : E + F is a continuous linear mapping with respect to F and u is also continuous with respect to the topologies T* topologies F and Fl, and F . 7 19. (a) Let E be a linearly compact A-module. Show that the following conditions are equivalent: (a) For every continuous linear mapping u from E to a Hausdorff linearly topologized A-module F, u is a strict morphism (General Topology, Chapter 111, 5 2, no. 8) from E to F. (p) For every closed submodule F of E, the quotient topology on E/F is a minimal topology (Exercise 17). (y) E is complete and there exists a fundamental system (U,) of open neighbourhoods of 0 in E, consisting of submodules and such that the E/U are Artinian modules. (To see that (y) implies (p), reduce to the case where F = 0 and use Exercises 17 and 18.) If E satisfies the equivalent conditions (a) , (p) and (y), E is called strictly linearly compact. (b) Let E be a Hausdorff linearly topologized A-module and F a closed submodule of E. For E to be strictly linearly compact, it is necessary and sufficient that F and E/F be so. (c) Every inverse limit of strictly linearly compact modules is strictly linearly compact. (d) Let E be a Hausdorff linearly topologized A-module and u a linear mapping from E to a strictly linearly compact A-module F. Show that, if the graph of u is closed in E x F, u is continuous (use Exercise 16 (c) and the fact that, if M is closed in E and E/M is Artinian, M is open in E). 7 20. (a) Show that a discrete linearly compact module cannot be the direct sum of an infinite family of submodules # 0 (b) Give an example of a minimal linear topology (Exercise 17) which is not linearly compact (consider an infinite direct sum of simple modules no two of which are isomorphic). (c) Let E be a Hausdorff linearly compact module such that there exists a family of simple submodules whose sum is dense in E. Show that: (1) E is strictly 239 111 EXERCISES GRADUATIONS, FILTRATIONS AND TOPOLOGIES linearly compact (apply (a) to the quotient of E by an open submodule) ;(2) E is isomorphic to the (topological) product of a family of discrete simple modules. (Consider the sets of maximal open submodules of E such that for every finite /(kbl G k)is the direct sum space (Gk)< k< ,,of n distinct elements of 0,E of n simple submodules. Show that there exists a maximal set 0 (with respect to inclusion) and that the intersection of all the submodules G belonging to such a set is reduced to 0; use the fact that (0) is an intersection of maximal open submodules and that for every maximal open submodules of E there is at least one simple submodule of E not contained in G. Conclude by using the fact that E is strictly linearly compact.) (d) Deduce from (c) that every linearly compact vector space over a field K is strictly linearly compact and isomorphic to a product Kr. 7 21. Recall that on a ring A a topology is called (left) linear if it is a linear topology on the A-module A (Chapter 111, 3 2, Exercise 16). A topological ring A is called (left) linearly compact (resp. strictly linearly compact) if it is a linearly topologized A-module which is linearly compact (resp. strictly linearly compact). A-module. (a) Show that, if A is left linearly compact with the topology F, the topology F*defined in Exercise 18 (b) is also compatible with the ring structure on A (use Exercise 18 (d)). (b) Suppose that A is linearly compact; let u # 0 be an idempotent of A/%, where 31 is the Jacobson radical of A. Show that if A is linearly compact with the discrete topology, there exists a unique idempotent e E A whose image in A/% is equal to u. (Show that among the linear affine varieties x, where 0 < x < 31 and x2 - x E b, which are closed in A ... which is minimal. Deduce that e2 = e and e = 0, by considering the element e ea - e = rand showing that r E Ar2, using Algebra, Chapter VIII, 5 6 , Exercise 10 (a). Prove the uniqueness of e by showing that if el, e2 are two idempotents of A such that e,e2 E %, then e1e2 = 0.) (c) Show that every commutative ring A which is linearly compact with the discrete topology is a direct composition of a finite number of local rings (which are linearly compact with discrete topology). (Consider first the case, where 31 = 0, using Exercise 15 (b) and Chapter XI, 5 1, no. 2, Proposition 5, then apply (b) to the idempotents of A/%.) (d) Show that every linearly compact (resp. strictly linearly compact) commutative ring A is the product of a family of linearly compact (resp. strictly linearly compact) local rings. (Let (mb)be the family of open maximal ideals of A; for every open ideal a not containing mh, let AI, X A: be the decomposition of A/a as a direct composition of two rings such that AI, is a local ring with maximal ideal (mh + a)/a defined in (c); let el, be the unit element of A: considered as a class mod. a in A; the e?(a) form a filter base + + 240 which converges in A to an idempotent e, and Ae, is a closed ideal of A which eh is the unit element. Show that the ring Ae, is a local ring and that A is isomorphic to the product of the Ae,.) 7 22. (a) Let A be a local ring and m its maximal ideal. Show that, if for a linear topology F on A, A is strictly linearly compact, F is coarser than the m-adic topology. (b) Let A be a commutative ring and m an ideal of A. For A to be strictly linearly compact with the rn-adic topology, it is necessary and sufficient that A/m be Artinian, that A be complete with the m-adic topology and m/m2 be a finitely generated A-module. (c) Let K be a field and A = K[[X,]],El the ring of formal power series in the family of indeterminates (xL)LE~ (Algebra, Chapter IV, 3 5, Exercise 1) ; A is a local ring. As a vector space over K, A may be identified with the product space KN"" if K is given the discrete topology, [illegible] the powers of the same maximal two-sided ideal. 1. Let A be a commutative ring which is Hausdorff and complete with a filtration domain is a field (Algebra, Chapter VIII, 5 6, no. 4,Proposition 9). PROPOSITION 7. Let M be ajinitely generated module over a Noetherian ring A. The following properties are equivalent: (a) M is of finite length. (b) Every ideal p E Ass(M) is a maximal ideal of A. (c) Every ideal p E Supp(M) is a maximal ideal of A. Let (Mi)ocicthe a composition series of M such that, for 0 < i < n - 1, M,/M,+, is isomorphic to A/p,, where p, is prime (3 1, no. 4, Theorem 1). If M is of finite length, so is each of the A-modules A/p,, which implies that each of the rings A/p, is Artinian, hence, as A/pt is an integral domain, it is therefore a field, in other words pt is maximal; we conclude that (a) implies (b) (3 1, no. 4,Theorem 2). Condition (b) implies (c) by 3 1, no. 3, Proposition 7. Finally, if all the ideals of Supp(M) are maximal, so are the pt (3 1, no. 4, Theorem 2), hence the A/p, are simple A-modules and M is of finite length, which completes the proof. of jinite length M over a Noetherian Zing A, Every element of Supp(M) is then minimal in Supp(M) and the conclusion follows from 5 1, no. 3, Corollary 1 to Proposition 7. COROLLARY 2. Let M be ajinitely generated module over a Noetherian ring A and p a prime ideal of A. For M, to be a non-zero A,-module ojinite length, it is necessary and suflicient that p be a minimal element of Ass(M). By 5 1, no. 2, Corollary to Proposition 5, AssA,(M,) is the set of ideals q,, where q runs through the set of ideals of Ass(M) which are contained in P. On the other hand, p is the unique maximal ideal of Ap;by Proposition 7, for Mp to be an A, -module of finite length it is necessary and sufficient that no element of Ass(M) be strictly contained in p. On the other hand, for Mp # 0, 2 74 it is necessary and sufficient by definition that p ~ S u p p (M)(Chapter 11, 5 4,no. 4),that is that p contain an element of Ass(M) (8 1, no. 3, Proposition 7). This proves the corollary. DJ(S-lM/S-lN) is surjective. COROLLARY 1. For every module Ass(M) = Supp(M). 3 2.5 RINGS AND MODULES OF FINITE LENGTH Remark (1). Let M be a finitely generated module over a Noetherian ring A; let (M I),,,,, be a composition series of M such that, for 0 < i < n - 1, M,/M,+l is isomorphic to A/p,, where p, is a prime ideal of A (4 1, no. 4, Theorem 1). If p is a minimal element of Ass(M), the length longA,(M,) is equal to the number of indices i such that pi = p. For the form a composition series of M, and (Mf)p/(Mi+l)p is isomorphic to (A / P ~and) ~ hence to (0)if p, # p (since p is minimal in the set of pl by $ 1, no. 4, Theorem 2) and to (A/p), which is a field, if p, = p. PROPOSITION 8. Let M be of jinite length over a Noetherian ring A. (i) There only exists a single primary decomposition of{O} which is irredundant and which is indexed by Ass(M) (necessarily reduced) ; let {0} = ,€ Q(p) be this decomposition, where Q (p) is p-primary with respect to M . (ii) There exists an integer no such that, f o r all n 2 no and all p E Ass(M), Q(P) = p"M** (iii) For all p E Ass(M), the canonical mapping of M to M, is surjective and its kernel is Q(p). (iv) The canonical injection of M into @(M/Q(p)) is bijective. CCM) %(, As every element p E Ass(M) is minimal in Ass(M) (Proposition 7), assertion (i) follows from no. 3, Proposition 5. As M is finitely generated, there exists no such that p"M c Q (p) for all pEAss(M) and all 2 no (no. 1, Remark); but as p is a maximal ideal, p"M is p-primary with respect to M (no. 1, Examples 2 and 3) and as pnM = {0}, it follows from (i) that necessarily pnM = Q (p) for all p E Ass(M); whence (ii). As the p", for p E Ass(M), are relatively prime in pairs (Chapter 11, fj 1, no. 2, Proposition 3), the canonical mapping M (M/p"M) is surjective (Chapter 11, fj 1, no. 2, Proposition 6) , whence (iv). Then Ass(Q(p)) = Ass(M) {p} and &(M/Q(p)) = {p} (no. 3, Proposition 4); as the elements of Ass(M) are maximal ideals, p is the only element of Ass(M) which does not meet A p; Q(p) is therefore the kernel of the canonical mapping j : M -+M, (9 1, no. 2, Proposition 6). If s E A p, the homothety of M/Q(p) with ratio s is injective by virtue of the relation Ass(M/Q(p)) = {p} (no. 1, Proposition 11); since M/Q(p) is Artinian, this homothety is bijective (Algebra, Chapter VIII, 0 1, no. 2, Lemma 3). The canonical mapping M -+M/Q(p) is then written f o j , where3 M, -+M/Q(p) is an A-homomorphism (Chapter 11, fj 2, no. 2, Proposition 3) ; as Ker(j) = Ker(f o j) = Q (p) , f is injective; we conclude that j is surjective and f bijective. - - - 275 IV RINGS AND MODULES OF FINITE LENGTH ASSOCIATED PRIME IDEALS AND PRIMARY DECOMPOSITION I t follows from Proposition 9 and Proposition 8 (iii) and (iv) that, if (mt)l 0, there exists n > 0 such that F,, c mPE. As A is a Zariski ring, E is Hausdorff and the F, are closed under the m-adic topology. On the other hand, E is complete (Chapter 111,s 2, no. 12, Corollary 1 to Proposition 16). Finally, E/mPE is a finitely generated module over the k g A/mp, which is Artinian (Corollary 2); then E/mpE is an Artinian (A/mp)-moduleand hence an Artinian A-module. The corollary then follows from Chapter 111,s2, no. 7, Proposition 8. COROLLARY 1. Every Artinian ring A is isomorphic to the direct composition of ajinite family o f Artinian local rings. 276 277 ASSOCIATED PRIME IDEALS AND PRIMARY DECOMPOSITION IV PRIMARY DECOMPOSITION AND EXTENSION OF SCALARS homomorphism S-lA+t = 1 (S-'A/S-'p,) is bijective. We know moreover that the canonical homomorphism S-'A -+ A,, is surjective and has kernel S-lpr and the COROLLARY 5. In a complete semi-local Noetherian ring every decreasing sequence of &ah whose intersection is 0 is ajlter base which converges to 0. n n canonical homomorphism S-lA, + A,, is composed o&, and an isomorphism (S-lA)s-l,, + A,, (Chapter 11, 3 2, no. 3, Proposition 7). Finally, it follows from Proposition 8 that (S-lA)s-lp, is isomorphic to S-lA/S-lp, and hence is a field since S-lp, is a maximal ideal. It t is sufficientto apply Corollary 4 to the A-module E. PROPOSITION 10. Let A be a Noetherian ring and ply . . .,pn the prime ideals associated with the A-module A, where pl # p, f o r i # j , ic n 6. PRIMARY DECOMPOSITION AND EXTENSION OF SCALARS (i) The set S = (A- pi) is the set of elements which are not divisors of0 in A. (ii) I f a l l the pi are minimal elements ofAs(A), the total ring ofractions S-IA of A is Artinian. (iii) Ifthe ring A is reduced, 1111the pl are minimal elements of Ass(A) (and therefore are the minimal elements of Spec(A)) and each of the 4,is a jel d ; for each index i, the canonical homomorphism S-IA -+ A,, (Chapter 11, 3 2, no. 1, Corollary 1 to Proposition 2) is surjective and its kernel is S - 'p, ;jnally the canonical homomorphism In this no., A and B will denote two rings and we shall consider a ring homomorphism p: A +- B which makes B into an A-algebra; recall that, for every B-module F, p,(F) is the commutative group F with the A-module structure defined by a .y = p(a) y for all a E A, y E F. LEMMA 1. Let A be a Noetherian ring, p a prime ideal of A, E an A-module whose annihilator contains a power of p and such that Ass(E) = {p} and F a B-module such that p,(F) is a jlat A-module. The condition E AssB(E @A F) then implies n n from S-1A to i = l (S-'A/S-'p,) is bijective. -1 p - i f a E A p, the homothety h with ratio a on E is injective (3 1, no. 1, Corollary 2 to Proposition 2); as h @ lF is the homothety h' with ratio p(a) on E @A F and p*(F) is flat, h' is injective (Chapter I, Q 2, no. 2, Definition 1); n u of the form S-lp, where p is a prime ideal of A contained in i = 1 p, (Chapter 11, $2, no. 5, Proposition 10) that is contained in one of the p, (Chapter 11, 3 1, no. 1, Proposition 2). If p, is a minimal element of Ass(A), it is a minimal element of Spec(A) (3 1, no. 3, Corollary to Proposition 7), which implies that the ideals of S-'A are the S-lp, and they are therefore all maximal, which proves that S-lA is Artinian (Proposition 9). this proves that p(a) % Y,whence>'(V) B-module such that p*(F) is a j u t A-module. Then (8 1, no. 3, I Corollary 2 to Proposition 7). We deduce that (0) = i(pi is a reduced primary =1 decomposition of the ideal (0) (no. 3, Corollary to Proposition 4) ;in particular, none of the p, can contain a p, of index j # i and therefore the pi are all minimal elements of Ass(A).The ring S-IA is then Artinian by (ii). The S-lp, are prime ideals associated with the S-lA-module S-IA (8 1, no. 2, Corollary to Proposi- I ,fi i=1 tion 5) and(0) = S-l p,) = S - Ip, (Chapter 11, 5 2, no. 4) ;as the S-'p(are distinct, (S - I p r) l c r ~is n a reduced primary decomposition of (0) in S-'A (no. 3, Corollary to Proposition 4). Proposition 8 then shows that the canonical 278 = p. THEOREM 2. Let p: A -+ B be a ring homomorphism, E an A-module and F a n n pi = (0) (W= P. If n is such that p"E = 0, then p"B c Ann(E @A F), which implies that p"B c g,which implies pn c -p1 (a) and therefore p c pl(~) since-:(P) is prime. Moreover, The fact that S is the set of elements which are not divisors of 0 in A has already been seen (Q1, no. 1, Corollary 3 to Proposition 2). The prime ideals of S-'A are Suppose finally that the ring A is reduced. Then 3 2.6 (5) @A F) of the Supp(F/pF). (5) are equal. Let p E Ass(E) ;by definition there exists an exact sequence 0 +-A/p -+E. Shce F is a flat A-module we derive an exact sequence O-+F/) Whence AssB(F/pF)c AssB(E @AF), which proves the inclusion (5). Suppose now that A is Noethan'an and let US prove the opposite inclusion. 279 ASSOCIATED PRIME IDEALS AND PRIMARY DECOMPOSITION IV We proceed in stages: (i) Suppose first that E is a finitely generated A-module and that AssA(E)is reduced to a single element p. By 9 1, no. 4,Theorem 1 there exists a composition of E such that Ei/Et+lis isomorphic to A/pi, where p r is a series (E)oGi5n prime ideal of A; moreover (3 1, no. 4, Theorem 2 and no. 3, Proposition 7) all the p i contain p. As F is a flat A-module, the E, @A F) form a composition series of E @A F and (El @A F)/(E1+1@AF) is identified with (A/pi) = F/piF* @AF Then by virtue of 3 1, no. 1, Proposition 3 F, ;, Let us apply Theorem 2 to the A-module E / Q and the B-module B; then AssA(E/Q) = {p} and (E/Q) @A B is isomorphic to (E @A B)/(Q @A B) and hence AssB((E @AB)/() @A B) is reduced to 'p, whence the corollary. - AssB(F/pLF)* We know that E is annihilated by a power of p (no. 1, Remark); Lemma 1 then shows that, for 'p E AssB(E COROLLARY 2. Suppose that A and B are Noetherian and that B is a j a t A-module. Let p be a prime ideal of A, Q c E a p-primary submodule and 'p a prime ideal of B. For Q @A B to be a 9-primary submodule of E @A B, it is necessary and sufficient that pB be a 'p-primary ideal of B. Remark. Suppose that A and B Noetherian. Let 'p be a prime ideal of B and n-1 @A 3 2.6 PRIMARY DECOMPOSITION AND EXTENSION OF SCALARS F), Q('p) = pi for all 'p E AssB(F/P~F)by Lemma 1, whence AssB() F) n Ass(F/p,F) = % if pi # p, which proves the theorem in the case considered. (ii) Suppose only that E is a jnitely generated A-module. Let p i (1 < i < n) n be the elements of AssA(E) and let (0) = L = l Ql be a corresponding reduced primary decomposition (no. 3) ; E is then isomorphic to a submodule of the direct sum of the El = E/QLand, as F is a flat A-module, E @A F is isomorphic to a submodule of the direct sum of B-modules El @A F. We deduce (§ 1, no. 1, Proposition 3 and Corollary 1 to Proposition 3) that pB = p l (9); let us write S = A p and let k (p) = S-I(A/p) be the field of fractions of A/p. Since 9 contains pB, 'p/pB is a prime ideal of B/pB. If p' is the composite homomorphism A -% B +B/pB, we know that S-'(B/pB) is identified with the ring (p'(S))-I(B/pB) and ('ps' = S-l(g/pB) with an ideal of this ring (Chapter 11, § 2, no. 2, Proposition 6); as 'p/pB does not meet p'(S), q'is a prime ideal of S-l(B/pB) (Chapter 11, 9 2, no. 5, Proposition 11) ; moreover there are canonical isomorphisms between S-l(B/pB), S-1 ((A/p) @A B) and (S-l(A/p)) @A B = k (p) @A B; similarly S-'(F/pF) is canonically identified with k(p) @A F. There exists an p E Ass,(p/gA~(k(~) @A F). By Theorem 2 and its Corollary 1, it amounts to verifying that the conditions n "V E AssB(F/pF)" and "V E As s ~ < ~) B ~ (~ F)" (P) But El is a finitely generated A-module such that AssA(E1) is reduced to a single element p i (no. 1, Definition 1). By (i), AssB(E1 @A F) = AssB(F/piF), whence the theorem in this case. (iii) General case. The B-module E @A F is the union of the submodules E' @A F, where E' runs through the set of finitely generated submodules of the A-module E. If Cp belongs to AssB( F), then there exists a finitely generated submodule E' of E such that 'p E AssB(E' @A F). By (ii), there exists p E Ass,(E') such that 'p E Ass,(F/pF) ; as Ass,(E') c Ass,(E), this completes the proof of Theorem 2. COROLLARY 1. If A is Noetherian and 'p E AssB(E, F), then p'('p) E Ass,(E) 280 PROPOSITION 11. Suppose that A and B are Noetherian and that B is a frat A-module. k t E be an A-module and E' a submodule ofE such that,for every ideal p E AssA(E/E'), the ideal pB is prime. Let E' = Q (p) be a reducedprimary decomposition ofE' in E, Q(p) being p-primary for all p E Ass(E/E'). (i) I f p E Ass(E/E') and pB = B, then Q (p) @A B = E @A B. (ii) I f p E Ass(E/E') and pB # B, Q (p) @A B is pB-primary in E @A B. (iii) If is the set of p E Ass(E/E') such that pB is prime, then E' @A B = and-t(p) is the onlyprime ideal p ofA such that 'p E AssB(F/pF)* @A B. This follows from Theorem 2 and Lemma 1 applied to the case where E are equivalent; but, as B is Noetherian, this follows from 3 1, no. 2, Corollary to Proposition 5 and the above identifications. = A/p. pG(Q (p) @A B) and this relation is a reducedprimary decomposition of E' @A B in E @A B. 28 1 IV If pB = B, Theorem 2 applied to E/Q(p) and B shows that ~ B ((E / Q (P)@A) B) = 5 3.1 PRIME IDEALS ASSOCIATED WITH A GRADED MODULE ASSOCIATED PRIME IDEALS AND PRIMARY DECOMPOSITION 3. PRIMARY DECOMPOSITION IN GRADED MODULES 63 and, as B is Noetherian and is a flat A-module, we conclude (§ 1, no. 1, Corollary 1 to Proposition 3) that Q (p) @A B = E @A B. Assertion (iii) follows from Corollary 2 to Theorem 2, taking = pB. Finally the relation E' @A B = (Q (p) @A B) follows from the fact that B is a flat A-module 1. PRIME IDEALS ASSOCIATED WITH A GRADED MODULE pcm PROPOSITION 1. Let A be a torsion-jiree commutative group, A a graded ring of type A and M a graded A-module of type A. Every prime ideal associated with M is graded and is the annihilator of a homogeneous element of M. (Chapter I, $ 2 , no. 6, Proposition 6); as p = pl(pB) for p E Q (Lemma 1), pB # p'B for two distinct ideals p, p' of the set 0;on the other hand, We know that A can be given a total order structure compatible with its group structure (Algebra, Chapter 11, 5 11, no. 4,Lemma 2) . Let p be a prime ideal associated with My the annihilator of an element x E M, and let (x,) , ~ ~ be the family of homogeneous components of x ; let i (1) < i (2) < . + < i (r) be the values of i for which xi # 0. Consider an element a E p and let (aJIEA be the family of its homogeneous components; we shall prove that a, E p for all i E A, which will show that p is a graded ideal. We argue by induction on the number of indices i such that a, # 0. This assertion is obvious if this number is 0; if not, let m be the greatest of the indices i for which a, # 0; if we prove that a, E p, the induction hypothesis applied to a - a, will give the conclusion. Now, ax = 0; for all j E A, using the fact that the homogeneous component of degree m + j of ax is 0, we obtain (Ass(E @A B)/(E' @A B)) = by Theorem 2; we conclude from no. 3, Proposition 4 that + is a reduced primary decomposition. COROLLARY. Suppose that pB is prime for all p E AssA(E/E'). Then, if pl , . . .,pn are the minimal elements of AssA(E/E'), the,p B are minimal elements of Ass,(E @A B)/(E' 8.4 B))It follows from Proposition 11 that in this case pB # p,B for i #j . @A c a,+i=0 we conclude that a,xj is a linear combination of the x, of indices E' > j . In particular therefore amxf(r;= 0, whence, by descending induction on n < r, a,+lxt(n, = 0. Then ahx = 0, whence a; E p, and as p is prime, a, E p. We now show that p is the annihilator of a homogeneous element of M. Let us write 6, = Ann(x,(,,) for 1 < n < r. For every homogeneous element b of P and all n the homogeneous component of bx of degree i (n) + deg(b) is bxi(n),hence bx,,,) = 0 and therefore b E 6,; as p is generated by its homogeneous Examples (1) Let us take B = S-IA, where S is a multiplicative subset of A; if A is Noetherian, the hypotheses of Proposition 11 are satisfied and we recover a part of Proposition 6 of no. 4. (2) Let A be a Noetherian ring, m an ideal of A and B the Hausdorff completion of A with respect to the m-adic topology; then B is a flat A-module and Theorem 2 may be applied with F = B; but in general the hypotheses of Proposition 11 are not satisfied for the prime ideals of A (Chapter 111, 5 2, Exercise 15 (b)). (3) Let A be a Noetherian ring and B the polynomial algebra A[X,, . . ., X,] ; B is Noetherian and is a free A-module and hence a flat A-module. Also, if p is a prime ideal of A, B/pB is isomorphic to (A/p) [X,, . . ., X,], which is an integral domain, and hence pB is prime; the hypotheses of Proposition 11 are therefore satisfied for every A-module E and every submodule E' of E. (4) Let A be a finitely generated algebra over a field K , K an extension of K and B = A @k K the algebra over K obtained by extension of scalars; A and B are Noetherian and B is a free A-module and hence Theorem 2 may be applied to F = B. In certain cases (for example if k is algebraically closed) it can be shown that for every prime ideal p of A, pB is prime or equal to B; we shall return later to this example. 1 282 I, E - r I n elements, p 6,. On the other hand, clearly 6, c Ann(x) = p; as p is == 1 prime, there exists an such that 6, c p (Chapter 11, $ 1, no. 1, Proposition l), whence 6, = P = Ann(x,(,,), which completes the proof. COROLLARY. For every (necessarily graded) prime ideal p associated with a graded A-module M, there exists an integer i such that the graded A-module (A/p)(k) obtained from the graded A-module A/p by diminishing the degrees by k (Algebra, Chapter 11, 5 11, no. 2) is isomorphic to a graded submodule of M. With the notation of the proof of Proposition 1, consider the homomorphism obtained, by taking quotients, from the homomorphism a H ax,(,, of A to M; the latter is a graded homomorphism of degree i (n) and hence it 283 5 3.3 ASSOCIATED PRIME IDEALS AND PRIMARY DECOMPOSITION IN GRADED MODULES gives on taking quotients a graded bijective homomorphism of degree i (n) of A/p onto a graded submodule of M . Consider now a homogeneous element b of A p'; then b 6 p since b is homogeneous. Let x be an element of M such that bx E N', and let (x i) l E Abe the family of homogeneous components of x. As N' is graded, bx, E N' for all i, hence bx, E N and, as b 6 p, we conclude that xi E N; as xi is homogeneous, X , E N', whence x E N' and the homothety with ratio b on M/N' is injective. Proposition 4 then follows from Proposition 3 applied to p' and M / N ' . IV PROPOSITION 2. Let A be a torsion-free commutative group, A a graded Noetherian &g of type A and M a gradedjinitely generated A-module of type A. There exists a composition series (Mt),,GiGn consisting of graded submodules of M such that for 0 Gi < n - 1 the graded module M t / M I + Iis isomorphic to a shifted graded module (Alp,) (k,), where pt is a gradedprime ideal of A and k, E A. It is sufficient to retrace the argument of 8 1, no. 4, Theorem 1 taking on this occasion to be the set of graded submodules of M with a composition series with the properties of the statement; we conclude using the Corollary to Proposition 1. 2. PRIMARY SUBMODULES CORRESPONDING TO GRADED PRIME IDEALS PROPOSITION 3. Let A be a torsion-free commutative group, A a graded Noetherian ring of type A, p a graded ideal o f A and M a graded A-module of type A reduced to 0. Suppose that for every homogeneous element a o f p the homothety of ratio a on M is nilpotent and that for every homogeneous element b o f A p the homothety of ratio b on M is injective. Then p is prim and the submodule (0) o f M is p-primary. - It suffices to show that A s s (M) = {p} (3 2, no. 1, Proposition 1). Let q be a prime ideal associated with M ; it is a graded ideal and it is the annihilator of a homogeneous element x # 0 of M (no. 1, Proposition 1). For every homogeneous element a of q, ax = 0 and hence the homothety of ratio a on M is not injective, whence a E p. Conversely, let b be a homogeneous element of p ; there exists an integer n > 0 such that bnx = 0, whence 6" E Ann(x) = q, and as q is prime, b E q. As p and q are generated by their respective homogeneous elements, p = q, which proves that A s s (M) c {p}. As M # {0},A s s (M) # o (3 1, no. 1, Corollary 1 to Proposition 2), whence A s s (M) = {p}. PROPOSITION 4. Let A be a torsion-free commutative group, A a graded Noetherian ring of type A and M a graded A-module of type A. Let p be aprime ideal o f A and N a submodule of M which is p-primary with respect to M . (i) The largest graded ideal p' o f A contained in p (Algebra, Chapter 11, 9 11, no. 3) isprime. (ii) The largest graded submodule N' of N is p'-primary with respect to M . - 3. PRIMARY DECOMPOSITION IN GRADED MODULES PROPOSITION 5. Let A be a torsion-free commutative group, A a graded Noetherian ring o f type A, M a graded A-module of type M , N a graded submodule o f M and Q = Qt a primary decomposition of N in M . (i) Let Q'be the largest graded submodule of M contained in Qt. Then the Qt are Qt. primary and N = tG tG (ii) I f the primary decomposition N = tG tG Qt is reduced, so is the primary decompo- sitin N = Qt andfor all i E I the prime ideals corresponding to Qt and Qtare equal. (iii) IfQ, corresponds to aprime ideal p which is a minimal elementofAss (M/N), Qt is a graded submodule of M. We have seen (no. 2, Proposition 4) that the Qt are primary with respect to M and N c Q" c Qt, which proves (i). Proposition 4 of no. 2 also shows that the prime ideal corresponding to Qt is the largest graded ideal contained in the prime ideal pt corresponding to Q, . If the decomposition N = (?f Q, is reduced, p, E A s s (M / N) for all i (3 2, no. 3, Proposition 4),hence is a graded ideal (no. 1, Proposition 1) and therefore p't = pt. Then (3 2, no. 3, Proposition 5) Ass(M/N) = {pi} (no. 3, Proposition 4), which proves that the decompo- tg tGQ;is reduced (3 2, no. 3, Proposition 4). Finally, if p if is a minimal sition N = element of A s s (M / N) , then pi = p, since p i is graded (no. 1, Proposition I), whence Qt = Ql by virtue of 5 2, no. 3, Proposition 5. We know (loc. cit.) that the homogeneous elements of p' (resp. N) are just the homogeneous elements of p (resp. N) . Let a be a homogeneous element of p; if x is a homogeneous element of M, there exists an integer n > 0 such that anx E N; as anx is homogeneous, anx E N'; as every y E M is the direct sum of a finite number of homogeneous elements, we conclude that there exists an integer q > 0 such that a 9 E N', so that the homothety with ratio a in M/N' is almost nilpotent. 284 285 EXERCISES EXERCISES composition series of a all of whose factor modules are isomorphic to A. (The existence of such a series would imply that a was isomorphic to a module A"; then necessarily n = 1, which is absurd.) 7 6. Let A be a ring and E an A-module. (a) Show that for a prime ideal p of A to belong to Supp(E), it is necessary and sufficientthat there exist a submodule F of E such that p E Ass(E/F) (to see that the condition is necessary, consider a submodule F of E of the form px, where x E E; to see that the condition is sufficient, use Proposition 7 of no. 3). (b) Suppose that A is Noetherian and E finitely generated. Show that for every prime ideal p E Supp(E), there exists a composition series (EJ0 0, a the ideal of A consisting of the elements with valuation > a and C the ring A/a. Then Spec(C) reduces to a point p; for all x # 0 in C, p x # 0, but for all h E p, there exists y # 0 in C such that hy = 0. In particular, Ass(C) = a, although Supp(C) = Spec(C) = {p). * 3. Let M be an A-module and N a submodule of M. Show that every prime ideal p E Ass(M/N) which does not contain Ann(N) is associated with M. Give an example of an ideal p belonging to Ass(M/N) but not to Ass(M) (take A to be an integral domain, M = A). 4. Give an example of a ring A such that M = A does not satisQ the conclusion of Theorem 1 of no. 4 (cf. Exercise 1 (b)). 5. Let A = K F , y1 be the polynomial algebra in two indeterminates over a commutative field K and the maximal ideal AX + AY of A. Show that Supp(a) = Spec(A) is infinite and Ass(a) = (0). Prove that there is no 286 a = Ann(M). (a) . . Show that, if a is prime, a is the least element of Ass(M). (Note that p.) p EA d M) (b) Show that every prime ideal associated with A/a is associated with M. (Note that if p is a prime ideal of A the annihilator of the class in A/a of an element a E A, then p = Ann(aM) and use (a).) (c) Let p, q be two distinct prime ideals of A such that p c q. Show that, if M = (A/p) 0 (A/q), then Ass(A/a) # &(MI. a = n8. Let A be a Noetherian ring, a an ideal of A, M a finitely generated A-module and P the submodule of M consisting of the x E M such that ax = 0. Show that Ass(M/P) c Ass(M) (note that for all x E M the annihilator of (Ax + P) /P is also that of QY and use Exercise 7 (a)). 9. Let A be a Noetherian ring and a an ideal of A. (a) For an ideal b ofA to satisfy a: b # a, it is necessary and sufficient that b be contained in a prime ideal p E Ass(A/a). (b) Let A be the polynomial algebra K[X, Y, Z] in 3 indeterminates over a field K. Let n = AX, m = AX + AY + AZ, a = n n m2.Show that there is a prime ideal p containing a such that a: p # a but which is not a prime ideal associated with A/a. 10. (a) Give an example of a Z-module M such that Ass(Hom,(M, M)) is not contained in Supp(M) (cf. Chapter 11,s4, Exercise 24 (c)). (b) Give an example of Z-modules E, F such that Ass(Hom,(E, F)) = 0, but Ass(F) n Supp(E) # 0 (take F = Z). 11. (a) Let A be a Noetherian ring and E an A-module. Show that the 287 IV ASSOCIATED PRIME IDEALS AND PRIMARY DECOhII'OSITION EXERCISES n canonical homomorphism of E to the product E, is injective (if N is p E AWE) the kernel of this homomorphism, show that Ass(N) = a). (b) Take A to be the polynomial ring K[X, Y, Z] over a field K ; let p1 = AX AY, p2 = AX AZ, which are prime ideals and the ideal p1p2. The set Ass(A/a) consists of pl, p2 and the maximal ideal m = p1 p2; show that the canonical homomorphism from E = A/a to E,, x E,, is not injective. + + + 12. Let A be a Noetherian ring and P a projective A-module. Show that, if, for all p E Ass(A), Pp is a finitely generated A,-module, then P is a finitely PEE(A) generated A-module (embed A in the product use Algebra, Chapter 11, 3 5, no. 5, Proposition 9). A, (Exercise 11) and 7 13. Let A be a Noetherian ring, E a finitely generated A-module, p, q two prime ideals of A such that p c q and a an element of q. Suppose that p E Ass(E) and that the homothety aE is injective. Show that there exists a prime ideal n E Ass(E/aE) such that p + Aa c n c q. (Replacing A by A,, we may assume that A is local with maximal ideal q. Let F # 0 be the sibmodule of E consisting of the x such that p x = 0. Show that the relation F c aE would imply F = aF and obtain a contradiction using Nakayama's Lemma.Then use Proposition 8 of no. 4.) 14. Let A be an integral domain, a # 0 an element of A and p an element of Ass(A/aA). Show that, for every element b # 0 of p, p E Ass(A/bA) (if c E A is such that the relation xc E aA is equivalent to x E p, show that there exists d E A such that xd E bA is equivalent to xc E aA). 15. Let A be a Noetherian ring, E a finitely generated A-module, F a submodule of E and m an ideal of A. For F to be closed in E under the m-adic topology, it is necessary and sufficient that p + m # A for every ideal p E Ass(E/F). (Reduce it to the case where F = 0, use Chapter 111, 3 3, no. 2, Corollary to Proposition 5 and apply Corollary 2 to Proposition 2 of no. 1 to an element 1 + m, where m E m.) 16. Let A be a Noetherian ring. For A to be isomorphic to a finite product of integral domains, it is necessary and sufficient that for every prime ideal p of A the local ring A, be an integral domain. (To see that the condition is sufficient, note first that it implies that that ring A is reduced; deduce that (0) =)f pt, where the pi (1 < i < n) are the minimal prime ideals of A. Show that, for i # j , we have p, + p, = A; for this, note that, if there existed a maximal ideal m containing pt + p,, the ring A,,, would not be an integral domain, using Corollary 3 to Proposition 2 of no. 1, and the Corollary to Proposition 5 of no. 2.) 288 7 17. Let A be a ring and M an A-module. A prime ideal p of A is said to be weakly associatedwith M if there exists x E M such that p is a minimal element of the set of prime ideals containing Ann(x) ; we denote by Ass,(M) the set of ideals weakly associated with M. Then Ass(M) c Ass,(M). (a) Show that the relation M # 0 is equivalent to Ass,(M) # 0. (b) For a E A to be such that aMis injective, it is necessary and sufficient that a belong to no element of Ass,(M) (note that, if a belongs to the radical of an ideal Ann(x) where x # 0 in M, there exists y # 0 in M such that a E Ann(y). To show that the condition is necessary, reduce it, by considering the ring A/Ann(x), to proving that in a ring A every element belonging to a prime ideal p which is minimal in the set of prime ideals of A is necessarily a divisor of 0 (Chapter 11, 3 2, no. 6 , Proposition 12).) For a E A to be such that aM is almost nilpotent, it is necessary and sufficient that a belongs to all the elements of Ass,(M). (c) If N is a submodule of M, then Ass,(N) c Ass,(M) c Ass,(N) u Ass,(M/N). (Note that, if p is a prime ideal, a 6 p, x E M such that ax E N and Ann(x) c p, then Ann(ax) c p.) (d) Let S be a multiplicative subset of A and CD the set of prime ideals of A not meeting S. Show that p E-S-lp is a bijection of Ass,(M) n CD onto Ass,(S-lM). (Observe that the inverse image under the canonical mapping A +-S-lA of the annihilator of an element XIS, where x E M, s E S, is the saturation with respect to S of A n n (x) .) (e) Let S be a multiplicative subset of A; show that, if N is the kernel of the canonical homomorphism M -+S-IM, Ass,(N) is the set of p E Ass,(M) which meet S and Ass,(M/N) the set of p E Ass,(M) which do not meet S. (TO prove the latter point, consider a prime ideal q which is minimal in the set of those containing Ann(y), where ij E M/N; note that, ify E ij and t E q, there exists c 4 q and an integer n > 0 such that ct"y E N (Chapter 11, 3 2, no. 6, Proposition 12); deduce first that q n S = 0.There exists s E S such that sct"y = 0; conclude that there can be no prime ideal q' # q such that Ann(y) c q' c 9.) (f) For a prime ideal ofA to belong to Supp(M), it is necessary and sufficient that it contain an element of Ass,(M). (g) Show that, if A is Noetherian, Ass,(M) = Ass(M). (h) If A is an absolutely flat ring, then Ass,(A) = Spec(A). (i) For every A-module E the canonicalhomomorphism from E to the product is injective; in other words, the intersection of the saturations of (0) in E with respect to the ideals p E Ass,(E) is reduced to 0. Generalize Exercise 12 similarly. P E Aasl(E) Ep 289 EXERCISES ASSOCIATED PRIME IDEALS AND PRIMARY DECOMPOSITION lv (j) Let M be a finitely generated A-module. Show that the minimal elements of the set of prime ideals containing a = Ann(M) belong to Ass,(M) (if is a system of generators of Myshow that such an ideal contains one of the Ann(x,)). Deduce that Ass,(A/a) is contained in Ass,(M) (if a prime ideal p is the annihilator of the class mod. a of an element a E A, note that p contains the annihilator of the submodule aM of M) ; show that Ass,(A/a), Ass(M) and the set of prime ideals containing a have the same minimal elements. 18. Let A be a ring and M an A-module. For an element c E A to be such that, for all a E A such that the homothety aMis injective, 6 , is an injective homothety for all b of the form a + Ac, where ~ E A it, is sufficient that c belong to the intersection of the maximal elements of Ass,(M) (use Exercise 17 (b)). Is this condition necessary? * 19. Let A be the ring of a valuation of height 2, I? its order group, I?l the unique isolated subgroup of I? distinct from (0) and I? and y > 0 an element of I? not belonging to rl. Let a be the ideal of those x E A such that v (x) 2 y, b the ideal of those x E A such that u(x) > y, E = A/a and F = A/b. Show that Ass(Hom,(E, F)) is distinct from Assl(F) n Supp(E). * §2 1. (a) Show that in the Noetherian polynomial ring A = Z[X] in one indeterminate over Z, the ideal m = 2A + AX is maximal and that the ideal q = 4A + Ax is m-primary, but is not equal to a power of m. (b) In the ring B = Z[2X, Xa, X3] c A which is Noetherian, show that the ideal p = 2BX BX2 is prime, but that p2 is not p-primary, although its radical is equal to p. (c) Let K be a commutative field and A the quotient ring of K[X, Y, 21 by the ideal generated by Z2 - XY; let x, y, z be the canonical images of X, Y, Z in A. Show that p = Ax + Az is prime, that p2 is not primary and that p2 = a n b2 is a primary decomposition of p2, where a = Ax and b = Ax Ay Az. + + + 2. In the example of Exercise 11 (b) of $ 1, show that a = m2 n p1 A pa is a reduced primary decomposition of a in A and that the saturation of a with respect to m is equal to a (and is therefore not primary). 3. Let A be a Noetherian ring and M a finitely generated A-module. Let Q be a p-primary submodule in M. The greatest lower bound of the integers n >, 1 such that pnM c Q is called the exponent of Q in M and denoted by e(M/Q). Let (Q J A s L be a family of p-primary submodules in M. For Q = Qh 290 to be p-primary in Myit is necessary and sufficient that the family (e(M/Qh))heL be bounded above; then e(M/Q) 2 e(M/Q,) for all h E L. 7 4. Let A be a Noetherian ring and M a finitely generated A-module. Let p be an element of Ass(M) and let &p be the set of submodules Q of M such that Ass(M/Q) = {p} and Ass(Q) = Ass(M) {p} (a set which is not empty by 1, no. 1, Proposition 4). We write e,(M) = inf e(M/Q) (Exercise 3). - Q€@p (a) Let n, be an integer >e,(M) and let $(no) be the subset of G, consisting of the submodules Q such that e(M/Q) < n,. Show that $(n,) has a least element Q(p, n,). (b) Let (np)pEAss(M)be a family of integers such that n, 2 e,(M) for all p E Ass(M). Show that the submodules Q (p , n,) corresponding to this family form a reduced primary decomposition of (0) in M said to be canonically determined by thefamily (n,). (c) If we take n, = e,(M) for all p E Ass(M), the primary decomposition consisting of the Q (p) = Q (p , e,(M)) is called the canonical primary decomposition of (0) in M. Let (0) = Q"p) be any reduced (Q p /()' for primary decomposition of (0) in M. Show that e(M/Q"(p)) < eM all p €Ass(M) and that, if e(M/Q(p)) = e(M/Q'(p)) for some p, then Q(p) c Q'(p) ("Theorem ofOrti2'). (c) Show that Q (p , n,) is the saturation of p " M ~ with respect to p (use 5 1, no. 2, Proposition 6) ; p is the least element of Supp(M/p"M). (d) Let S be a multiplicativesubsetofAnotmeetingaprimeidea1 p E Ass(M) andletQbeap-primarysubmoduleofM.Showthate(M/Q) = e(S-IM/S-lQ). Show that, if S is a multiplicative subset of A, @ the set of p E Ass(M) such that S n p = and N the saturation of{O}in M with respect to S, the Q (p , n,) where p E @ form the reduced primary decomposition of N in M canonically determined by the family (np)p)pE(D and the S - l Q (p , n,) where p E @ the reduced primary decomposition of (0) in S -lM canonically determined by the family (n,), *. Consider the particular case of canonical primary decompositions. pefi(M) 5. Let L be a finitely generated free Z-module and T a finite commutative group whose order is a power of a prime number p. Show that the canonical primary decomposition (Exercise 4) of (O} in M = L 0T is (0) = pnL n T, where n is the least integer 2 0 such that pnT = 0 (note that pnM = pnL). 6. In Exercise 5 of 4 1, (0) is primary in the A-module a relative to the prime ideal (0) of A. Show that the submodule AX of a is primary with respect to a relative to a prime ideal # {0}and that the submodule AXY of a is not primary with respect to a. 7. Let A be a Noetherian ring, M a finitely generated A-module and (Pt)lccGn a sequence obtained by arranging the elements of A.s(M) in any 29 1 N EXERCISES ASSOCIATED PRIME IDEALS AND PRIMARY DECOMPOSITION does not extend to the case where A is not an integral domain (take A = B/b, where B = K[X, Y] (K being a field), b = BX' + BXY). (d) If A is an absolutely flat ring (Chapter I, § 2, Exercise 17), the primary ideals of A are identical with the prime ideals of A. (e) Give an example of a Z-module M such that (0) is p-primary (for a prime number p) but that for no a ≠ 0 in Z is the homothety a_M nilpotent (cf. Chapter II, § 2, Exercise 18). order. Show that there exists a composition series (M_i) of M such that, for 0 < i < n − 1, M_i/M_{i+1} is primary in M, (use Proposition 4 and no. 3). * 8. Let A be a Noetherian ring, F a finitely generated A-module, F a submodule of E and m an ideal of A. Let P = p_i (A/E, F) Q(p) be a reduced primary decomposition of F in E. Show that the closure of F in E under the m-adic topology on E is equal to $\bigcap$ Q(p), where p is the set of P ∈ Ass(E/F) such that p + m ≠ A. (Consider first the case where F is primary in E and show that, if p + m = A, F is dense in E; proceed to the general case using Exercise 15 of § 1 and Chapter III, § 3, no. 4, Corollary 1 to Theorem 3). ¶ 9. Let A be a Noetherian ring and M an A-module. Show that, if N is a primary submodule in M, then N is also primary in M and the corresponding prime ideal is also the corresponding prime ideal. Does the same hold for N? Show that every p-primary submodule of M is the intersection of a finite family of primary submodules.

the polynomial domain K[X, yl in two indeterminates consider the subrings A = K[X4, Y4], A' = K[X4, X3Y, XY3, Y4];A is Noetherian and A' is a finite A-algebra. Let p = AY4, which is a prime ideal of A; show that m = AX4 + AX3Y + AXY3 + A'Y4 is an (immersed) prime ideal associated with the ideal PA' of A' but does not lie above p (note that m is the annihilator of the class of X2Ys in the ring A'/pA') (cf. 3 1, Exercise 26 hence integral over A[[X]], belonging to the field of fractions of A[[X]] but not belonging to A[[X]], so that A[[X]] is not integrally closed. 28. Let k be a field and A, the polynomial ring k[X,, Ynlnszin two infinite families of indeterminates. Let G be an infinite monogenous group (therefore isomorphic to Z) and let IS be a generator of B. G is defined as operating on A, by the conditions 5(Yn) = Y, and IS(X,) = X,+l for all n E Z. Let 3 be the ideal of A, generated by the elements Y,(X, - X,, 1) for all n E Z and let A be the quotient ring A,/3; as o (3) c 3, the group 9 also operates on A by passing to the quotient. Let S be the multiplicative subset ofA generated by the canonical images of the Y, in A, so that S consists of the elements invariant under G. Show that S-l(A9) # (S-lA)s. 29. Let k be a field of characteristic 2 2 , A the polynomial ring k[T] in one indeterminate and a, b two elements of k such that a # 0, b # 0 and a # b. Let K = k(T) be the field of fractions of A and L, M the extensions of K adjoining to K respectively a root of X2 - T(T - a) and a root of X2 - T(T - b) . Let B, C be the integral closures of A in L and M respectively, which are finitely generated free A-modules. Show that L @K M is a field, a separable finite extension of K, but that B @A C, which is canonically identified M, is not the integral closure of A in L & M. with a subring of L (4). 6. Define an increasing sequence of algebraic number fields K O= Q, K,, . . .,K,, . . . such that, if A, denotes the integral closure of Z in K,, p a prime number #2, K, is a quadratic extension of KnV1and there exists in A, a prime ideal P, lying above (p) such that there are in A,+1 two distinct prime ideals p, + ,, p; + lying above pn (observe that, in a finite field of characteristic 2 2 , there are always elements which are not squares). Let K be the union of the K, and A' the integral closure of Z in K ; show that there exists an infinity of (maximal) ideals of A' lying above the maximal ideal (p) of Z. , ~ 7 7. Let A be a Noetherian integral domain and A' its integral closure. Show that for every prime ideal p of A there exists only a finite number of prime ideals of A' lying above p. (Reduce it first to the case where A is a local ring with maximal ideal p; consider its completion A and the total ring of fractions B o€A and note that the field of fractions K of A is identified with a subring of B (Chapter 111, 9 3, no. 4, Corollary 2 to Theorem 3). Note that the spectrum of B is finite and therefore that in B there is only a finite number of idempotents which are orthogonal to one another. Then let C 3 A be a subring of K which is a finitely generated A-module and therefore semi-local. Note that the completion of C is identified with a subring of B; conclude by noting that fi is the product of a finite number of local rings, this number being equal to the number of maximal ideals of C). Generalize to the integral closure of a Noetherian ring in its total ring of fractions (reduce it to the case of a reduced ring). §2 e 1. Give an example of an injective ring homomorphism p : A -+ B such that B is finite A-algebra, the mapping =p: Spec(B) -+ Spec(A) is surjective but B is not a flat A-module. Conversely, give an example of a faithfully flat A-algebra which is finitely generated but not integral over A. 2. Let A be a ring such that Spec(A) is Hausdorff (Chapter 11, 3 4, Exercise 16). Show that, for every A-algebra B integral over A, Spec(B) is Hausdorff. 8. A local ring A is called unibranch if its integral closure is a local ring. (a) Let A be a local integral domain and K its field of fractions. For A to be unibranch, it is necessary and sufficient that every sub-A-algebra of K which is a finitely generated A-module be a local ring. (b) Show that, if the completion of a Noetherian local ring A is an integral domain, A is unibranch (if B is a finite A-algebra contained in K, show that the subring of the field of' fractions of A generated by B and A is isomorphic 3. Let A be a ring and A' a ring containing A and integral over A. For every ideal a of A, show that the radical of a is the intersection of A and the radical of aA'. Show that the latter is the set of elements x E A' satisfying an equation of integral dependence whose coefficients (other than the dominant coefficient) belong to a (note that, if y, z are two elements of A' satisfying such a n equation of integral dependence, so does y - 2). I 362 363 V INTEGERS to B @A A, using the flatness of the A-module A and the fact that B is contained in a finitely generated free A-module contained in K ; then use (a) and Chapter 111, 3 2, no. 13, Corollary to Proposition 19). 9. Let ko be a field and A' the polynomial ring ko[X,]n.N in an infinite sequence of indeterminates; it is an integrally closed domain whose field of fractions is K' = ko(Xn)nEN. Let B denote the k,-automorphism of A' such that 4 h n) = -Xzn + X2n+1s Q(Xzn+l)= & n + l for all n > 0; Q and the identity automorphism form a group 9 of automorphisms of A. Let A be the ring of invariants of 9 and let K be its field of fractions; K' is a separable extension of K of degree 2 and A' is the integral closure of A in K'. (a) Show that A' is an A-module admitting an inznite basis. (If k, is of characteristic 2 2 , show that, if we write Y, = X,, - +X,,+,, A is the subring of A' generated by the X,, + and the products Y,Y, for n > 0, m 3 0. If k, is of characteristic 2, A' is generated by the X,, + and the Xtn + XZnXzn+l for n 3 0.) (b) Let m' be the maximal ideal of A' generated by all the X, and let m = A n m'; show that m' = mA', that m' is the only ideal of A' lying above m and that the fields A/m and A'lm' are canonically isomorphic. (c) Let p' be the prime ideal of A generated by the X,,,, for n > 0 and let p = p' n A; let k, k' be the fields of fractions of A/p and A l p ' respectively; P'is the only prime ideal of A' lying above p. If k, is not of characteristic 2, k' k a separable extension of k of degree 2; if k, is of degree 2, k' is an infinite radicial extension of k. 10. (a) Let A' be the polynomial ring Z[X, yl in two indeterminates and let B be the automorphism ofA'leaving Y invariant and such that B(X) = - X ; Q and the identity automorphism form a group 9 of automorphisms of A' and the ring of invariants of 9 is A = Z[X2, Y]. Let p' be the prime ideal A'(Y - 2X), P = A n p'; the decomposition group g Z (p ') is reduced to the identity element. Show that A/p and A'/p' are not isomorphic (consider the tensor products of these rings with 2/22). (b) Let K be a field of characteristic 2 2 , A' the polynomial ring K[X, Yl and 9 the automorphism group of A consisting of the identity and the KIN-automorphism B of A' such that B(X) = - X ; the ring of invariants A of 9 is K[X2, Y]. Let p' be the prime ideal A'(X3 - Y) of A' and p = A n p'; the decomposition group gZ(p') is reduced to the identity element but A/p and A l p ' are not isomorphic. 7 11. (a) Let A be a local integrally closed domain, m its maximal ideal, K its field of fractions, K' a finite Galois extension of K, A' the integral closure 364 EXERCISES of A in K', m' a maximal ideal of A' lying above m, B = AZ(m') its decomposition ring and n = m' n B. For every integer k > 0, B = A + nk (argue as in Proposition 4). Moreover there exists a primitive element z of Kz (field of fractions of B) such that z E n; deduce that n n A[z] = mA[t]. (b) Show that, for every integer k, mkBnn A = mk. (If x E mkBnn A, note that there exists t E A[z] (where z is defined in (a)) such that t $ n and t x E mkA[z]; writing t = to + t,z + . . + t,-lzr-l (where r is the degree [KZ:K]), deduce that t,x E mk and to $ m.) (c) Suppose now that K is any Galois extension of K. Keeping the same notation as above, show that B = A + nk and mkBnn A = mk still

VALUATION RINGS IN AN ALGEBRAIC EXTENSION PROPOSITION 6. Let K be ajeld, v a valuation on K, A its ring, L an algebraic extension of K and A' the integral closure o f A in L. Let 23 be the set o f valuation rings on L which extend v and m' the set o f maximal ideals o f A'. Then the mapping V H m(V) n A' is a bijection of23 onto m' and m' HA:,. is the inverse bijection. Every maximal ideal m' of A' is such that m' n A is the maximal ideal of A is dominated by a valuation (Chapter V, 3 2, no. 1, Proposition 1) and ring V of L (which is therefore the ring of a valuation on L extending v) (3 1, no. 2, Corollary to Theorem 2). The field L is the union of a directed family of sub-extensions K, of L which are finite over K and it will suffice, in order to see that V = &,,to prove that V n K, = Air n K, for all a. Now, if we write = A'r n K,, & is the integral closure of A in K, and hence is the intersection of the rings of the valuations on K, which extend v and these rings V,, are finite in number and are the local rings (A@,;, of & (1 < i < n),where the mi, are the diqtinct maximal ideals of A& (no. 3, Remark) ;but m' n A& is one of x. 42 7 VI 3 8.7 VALUATIONS THE EXTENSION OF ABSOLUTE VALUES the mi, and V n K, is therefore equal to the corresponding local ring (&),,ia c A&, which completes the proof that V = 4,. Conversely, if V E 27, then A' c V ($3, no. 3, Proposition 6) and, if m' = m(V) n A', then m' n A = m, hence m' is a maximal ideal of A' (Chapter V, 3 2, no. 1, Proposition 1) and the above argument shows that V = 4.. Suppose first that there exists a valuation v on K with real values such that f (x) = e-u(x). There exists a valuation v' on L whose restriction to K is equivalent to v ($ 3, no. 3, Proposition 5). Then v' is of height 0 or 1 (no. 1, Corollary 2 to Proposition 1) and therefore may be assumed to have real values. The restriction of the mapping x H e-u'(x) to K is an absolute value equal to f and hence of the formfS with s > 0 (General Topology, Chapter IX, $ 3, no. 2, Proposition 5). We conclude that PROPOSITION 7. Let K be ajeld, L a quasi-Galois extension of K and f and f ' places ofL with values in the samejeld F. Suppose that the restrictions off andf' to K coincide. Then there exists a K-automorphism s of L such thatf' = f 0 s. Let A be the ring of the place of K the common restriction off and f '. The rings off andf' contain the integral closure A' of A in L (3 1, no. 3, Corollary 3 to Theorem 3) and hence (Chapter V, 3 2, no. 3, Corollary 1 to Proposition 6) there exists a K-automorphism s of L such that the restrictions o f f ' and f o s to A' are equal; if m' is the common kernel of these restrictions, m' n A is the maximal ideal of A', hence m' is a maximal ideal of A' and the places f ' and f o s coincide on the ring &,:but by Proposition 6 the only valuation ring of L dominating A:, is the ring A;, itself and hence the rings of the placesf'and f o s are the same. 0 COROLLARY 1. Let K be ajeld, v a valuation on K, L a quasi-Galois extension ofK and u' and u" two extensions o f u to L. Then there exists a K-automorphism s 0fL such that u" is equivalent to v' s. 0 Let f'and f be the places of K associated with v' and v"; replacing them if need be by equivalent places, it may be assumed that they both take their values in the algebraic closure of the residue field of v (no. 1, Proposition 1). Then there exists a K-automorphism s of L such that f "= f ' s (Proposition 7) ; thus U" is equivalent to v' o s by virtue of the correspondence between places and valuations ($ 3, no. 3). 'I 0 COROLLARY 2. Let K be a j e l d , f a place of K (resp. v a valuation on K) and L a radicial extension ofK. Then all the extensions off (resp. v) to L are equivalent. L is a quasi-Galois extension and its only automorphism is the identity. Corollary 2 therefore follows from Proposition 7 (resp. Corollary 1). PROPOSITION 8. Let K be ajeld, v a valuation on K, L a j n i t e quasi-Galois extension ofK ofdegree n and (u :) 6~ L 4 g a completesystem ofextensions o f v to L. Then e(vi/v) and f (v ~ / vhave) values e and f independent o f i . Then e f s < n. I f t h e integral closure in L of the ring A of v is ajnitely generated A-module, then e f s = n. This follows immediately from Theorems 1 (no. 3) and 2 (no. 5). 7. THE EXTENSION OF ABSOLUTE VALUES PROPOSITION 9. Let K be ajeld, L an algebraic extension of K and f an absolute value on K. Thenf can be extended to an absolute value on L. 428 x t+ - V ' (X) / S is an absolute value on L extendingf. Suppose now thatfis not ultrametric. Then K is identified with a subfield of C such that f (x) = lxls where 0 < s 6 1 ($ 6 , no. 4, Theorem 2). As C is algebraically closed, L is identified with a subfield of C and the absolute value x t+ lxls extendsf. PROPOSITION 10. Let K be ajeld,f an absolute value on K such that K is complete and not discrete with respect to f and L an algebraic extension of K. Then f can be extended uniquely to an absolute value f' on L and, ifL is ofjnite degree n, then f'b)= (f(NL/K(X))I1ln f o r all x E L. The existence off' follows from Proposition 9 and its uniqueness (over every finite sub-extension of L and therefore over the whole of L) from Lemma 2 of 3 6, no. 4. Letf ' be the unique extension o f f to the algebraic closure of K and n xi, where each xi suppose L is of finite degree n. We know that N,/,(x) = is a conjugate of x over K (Algebra, Chapter VIII, $ 12, no. 2, Proposition 4). I n view of the uniqueness off', f ' (x L) = f ' (x) for all i, whence the stated formula. PROPOSITION 11. Let K be a jield, f a non-ultrametric absolute value on K, R the completion of K with respect to f,f the continuous extension o f f to R and L a finite extension of K of degree n. (a) Letf' be an absolute value on L extending f ; let Lf,denote the completion ofL with respect tof' and let R be identiJied with the closure ofK in f&; then [f& : K] < n. (b) The absolute values on L extending f arejnite in number. Ifthey are denoted by f;,. . .,fs' and the completion of L with respect to ff' by ti,the canonical mapping n n R C& (10) L -+ L = l fLi is an isomorphism and 2 [L,:R] L = l = n. The proof is the same as that for the analogous assertions in Proposition 2 (no. 2). The references 3 7, no. 2, Theorem 1; 3 5, no. 2, Corollary to Proposition 4 429 VI THE MODULUS FUNCTION ON A LOCALLY COMPACT FIELD VALUATIONS Remark (3). If k is isomorphic to R,Proposition 12 shows that all the completions 2, of L (in the notation of Proposition 11) are isomorphic to one another. Thus, with the notation of Remark 2 above, either rl = n and r, = 0, or rl = 0 and 272 = n. should be replaced by the following 3 7, no. 3, Theorem 2; Topological Vector Spaces, Chapter I, 5 2, no. 3, Corollary 1 to Theorem 2. Observe that two extensions off to L which define the same topology are equal (General Topology, Chapter IX, 3 3, no. 2, Proposition 5) . Finally, as f is not ultrametric, K is of characteristic 0 and hence the Jacobson radical of I?i @, L is zero. Remarks (1) Proposition 11 (b) shows that every com osite extension of R and L over and that these are composite K is isomorphic to one of the completions extensions no two of which are isomorphic. (2) We know that the completions and are isomorphic to R or C (3 6, no. 4, Theorem 2). If R is isomorphic to C, so is for all i and (10) shows that the number of extensionsf,' is equal to n. If R is isomorphic to R (for example if K = Q), let rl (resp. r,) denote the number of indices i such that is isomorphic to R (resp. C); then (10) may be written: E, a e, e, e, rl + 2ra = n. (11) PROPOSITION 12. Let K be afield, f an absolute value on K, L a quasi-Galois extension o f K and f ' and f w two extensions off to L. Then there exists a K-automorphism s ofL such that f " = f ' s. 0 Iff is ultrametric, Corollary 1 to Proposition 7 (no. 6) shows that there exists a K-automorphism s of L such thatf" andf' s are equivalent absolute values; then there exists a real number a > 0 such thatf"(x) = (f'(s(x)))a for all x E L. Iff is not improper, take x E K* such that f (x) # 1, which shows that a = 1. Iff is improper, so aref' andf" (Corollary 2 to Proposition 1, no. 1) and s may be taken to be the identity automorphism. Iff is not ultrametric, there exist Q-isomorphisms u', u" of L onto subfields of C and real exponents a' > 0, u" > 0 such that f '(x) = Iu'(x) and 0 la' f"(X) = lu"(x)la" for all x E L (5 6, no. 4, Theorem 2). Taking x = 2, it is seen that a' = a". The restrictions of u' and U" to K extend by continuity to isomorphisms u1 and u2 of I? onto R (resp. C). Then u2 o i,' is an automorphism of the valued field R (resp. C) and is therefore the identity (resp. the identity or the automorphism c : 1: -+ 4). Replacing if need be u' by c o u', it is seen that the restrictions of U' and u" to K may be assumed to coincide. Identifying K with a subfield of C by means of this common restriction, u' and u" are K-isomorphisms of L onto subfields of C. As L is a quasi-Galois extension of K, there exists a K-automorphism s of L such that un = u' s; since a' = a", we deduce immediately that 3 9.1 9. APPLICATION: LOCALLY COMPACT FIELDS 1. THE MODULUS FUNCTION ON A LOCALLY COMPACT FIELD Let K be a locally compact field (not necessarily commutative). Recall that the function mod (or mod,) has been defined (Integration, Chapter VII, 9 1, no. 10, Definition 6) on K as follows: mod,(O) = 0 and for x # 0 in K, the number mod,(x) is the modulus of the automorphism y t+ xy of the additive group of K. PROPOSITION 1. IfK is a locally compactfield, the function mod, belongs to V(K) (5 6, no. 1). Moreover: (i) If s > 0 is such that (mod,)s = g is an absolute value, then g defines the topology on K. (ii) If K is not discrete and mod, is an ultrametric absolute value, there exists a normed discrete valuation v on K whose ring is compact and whose residue field isjnite with q elements, so that mod, = q-v. The topology on K is defined by v. This follows from 5 6, no. 1, Proposition 1, 5 5, no. 1, Proposition 2 and Integration, Chapter VII, 5 1, no. 10, Propositions 12 and 13. PROPOSITION 2. Let K, K' be two (not necessarily commutative) locally compactfields such that K is a topological subfield o f K' and K is not discrete. Then: (i) K' is afinite dimensional l g t (resp. right) vector space over K. (ii) I f K is contained in the centre o f K', then, for all x E K'. (1) mod,,(x) = modK(NK',K(X)). As K is a complete valued field which is not discrete, assertion (i) follows from Topological Vector Spaces, Chapter I, 5 2, no. 4, Theorem 3; assertion (ii) is just Integration, Chapter VII, 5 1, no. 11, Proposition 17. COROLLARY 1. Every locally compactfield whose centre is not discrete is ofjnite rank over its centre. The centre Z of a locally compact field K is closed in K and therefore locally Compact. COROLLARY 2. Let K' be a locally compactjeld and K a closed subjield of K' (neither necessarily commutative). I f K ' is a lgt (resp. right) vector space ofjnite dimension n over K, then 0 f" = f ' o s . 430 (2) mod,.(x) = (mod,(x))' for all x E K. 43 1 vf VALUATIONS STRUCTURE OF LOCALLY COMPACT FIELDS I n general it is known that in a (left or right) vector space of finite dimension n over K, the homothety with ratio x E K has modulus equal to (mod,(x))n; it suffices to apply this to K'. Let us write 0-2 C u = j = o s-fasjpr. Then u e (q - l) a = - a (mod. m2) since p . 1 ~ m we; conclude that u is also a uniformizer for v ; moreover (3) s-1mP' = 2. EXISTENCE OF REPRESENTATIVES PROPOSITION 3. Let K be a (not necessarily commutative) locally compactjeld which is not discrete and whose topology is d&ed by a discrete valuation v; let A be the ring and m the ideal of v and let us write Card(A/m) = q = p f (p prime). Then, there exists a system of representatives S o f A/m in A and a uniformizer u for v such that 0 E S, S* = S n K* is a cyclic subgroup o f K* and u - Su = S. Moreover, every element o f A i whence we deduce that u - l Su = S. Finally, for all xnE A there exists a unique sequence (si) (i E N)such that si spi, where si E S. + LEMMA 1. Let x , y be two permutable elements o f A such that x - y E mj (j 2 1); then xp" - yp" E mj+"f o r every integer n 2 0. 3. STRUCTURE OF LOCALLY COMPACT FIELDS By induction on n, it is reduced to proving the lemma for n = 1. Then - y' = (x The completions R and Qp of the field Q with respect to the non-improper absolute values on Q (p any prime) are locally compact. On the other hand, for every power q = p f of a prime number p , the field Fq((T))of formal power series over the finite field F, with the valuation defined in 4 3, no. 4,Example 3 is locally compact: for the maximal ideal of the valuation ring F,[[T]] is generated by T ; we know that this ring is complete with the (T)-adic topology (Chapter 111, 9 2, no. 6, Proposition 6) and, as the residue field F, is finite, Proposition 2 of 5 5, no. 1 proves our assertion. Conversely: - y)(x"-l + xp-zy + . . . + yp-1); the second factor is a sum ofp terms congruent to one another mod. m and, as A/m is of characteristic p , p . 1 E m in A and hence xP-1 +~ p - 2 (mod. mn z) , where t' is a uniquely determined element of S. Then x = siui and the family (si) satisfying this relation and such that si E S for all i is determined uniquely. We shall use the following lemma : x p S 2 1 i=o E for all i and x = i = O siui (mod. mn+l) for all n 2 0: it is immediate by induction on n, every element t of m n + l satisfying a relation of the form t = t'un+l m OD may be written uniquely in theform 4 9.3 + 2 ~. . . + yp-1 E m ; whence xp - yp E mf+l. We know that the multiplicative group (A/m)* is a cyclic group with q - 1 elements (Algebra, Chapter V, 3 11, no. 1, Theorem 1) ;let x be a representative in A of a generator of this group; then XQ - x E m, whence, by Lemma 1, xq"+' - xq" E ml+," since xq and x are permutable. This proves that (tp")n20 is a Cauchy sequence in A; as A is compact and hence complete, this sequence has a limits in A which obviously satisfies s = x (mod. m) and SQ = s. As s # 0, fl-l = 1, more precisely s is aprimitive (q - 1)-th root ofunity in A. Clearly the set S consisting of 0 and the powers sj (0 < j < q - 2) is a system ofrepresentatives of the classes of A mod. m and is invariant under multiplication in A. NOWlet a be a uniformizer for v and consider the inner automorphism Y t-+ a-lya of K; it maps A to itself, m to itself and therefore, taking quotients, it defines an automorphism of the field A/m; it is known (Algebra, Chapter V, 3 11, no. 4,Proposition 5) that such an automorphism is of the form z Hzpr, where 0 < r < f - 1. Then a-lsja = sjp' (mod. m) for 0 < j < q - 2; as a E m and s 6 m, this implies that s-fasfp' = a (mod. m2). THEOREM 1. Let K be a (not necessarily commutative) locally compactjeld which is not discrete. (i) IfK is ofcharacteristic 0 and mod, is not an ultrametric absolute value then K is isomorphic to one of thefields R,C or H. (ii) If K is of characteristic 0 and mod, is an ultrametric absolute value, K is an algebra ofjnite rank over a P-adicjeld Q,. (iii) I f K is of characteristic p # 0, it is isomorphic to afield with centre ajeld o f formal power series F,((T)) (where q is a power o f p) and ofjnite rank over its centre. (i) It follows from Ostrowski's Theorem (3 6 , no. 4,Theorem 2) that K is a topological field isomorphic to an everywhere dense subfield of R,C or H and, as K is complete, it is isomorphic to R, C or H. (ii) Let A be the ring of the absolute value mod, and m its maximal ideal. We know that A/m is a finite field (3 5 , no. 1, Proposition 2) and hence the absolute valup induced by mod, on Q has a finite residue field, which is only I 432 433 VI possible if it is equivalent to a p-adic absolute value (5 6, no. 3, Proposition 4) ; the closure of Q in K is therefore isomorphic to Q, and is contained in the centre of K since the latter is closed in K ; we conclude using Proposition 2 of no. 1. (iii) The second assertion follows from the first and the Corollary to Proposition 2 of no. 2. TO show the first assertion, note that mod, is necessarily an ultrametric absolute value (5 6, no. 2, Corollary to Proposition 3) ;in the notation of the proof of Proposition 3 of no. 2, the centre Z of K consists of the elements which commute with both s and u ; but by virtue of (3), U-QSUQ 2 m s,T' E F,[[T]] to the COROLLARY 2. Every locally compactjeld is connected or totally disconnected; ;f it is connected, it is isomorphic to R,C or H. If the topology on a field K is defined by an ultrametric absolute value, K is totally disconnected with this topology. Remark. Let s be an integer > 0; the subfield F,((Ts)) = L of K = F4((T)) is closed in K and e(K/L) = s andJ(K/L) = 1. It is therefore seen that there are closed subfields L of K which are not discrete and such that e(K/L) (and afortiori the degree [K: L]) is arbitrarily large (contrary to what happens for locally compact fields of characteristic 0, where every locally compact subfield L of such a field K necessarily contains R or Q, and therefore [K : L] is bounded). 10. EXTENSIONS OF A VALUATION TO A TRANSCENDENTAL EXTENSION 1. THE CASE OF A MONOGENOUS TRANSCENDENTAL EXTENSION LEMMA1. Let K be ahfield,v a valuation on K, I? its order group, J?' a totally ordered = c f a,Xj (a, E r'. There exists a unique valuation w on K(X) K), w(P) = inf,(v(a,) + jE). By Proposition 4 of 5 3, no. 2, it suffices to show that the formula I w(7 (1) a,x,) = inG(v(a,) + j ~) defines a valuation on the ring K[X]. As + 6,) +jE 2 inf(v(a,), v(b,)) +jE = inf(v(a,) +jE, v(b,) + j E) , it follows that I I I s'u' is a bijective homomorphism of the ring F,[[T]] onto the ring element A, whence immediately the conclusion. COROLLARY 1. Every locally compactjeld which is not discrete is ofjnite rank over its centre. 434 such that,for P v(a, so that u p E Z and we conclude that Z is not discrete. As Z is locally compact, we may confine our attention to the case where K is commutative. The sub-F,algebra F,[s] in K is then a finite field since sq-l = 1 and obviously ya = y for every element of this field, which is therefore identical with S and isomorphic to F, since S c F,[s] has q elements. Since the sum of two elements of S is in S, m group containing r and E an element of = SqP' = $3 the mapping which maps each formal power series 3 10.1 THE CASE OF A MONOGENOUS TRANSCENDENTAL EXTENSION VALUATIONS w(P + Q) 2 inf(w(P), w(Q)) (2) for P, Q i n K[X], equality holding if w(P) # w(Q). We show that (3) w P Q) = w(P> + w(Q) c 2, for P = a,Xj and Q = b,Xj. Let i (resp. k) be the least of the integersj such that v(a,) + j [(resp. v(b,) + j E) attains its minimum; let a (resp. p) denote this minimum. Forj,j' in N, in P Q ; then c = + zz whence w (PQ) 2 a + ~ (6 +j'E ~) + 2 a p, p by (2). Consider now the term cX1 of degree i w(a,brXj+') = v(a,) +jE + +k a,+nbk-n;by the choice of i and k, the element W(at+nbk-nXL+k) = U(at+,) + (i + n) t + V(bk-,,) f (k - n)E takes its minimum value a + p once and once only with n W(CX'+~) = a + p, whence, by (l), w(PQ) = a = 0; hence + p = w(P) + w(Q). PROPOSITION 1. Let K be ajeld, v a valuation on K, I? its order group, I" a totally ordered group containing I' and (an element of I" such that the relations nE E F, n E Z imply n = 0. Then there exists a unique valuation w on K(X) with values in I" and extending v such that w(X) = E. The residuejeld of w is equal to that of v and its order group is the subgroup I? + ZE .f I". c We show first the uniqueness of w. Let P = a,Xf be an element of K[X]. f Then w(a,Xj) = v(a,) +jE, which shows that the monomials a,Xf such that a, # 0 have distinct values for W. It follows that w(P) = inf,(v(a,) +jE), which shows both the uniqueness of w on K[X] (hence also on K(X)) and the fact that the wder group o f w is F ZE.It is further seen that, if P # 0, we + 435 VI THE RATIONAL RANK OF A COMMUTATIVE GROUP VALUATIONS + may write P = aXn(l u) , where aEK*, n E N , U E K (X)and w(u) > 0; every element R # 0 of K(X) can therefore be written in the form R = bX"(1 which proves our assertion. Remark. I t should not be thought that the two types of extensions of v to K(X) which we have just met are the only ones; there may exist a third type of extension, where r'/r is a torsion group and k' a (not necessarily finite) algebraic extension of k. This third type is not necessarily provided by the procedure described in Lemma 1 (cf. 8 3, Exercise 1). + u'), + where b E K*, n E Z, u' E K(X) and w(u') > 0; then w (R) = v(b) nE,, hence w (R) = 0 if and only if v(b) = 0 and n = 0; thus, when w(R) = 0, R and b are congruent modulo the ideal of w, which shows that the residue field of w is equal to that of v. Finally the existence of w follows from Lemma 1. 2. THE RATIONAL RANK OF A COMMUTATIVE GROUP DEFINITION 1. The rational rank vector Q-space G gZQ. PROPOSITION 2. Let K be afield, v a valuation on K, I' its order group and k its residue fild. There exists a unique valuation w on K(X) extending v such that w(X) = 0 and the image t $X in the residuefield k' o f w is transcendental over k. The order group of w is equal to that of v and its residuejeld is k (t) . To show the uniqueness of w, it will suffice for us to show that, if P is a non-zero element of K[X], then w(P) = = 2 a,Xj f inf,(v(a,)). 7 PROPOSITION 3. Let G be a totally ordered Commutative group and H a subgroup G. Ifh(G) and h (H) denote the heights ofG and H (9 4,no. 4),then the inequality 0 = inf,(v(aj)). + h(G) < h(H) r(G/H) (5) holdr. I n fact, let Go c GI c . . . c G, be a strictly increasing sequence of isolated subgroups of G. It is necessary to establish the inequality We now show the existence of w. The formula w(P) = inf,(v(a,)) (for P = ajXj) defines a valuation w on K(X), by virtue of Lemma 1, and w obviously has the same order group as v. Then w (X) = 0. We show that the canonical image t of X in the residue field k' of w is transcendental over k : if 7 E j t j = 0, where c, Ek for all j , then, denoting by a, (T / (T ajXj) + n - 1 < h(H n G,-l) r(Gn-l/(H n Gn-1)). Then we distinguish two cases: (a) H n G,-l = H, in other words H c G,-l. Inequality (7) may be written (7) bjX'), where c, a,, b, are in K, 0 and v(bj) 2 0 for allj, one of the v(a,) and one of the v(b,) being zero; then w (R) 2 0 if and only if v(c) 2 0; denoting bythe canonical homomorphism of the ring of w onto k', ~(aj2) i 436 < h (H) + r(G/H). = 0. Suppose n 2 1 and let us argue by induction on n. Applying the induction hypothesis to the group G,-l and its subgroup H n G, - we obtain Cj = 0 for all j . We show finally that k' = k (t) : every element R of =c n (6) It is obvious for n a representative of Zj in the ring of v, w (T a,XJ) > 0; whence v(aj) > 0 for all j, hence K(X) may be written R G is the dimension of the r(G) = r(G') + r(G/G'). (4) residue field k' is G j t j ; as t is transcendental over k and one of the u, is nonzero, this image is non-zero, whence = of a commutative group This dimension may also be defined as the least upper bound (finite or infinite) of the cardinals r such that there exist r elements of G which are linearly independent over Z (Algebra, Chapter 11, 9 7, no. 10, Proposition 26). The rational rank of G is zero if and only if G is a torsion group. For a subgroup of an additive group R",the notion of rational rank coincides with that defined in General Topology, Chapter VII, fj 1. In the rest of this paragraph, we shall denote by r(G)the rational rank of the commutative group G. If G' is a subgroup of G, then (since Q i s a flat Zmodule) we have the additive equation We may divide P by an element of K* and suppose that v(a,) 2 0 for all j and that one of the v(a,) is zero. As w (X) = 0, P then belongs to the ring of w ; writing (z, for the canonical image of a, in k , the canonical image of P in the w(P) 8 10.2 1 (8) Now G/G,,- n- < h(H) + r(Gn-JH) + 1. is a totally ordered group not reduced to 0; it is therefore not a 437 VI THE CASE OF ANY TRANSCENDENTAL EXTENSION VALUATIONS + torsion group and r (G / G n - l) 2 1. Whence by (4),r(G/H) 2 r(G,,-l/H) 1. Substituting in (8), we certainly obtain the desired inequality (6). (b) H n G,-l # H. As H n G,,-l is an isolated subgroup of H , we conclude that h (H) > h(H n Gn-l) 1. On the other hand, obviously r(G/H) > r(G,,-J(H n G,,-l)). Substituting in (7), we again obtain (6). + COROLLARY.For every totally ordered commutative group G, h(G) < r(G). 3 10.3 order group and residue field of v (resp. v'). We shall write: d (K'/K) = dim. al, K' = transcendence degree of K' over K ; s(v'/v) = dim. al, k' = transcendence degree of k' over k ; r(v'/v) = r(r'/r)= rational rank of I"/I', We set H = (0) in Proposition 3. if the right-hand sides are finite; otherwise, we shall make the convention that d (K ' / K) = +co (resp. s(u'/v) = +a,r(v'/v) = +a). PROPOSITION 4. Let G be a totally ordered commutative group. Suppose that G is jnitely generated and that h (G) = r (G) . Then G is isomorphic to Zr(G)ordered lexicographically. THEOREM 1. Let xl, . . .,x, be elements ofthe ring ofv' whose canonical images 2, in k' are algebraically independent over k and y l , . . .,y, elements o f K' such that the canonical images Ofthe v'(y,) in r'/rare linearly independent over Z. Then the r + s elements x l , . . .,x,, y,, . . .,y, of K' are algebraically independent over K ; the restriction of v' to K (x l , . . . ,x,, y l , . . . , y,) admits k(El, . . . , Es) as residuejield and Let us write r = r(G) = h (G) . If r = 0, then G = (0). If r = 1, the structure of finitely generated commutative groups shows that there is an isomorphismj of G onto Z (Algebra, Chapter VII, Fj 4,no. 6, Theorem 3). Now Z has only two total orderings compatible with its group structure, namely the usual ordering and its opposite. Hence j or -j is an isomorphism of the ordered group G onto Z with the usual ordering. Suppose how that r > 2 and let us argue by induction on r. Let H be an isolated subgroup of G of height r - 1. Then r(H) + r(G/H) = r (formula (4)),r(H) > h (H) = r - 1 and r(G/H) 2 h (G / H) = 1 (Corollary to Proposition 3), whence r(H) = r - 1 and r(G/H) = 1. The induction hypothesis shows that H is isomorphic to Z'-l ordered lexicographically and the case r = 1 shows that G/H is isomorphic to Z . As Z is a free Z-module, H is a direct factor of G (Algebra, Chapter 11, Fj 1, no. 11, Proposition 21). The following lemma then shows that G is isomorphic (not canonically) to the lexicographical product H x (G/H), which completes the proof. LEMMA 2. Let H be an isolated subgroup Of a totally ordered commutative group G. I f H is a directfactor of G, the ordered group G is isomorphic to the group (G/H) x H ordered lexicographically. Let j be an isomorphism of (G / H) x H onto G such that j (0, x) = x for all x E H andj(y, x) belongs to the coset y of H. As (G/H) x H is totally ordered, it amounts to showing t h a t j is increasing (Set Theory, Chapter 111, Fj 1, no. 12, Proposition 11). Let (y , x) be an element > O of (G/H) x H ordered lexicographically. If y > 0, the coset of H containing j (y , x) is an element > 0, whencej(y, x) > 0, for, otherwise, y < 0 (Fj 4,no. 2, Proposition 3). Ify = 0 and x > 0, thenj(y, x) = x 2 0. Hencej is certainly increasing. 3. THE CASE OF ANY TRANSCENDENTAL EXTENSION I n this no. we shall use the following notation : K is a field, K' an extension of K , v a valuation on K , v' an extension of v to K , I'and k (resp. I" and k') the 438 r + z v y y l) + . . . + zU'(y,) as order group. + Our assertion is obvious if r + s = 0. We argue by induction on r s. If r' < r, s' < s and r' + s' < r + s, the induction hypothesis shows that the hypotheses of Theorem 1 hold if K is replaced by K (x l , . . . , x,, yl,. . .,yr.) and the families (x l , . . .,xs), (y l , . . .,yr) by (x,, 1, . . .,xS),(y,, 1, . . .,yr). The problem is therefore reduced to one of the two following cases: (a) There is an element x in the ring v' such that 2 is transcendental over k ; then it is necessary to show that x is transcendental over K and that the restriction of v' to K (x) admits k (x) as residue field and r as order group. (b) There is an element y in K' such that the relations nv'(y) E r and n E Z imply n = 0; it is necessary to show that y is transcendental over K and that the restriction of v' to K (y) admits k as residue field and I? Zv'(y) as order group. Now Proposition 1 of Fj 8, no. 1 shows that x (resp. y) cannot be algebraic over K . The other assertions of (a) (resp. (b))follow immediately by Proposition 2 (resp. Proposition 1) of no. 1. + COROLLARY 1. The inequality s(u'/u) + r(v'/v) < d (K ' / K) (9) holds. Further, fi K' is a finitely generated extension Of K and equality holds in (9), then r'/ris ajinitely generated Z-module and k' is afinitely generated extension of k. Let r and s be natural numbers such that r < r(v'/v) and s < s(u'/v) ;we show that r + s < d (K / K) and this will prove (9). By hypothesis there exist elements xl, . . .,x,, y l , . . .,y, of K' which satisfy the hypotheses of Theorem 1. 439 VI VALUATIONS EXERCISES They are therefore algebraically independent over K , which shows the inequality r s < d(K'/K). If K' is a finitely generated extension of K , d (K'/K)is finite, hence s(u'/u) and r(v'/u) are also finite; we denote them bys and r. There exist elementsx,, . . .,x,, y l , . . .,yr of K' which satisfy the hypotheses of Theorem 1. If r + s = d (K ' / K) , these elements form a transcendence basis of K' over K and K' is therefore a finite algebraic extension of K" = K(xl, . . . , yr). Let F" and k" be the order group and residue field of the restriction of u' to K". By Theorem 1, r"/ris a finitely generated Z-module and k" is a finitely generated pure extension of k. On the other hand, as K' is a finite algebraic extension of K , F'/r is a finite group and k' is a finite algebraic extension of k" (3 8, no. 1, Lemma 2). This proves the corollary. + 3' COROLLARY 2. Let h and h' be the heights o f v and u'. Then (10) By Proposition 3, h' s(u'/v) + h' < d (K ' / K) + h. < r(v'/v) + h. COROLLARY 3. Suppose that K' is ajnitely generated extension of K, that r is isomorphic to Zh (ordered lexicographically) and there is equality in formula (10). Then r ' is isomorphic to Zh' (ordered lexicographically) and k' is a jnitely generated extension of k. If there is equality in (lo), there is equality in (9), whence the fact that k' is a finitely generated extension of k and that I" is a finitely generated Z-module. whence Further, comparing (9) and (lo), it is seen that h' - h = r(r'/r), h' = r(r')and Proposition 4 (no. 2) then shows that I?' is isomorphic to Zh' ordered lexicographically. COROLLARY 4. Suppose that v is improper (in which case k = K) . Then (11) h(r') + d(k'/K) y,in particular, v' < r (r ') + D(k'/K) < d(K'/K). is of height 1, then d (k ' / K) < d (K / K) - 1; (12) further, ;fK' is ajnitely generated extension OfK and there is equality in (12), then u' is a discrete valuation and k' is ajnitely generated extension of K . I t is a series of special cases of Corollaries 1, 2, 3. 1. Let K be a field; for every subring A of K let L(A) denote the set of local rings A, of A where p runs through the prime ideals of A (these local rings being identified with subrings of K) . (a) For a local subring M of K to dominate a ring A, E L(A), it is necessary and sufficient that A c M; the local ring A, dominated by M is then unique and corresponds to the prime ideal p = m(M) n A. (b) Let M, N be two local subrings of K and P the subring of K generated by M u N. Show that the following conditions are equivalent: (a) There exists a prime ideal p of P such that m(M) = p n M, m(N) =p n N. (p) The ideal a generated in P by m(M) u m(N) is distinct from P. (y) There exists a local subring Q o f K dominating both M and N. If these conditions are satisfied, M and N are called related. (c) Let A, B be two subrings of K and C the subring of K generated by A u B. Show that the following conditions are equivalent: (a) For every local ring Q C K containing A and B, A, = B,, where p = m(Q) n A, q = m (Q) n B. (P) For every prime ideal r of C, A, = B,, where p = r n A, q = r n B. (y) If M E L(A) and N E L(B) are related, they are identical. (6) L(A) n L(B) = L(C). (Use (a) and (b)). 2. For an integral domain A to be a valuation ring, it is necessary and sufficient that every ideal of A be irreducible (Algebra, Chapter 11,3 2, Exercise 16). 3. Show that every valuation ring is coherent (Chapter I, 3 2, Exercise 12). 4. Let K be a field and 5 a set of valuation rings of K totally ordered by inclusion. Show that the intersection of the rings belonging to 5 is a valuation nng of K . 440 441 VI VALUATIONS EXERCISES - 5. Let K be a field, A a integrally closed subdomain of K with K as a field of fractions and (&) a family of valuation rings of K whose intersection is A. Then ifL is an extension of K, the integral closure of A in L is the intersection of the valuation rings of L which dominate one of the &. - - 16. Let R be a ring and A a subring of R such that S = R A is non-empty and the product of two elements of S belongs to S. (a) Let a, a' be two elements of A and s, s' two elements of S such that sa E A and S'U' E A. Show that one of the two elements sa', s'a belongs to A. Deduce that the set p1 of elements a E A for which there exists s E S such that sa E A is a prime ideal of A. (b) Show that the set po of a E A such that sa E A for all s E S is a prime ideal o f R and A; it is the greatest ideal of R contained in A and po c pl. (c) The set n of elements x E R such that there exists s E S for which sx = 0 is both an ideal of R and an ideal of A and n c po. (d) The ring A is integrally closed in R. (e) If R is a field, A is a valuation ring of R, po = (0) and p1 is the maximal ideal of A. 17. Let R be a ring. An ordered pair (A, p) consisting of a subring A of R and a prime ideal p of A is called maximal in R if there exists no ordered pair (A', p') consisting of a subring A' of R and a prime ideal p' of A' such that A c A', A' # A and p' n A = p. (a) For every subring B of R and every prime ideal q of B there exists an ordered pair (A, p)), maximal in R, such that A 3 B and q = p n B. (b) For an ordered pair (A, p) to be maximal in R, it is necessary and A, there exist a finite family of elements ct E p sufficient that, for all s E R (1 < i < n) such that the element b = cls + c2s2 + . . . + c,s" belongs to A p (use Chapter 11, 5 2, no. 5, Corollary 3 to Proposition 11). (c) Show that, if the ordered pair (A, p) is maximal in R, the product of two elements of R A belongs to R A. (Ifs, s' are in R A and ss' = UEA, consider the least integers n, m such that there exists ct E p (1 < i < n) for - - - - - - p and c; E p (1 < j < m) for which 6' = c;s'f E A - p; supposing for example n >/ my consider the product bb' E A - p and obtain a contradiction from the definition of the integer n.) (d) Under the hypotheses of (c), we write S = R - A; show that the ideal which b = cist E A 7 p1 of A consisting of the a E A such that there exists s E S for which sa E A is contained in p (use (b)). Afortiori the ideals po of A consisting of the a E A such that sa E A for all s E S is contained in p (Exercise 6 (b)). We write A' = Alp,, p' = p/po and R' = R/p,; the ordered pair (A', p') is then maximal in the 442 integral domain R and, for all non-zero a' E A', there exists s' E S' = R' A' such that s'a' E S'. (e) Let (A, p) be a maximal ordered pair in the integral domain R such that, A such that sa E S. We write for all non-zero a E A, there exists s E S = R So = S u (1) and denote by R, the ring of fractions SolR; the canonical homomorphism R + R, is injective and therefore identifies R with a subring of Ro. Show that R, is a field identified with the field of fractions of R. Let (B, q) be a maximal ordered pair in Ro such that B 3 A and q n A = p. Show that B n R = A; in other words, A is the intersection of R and a valuation ring of R, and p is the intersection of A and the maximal ideal of this valuation ring. (f) Let KObe a field, A, the polynomial ring K,[X], B the ring of formal power series A,[[Y]] and R the ring of fractions By consisting of the formal power series Y-hf(Y), wherefE B and h 2 0. Let P be the prime ideal YB of formal power series without constant term, A = KO+ p, which is a subring of B. Show that A is the intersection of R and a valuation ring C of the field of fractions K of R and p the intersection of A and the maximal ideal of C; moreover, the field of fractions of A is equal to that of R and every a # 0 in A is of the form s-ls', where s, s' are in S = R A. However, the ordered pair (A, p) is not maximal in R. I - 18. Given a ring A, a polynomial P(X1,.. ., X,) with coefficients in A is called dominated if it is of the form Xu + cDXo,where p < a in the product ordered set N" for all p such that cB # 0. In a ring R, a subring A is called puravaluative if, for every dominated polynomial P E AIXl, . . .,X,] (any n), P(sl,. . ., s,) # 0 for all elements s, E R A (1 < i < n). (a) Show that, if A is paravaluative in R, the product of two elements of S = R A belongs to S. (b) Let A be a subring of a ring R such that the product of two elements of s = R A belongs to S ;let po be the prime ideal of A and R consisting of the u E A such that sa E A for all s E S (Exercise 6 (b)). For A to be paravaluative in R, it is necessary and sufficient that Alp, be paravaluative in R/p,. (c) Let R be a ring and h: R -+ R' a ring homomorphism. If A' is a para- - - - -1 valuative subring of R', A = h (A ') is paravaluative in R. Deduce that, if (A, p) is a maximal ordered pair in R (Exercise 7), A is paravaluative in R (use (b) and Exercise 7 (d) and (e)). (d) Let R' be a ring and R a subring of R'. If A is a paravaluative subring of R, show that there exists a paravaluative subring A' of R' such that A' n R = A. (If S = R A and So = S u { l}, consider the ring T' = S, lR' and the canonical homomorphism h: R' + T'. Let B be the subring of T' generated by h (A) U (h (S)) - I and b the ideal of B generated by (h(S))-l. Show - 4.43 VALUATIONS EXERCISES that b # B; consider a maximal ordered pair (A', p") in T' such that B c A" S-lB contains subfields K,, K; respectively isomorphic to K and K' and is the ring generated by K1u K;. Show that, if q is the kernel of h, there exists a prime ideal p in B such that p c q and p n S = 0 and show that F may be taken as the field of fractions of S-lB/S-lp.) VI and b c p" and take A' = hiA).) Conclude from this that, if R is

2, Exercise 18)); then M* is Artinian (resp. Noetherian). (d) Let o(M*, M) denote the topology (on M*) of pointwise convergence on M (K/A being given the discrete topology). Show that, if N is a submodule of My a(No, M/N) is the topology induced on No by o(M*, M) and that o(M*/No,N) is the quotient by No of the topology o(M*, M). (For the second point, note that, if P is a submodule of M such that N c P, the dual of P/N is identified with No/Po). If M = lim Ma, the topology o(M*, M) is the inverse limit of the ---f topologies o(M*,*, Ma). (e) The topologies o(K, K) and a(A, K/A) are the x-adic topologies; the topologies u(A/xhA,A/xhA) and o(K/A, A) are the discrete topologies. Deduce that for every A-module M, the module M* with o(M*, M) is linearly compact (Chapter 111, 3 2, Exercise 15; consider M as a quotient module of a free A-module). (f) Let M, N be two A-modules; for every homomorphism u : M -+ N, from N* to M* such that let tu denote the homomorphism Hom(u, lK,A) 1 ('u (4 (4 = (u (XI 1 for all x E M and all w E N*; show that t~ is continuous for the topologies o(N*, N) and o(M*, M). If u is the endomorphism x H xx of M, t~ is the endo-1 morphism w H xw of M*. For every submodule P of M, (u(P))O = tu (PO). fi 10. The hypotheses and notation are the same as in Exercise 9. (a) If M is a discrete topological A-module, show that M is a torsion module. If further M is linearly compact, show that M is Artinian (if N is the kernel of the endomorphism x H xx, observe that N is linearly compact and discrete and can be considered as a vector (A/xA)-space; then use Exercise 20 (d) of Chapter 11, § 2). (b) Deduce from (a) that every linearly compact topological A-module is strictly linearly compact (Chapter 11, 5 2, Exercise 19). (c) The topological to& dual of a topological A-module M is the submodule M' of the algebraic toric dual M* consisting of the continuous homomorphisms 458 from M to K/A (the latter being given the discrete topology). If the topology on M is linear (Chapter 111, 3 2, Exercise 14) and N is a closed submodule of M, show that the topological toric dual of M/N is identified with No n M' and that of N with M'/(No n M') (to determine the dual of N, note that, for every continuous homomorphism u from N to K/A, there exists an open submodule U of M such that u (x) = 0 in N n U, then use Exercise 9). (d) For a topological A-module M of finite rank, the topological toric dual M' is equal to the algebraic toric dual M* (reduce it the case of modules of rank one). (e) Let M be a Hausdorff topological A-module whose topology is linear; show that for all x # 0 in M, there exists u E M' such that u (x) # 0 (note that there exists an open submodule U of M such that x 6 U) ;in other words, the canonical mapping M --f (M')* is injective. Dedum that, if N is a closed submodule of M, No n M' is dense in No with the topology o(M*, M) (use (d)), and consequently N = M n (NO n M')O in M**. Show that M is dense in (M')* with the topology o((M')*, M'). (Observe that, if U is an open submodule of MyM/U is Artinian by (a) and therefore Uo is Noetherian (Exercise 9 (c)) and deduce the identities of the topologies considered on M ; complete with the aid of (e).) (f) Let M be a linearly compact topological A-module; show that the canonical injection M -+ (M')* is a bijection and that the topology on M (identified with (M')*) is equal to o(M, M'). (g) Let M, N be two topological A-modules whose topologies are linear; for every continuous homomorphism u : M -+ N, % (N') c M' and tu is also used (by an abuse ofnotation) to denote the linear mapping from N' to M' with the same graph as k. If M and N are Hausdorff, show that the restriction to M of "('u) coincides with u (M and N being respectively considered as canonically embedded in (M')* and (N') ; moreover, for every submodule Q o f N, (~ ' (Q)) o n M' = t u (~ 0) (use (el). (h) Let M be a linearly compact A-module; deduce from (g) and Exercise 9 (f) that for M to be torsion-free, it is necessary and sufficient that M' be divisible and that for M to be divisible, it is necessary and sufficient that M' be torsion-free. §6 T[1. Every element z of thep-adic field Q, (p a prime number) may be written z0 Uniquely as ph Ckpk,where h E z, co # 0,0 < ck < p for all k 2 0 ('>-adic expansion" of 2). (a) Show that, in order that z E Q, it is necessary and sufficient that there 459 VI I VALUATIONS exist two integers m 2 0, n 2 1 such that c k + , = ck for all k that, if z = a/b E Qwhere b is not divisible by#, then c EXERCISES show that, for all i, a, = A,a. Conversely, if b is an ideal # 0 of A and 6, = A,b, then b = 6, (use Theorem 1 of no. 2). m. (Observe n U - b k=O c k f k = U,+lp"+' §* 1. Let K be a field and A = K[[X, Y,Z]] the ring of formal power series in three indeterminates over K ; let v' (resp. u") be the valuation on A with values in the group Z x Z ordered lexicographically, such that v'(X)= (1,0), v'(Y)= (0, l) , v' is improper in K[[Z]] (resp. v"(X)= (1, 0),U" is improper in K[[Y]], v"(Z)= (0, 1)). Let G be the automorphism ofA leaving invariant K and X and such that c(Y) = Z, ~ (2=) Y ;if B is the subring of A consisting of the elements invariant under G and E (resp. F) the field of fractions of A (resp. B), the valuations v' and v" (extended canonically to E) have the same restriction v to F, F is complete with the topology defined by v and E is a quadratic extension of F; the two valuations v', vw on E are dependent but not equivalent. where a,+, is an integer and the sequence lakl (ordinary absolute value) is bounded). (b) Suppose that the increasing sequence (k,,) of integers k such that ck # 0 is such that lim. sup(k,+Jk,) = +CO. Show that z is transcendental over Q. n- m (For x E Q ,let 1x1 and 1x1, respectively denote the usual absolute value and a p-adic absolute value. Suppose that P E Z[X]is an irreducible polynomial such 00 that P(z) = 0; if z, = p" z o C k p k , show that lP(zn)/(t - z,)lp tends to a limit # 0 as n tends to co,using Taylor's formula; then obtain a contradiction from the hypothesis considering the usual absolute values lP(zn)I.) + 2. Let D be a non-commutative field of characteristic #2 and Z its centre. Suppose that every commutative subfield K of D containing Z is of degree < 2 over Z. (a) Show without using Lemma 1 that [D: Z] = 4. (Let a E D Z be such that u2 E Z and let ~ (x =) uxa-l for all x E D ; note that D decomposes as a direct sum of two vector subspaces over Z, D + and D - such that G (X) = x on D +, a(#) = - x on D - ;note also that D + is a subfield of D and D - is a l-dimensional vector space over D + ; finally, show that D + cannot be distinct from - W).) (b) Show that D is a quaternion algebra over Z. (Form a basis of D over z with the aid of (a).) §7 2. With the hypotheses and notation of Proposition 1 of no. 1, let q be a prime ideal of B; show that B, is a valuation ring. 460 < i < n) be painvise independent valuation rings of a field K 4. For all i, let a, be an ideal i ~ I # O of A, and write a = (la,; 2. Let KObe the field obtained by adjoining to the 2-adic field Qzthe roots of all the polynomials X2" - 2 ; let v be the unique valuation on KOextending the 2-adic valuation and let K be the completion of KOwith respect to V. Show that the polynomial X2 - 3 is irreducible in K[X] ; let K' be the field of roots of this polynomial and let v' be the extension of v to K'; then n = [K': K] = 2, 1 I , e(v'/v) =f(u'/v) = 1. 3. Let k be the field of rational functions F(X,JnEN in an infinity of indeterminates over the prime field F, and let K = k(U, V) be the field of rational functions in two indeterminates over k. W i I 1. Let (+ J I E I be a family of places of a field K taking their values in a finite number of fields; suppose further that for some x E K, the set of C + ~ (X)is finite. Show that there exists a polynomialf(X) of the form (1) of no. 1 such that f (x) # 0 and that the element z = f (x) - l enjoys the following properties: (i) +,(x) = co implies C+~(XZ) = 0 and +&(z)= 0; (ii) &(x) # 00 implies + , (x t) # co and &(z) # 0. (Same proof as for Lemma 1). 3. Let A, (1 and let A = I , (a) Show that the element P(U) = n = O XKUnp of the field of formal power series k((U)) is not algebraic over the field k(U) of rational functions. The mapping F(U, V) H F(U, P(U)) of k[U, V] to k((U)) can be extended to an isomorphism of K onto a subfield of k ((U)); the restriction to this subfield of the valuation on k((U)) equal to the order of the formal power series ($3, no. 3, Example 3) is a discrete valuation v on K, whose residue field is k. (b) Let K' be the algebraic extension K(V1'P) of K so that [K': K] = @; if 0' is the unique valuation on K' extending u, show that e(v'/v) =f(v'/v) = 1. The ring of the valuation v' is therefore not a finitely generated module over the ring of the valuation v. 4. Let k be a field, K = k (X , Y) the field of rational functions in two indeterminates over k and v the valuation on K with values in the group Z x Z ordered lexicographically, such that v(X)= (0, l) , v(Y)= (1,O). Let K' be the field K(1, let K" be the field of invariants of BD and A" = K" n B; show that the order group of vlK" is equal to r : for this, use the Approximation Theorem (3 7, no. 2, Theorem 1) in order to prove that, for all 463 VI VALUATIONS x E K", there exists y E K" such that u(y) = V(X) and u(y,) = 0 for the conjugates y, of y with respect to k, distinctfrom y; then 9 may be replaced by YD and the induction hypothesis may be applied. If gD= 9, let B, be the valuation ring of K' generated by the a.B, where Q E 9 : let K' = K(B,) be its residue field, x : B, -+ K'the canonical homomorphism, = x(B) a valuation ring of K' and V the corresponding valuation on l?' such that u = V 0 x in B,, so that the order group of 6 is a subgroup of the order group A of v; if A, = A/& and ~ 3 A: -+ A, is the canonical homomorphism, u, = v o u is a valuation on K' corresponding to B, and invariant under 9. By taking quotients, 9 defines a group of automorphisms of K';let Jf be the kernel of the canonical homomorphism 9 -+ 3; show that Jy' c gZand deduce that, if Jf # {e}, 3 may be replaced by 91.N and the induction hypothesis may be applied. Suppose finally that .N = {e}; let A, = K n B, and w o be the restriction of u, to K ; show that the order group of w, is A, and that x(A,) = is the field of invariants of @ (cf. no. 1, Lemma 2) ; if z i is ~ the restriction to of and P its order group, A, is canonically isomorphic to r/P.On the other hand, the group gz(p(B)) is the canonical image of W(p(B)) in 3; observe that # 3 and that the induction hypothesis may therefore be applied to prove that is equal to the order group of the restriction of V to KZ.) (c) Let gT= ST(p(B)) be the inertia group of p(B) (Chapter V, 5 2, no. 2) and let KT denote the subfield of K' consisting of the invariants of gTand BT the ring of the valuation induced on KTby u, which is equal to B n KT; recall that, if k and k' are the residue fields of A and B, the residue field kT of BTis the greatest separable extension of k contained in the quasi-Galois extension k' of k and that $P/59Tis canonically isomorphic to the group of k-automorphisms of k' (or kT) (Chapter V, 5 2, Theorem 2 and Proposition 5). Let uT be the restriction of u to KT; show that the order group of uT is also equal to I7 (apply Lemma 2 of no. 1 to the extension KT of Kz). sD rz 9. Let K be a field, L a finite algebraic extension of K, u' a valuation on L, A' its ring, u the restriction ofv' to K and A = A' A K its ring. (a) Suppose that A is Henselian (Exercise 6) ; show that the product e(v'/u)f(v'/u) divides n = [L: K] and that the quotient n/e(v'/v)f(v'/v) is a power of the characteristic exponent of the residue field k of v. (Reduce it to the case where L is a Galois extension of K ; use Exercises 6 (e) and 7 and Chapter V, 5 2, Theorem 2 and Proposition 5.) (b) Suppose further that n is not divisible by the characteristic exponent of the residue field k of u and that f (u'/u) = 1. Show that, for every integer m equal to the order of an element y of the group I'u,/l?uthere exists x E L such that the class of u ' (x) mod. PVis equal to y and xm E K. 7 10. 464 Let w be the 2-adic valuation on the 2-adic field Q 2 ; on the field of EXERCISES rational functions Q2(X) consider the discrete valuation u extending w and such that u(ao + a,X + . f . + anXn) = inf(w(a,)) f (8 10, no. 1, Lemma 1) ;let K be the completion of Q2(X)with respect to this valuation and let its valuation also be denoted by u. Let L be the splitting field of the polynomial (Y2 - X)2 - 2 in K[Y] and let u' be the unique valuation on L extending u. Show that [L: K] = 8, e(v'/v) = 4,f(v'/v) = 2; if k (resp. k') is the residue field of u (resp. u'), k' is a radicial extension of k of degree 2; show that there exists no sub-extension E of L such that [E : K] = 2 for which the residue field of the restriction of u' to E is equal to k'. (Of necessity E = K(&), where cc E K would not be a square in K but such that cc = X (mod. 2) ; express &with the aid of a suitable basis of L over K(&) and observe that there exists in K(&) no element whose square is congruent to X mod. 2.) T[11. Let K be a field, L a finite Galois extension of K and 9 its Galois group. Let u be a valuation on L with residue field k and order group r; suppose that u is invariant under 9 and that the restriction vlK has the same residue field k as u, so that 9 = gz = gT(notation of Exercise 8). (a) Let x E L*, Q E 9.Show that x-'o(x) is a unit for u, that its image E.,(x) in k* depends only on the valuation U(X) and the class of Q modulo the commutator group 9' of 9 and that there is thus defined a Z-bilinear mapping x v(K*). (also denoted by c) (9/9')x l? -+ k*, which is equal to 1 on (9/9') (b) For all Q E 9, let +(a) be the homomorphism r/v(K*) -+ k* mapping c.,(x) to U (X) for all x E L*; thus there is defined a homomorphism +: 9 -+ Hom, (r/v(K*), k*). + Show that, if$ is the characteristic exponent of k, the kernel N of has order a power of p. (In the contrary case, there would exist a cs # e in N and a prime number q # p such that 09 = e; for some integer x in L K, write G (X) = x + y, where u(y) > u (x) , and calculate &(x) to obtain a contradiction.) Deduce that 9 is a solvable group. (c) Suppose that n = [L: K] is prime to p ; show that is bijective, that e(L/K) = n and that, if v is the lcm of the orders of the elements of 9, k* contains the v-th roots of unity. (Use (b) and Lemma 2 of no. 1.) - + 7 12. Let K be a field, u a valuation on K, A the ring of the valuation u and r its order group. (a) Letf(X) = a,X" ulXn-l + . . . + a, be a polynomial in A[X] such that u(uo) = 0, all ofwhose roots belong to K ; let xi (1 < i < r) be these distinct roots and let k, be the order of multiplicity of xi (1 < i < r) . Let + g(X) = box" + b,X"-' +. . . + bn = bo(X - ~1). . . (X - yn) 465 VI EXERCISES VALUATIONS another polynomial in A[X] such that u(b,) = 0 and the y h belong to K. Show that there exists A, E l? such that v(xt - x j) < A, for every ordered pair of distinct indices i , j and, for all A 2 A,, there exists p 2 A such that the relations v(a, - 6,) 3 p for all i imply that, for 1 < i < r, there are exactly k, indices h such that v(xi - y,) 2 A. (First evaluate U(f(Yh)) in two ways to show that necessarily u(x, - y,) 2 A for a t least one i ; then evaluate E Hxt has no cluster point with respect to Zl, the mapping 2 I-+ x t is bounded on a subset of U.) (b) Letf be a non-constant polynomial in K[X]. Show that, if 4 Hf (x,) converges .~ " to 0 in K with respect to U, 5 ~--fxt converges in R (decomposef into factors in an algebraic extension of K and use (a)). (c) Suppose that K is algebraically closed in R.Then the mapping x ~ f (x) of K to itself is closed (use (b)). Deduce that, if g is a rational function in K(X) and B is a bounded closed subset of K, then g(B P) (where Pis the set of poles of g in B) is closed in K. (d) Suppose that the algebraic closure of K is a radicial extension of K. Then show that R is algebraically closed. (Apply (b) to an algebraic closure -~ of R and a polynomialSE R[X] ; use also Exercise 12 (a).) - a t suitable points z E K.) If further b, = a, except for i = n - 1, show that, so long as h, is sufficiently large, the y, are all distinct (evaluate f'(Yh)lf(Yh) assuming that y, is not a simple root of 9). (b) Suppose henceforth that K is the algebraic closure of a subfield K Osuch that A, = A n K O is Henselian. Suppose that the polynomial f belongs to A,[X] and is irreducible and separable over KO.Let z E K be such that u(z - v,) > v(2 - x,) for a l l j # i; then show that K,(x,) c K,(z). (Show that z - xi is equal to all its conjugates with respect to K,(xJ.) nA (c) Suppose thatfE Ao[X] is separable and letf = uo be the decom1=1 position off into monic irreducible polynomials in K,[X] (which belong in fact to &[XI, cf. Chapter V, tj 1, no. 3, Proposition 11). Show (in the notation of (a)) that, if p is taken sufficiently large, the decomposition of g into monic n r irreducible factors in K,[X] can be written as b, g,, where, for all i, g, is of i=1 the same degree asA (a decomposition said to be "of the same type" as that of f)and further the splitting fields ofA and g, are the same for all i. (Show first that g is separable; consider then a finite Galois extension of K Ocontaining the roots off and g and consider the way in which the Galois group of this extension permutes these roots; finally use (b).) (d) Give a n example wherefis irreducible but not separable and where, for all p A,, there exists a polynomial g(X) = b o x " + blXn-' +. . . + b, E Ao[X] where v(ai - b,) 2 p for all i, which is not irreducible (take KOsuch that K # KOand K is a radicial extension of KO). fi 13. (a) Let K be a field and u a non-improper valuation on K. Let E be a set filtered by an ultrafilter U and 4 ~--fxt, 4 Hy, two mappings of E to K with the topology Yv.Show that, if the mapping 5 Hxty, converges to 0 in K with (Observe that, if respect to U, so does one of the mappings Hx,, E HY,. 466 fi 14. (a) For a field K to be Henselian with a valuation v, it is necessary and sufficientthat K be the greatest separable algebraic extension of K contained in R and that I? be Henselian. (To see that the condition is necessary, use Exercise 12 (b) ; to show that it is sufficient, observe that, to verify condition (H) of Chapter 111,tj 4, Exercise 3, we may confine our attention to the case where Pis separable over K, noting that, if Q i s an irreducible factor of P in R[X] such that Qpe belongs to K[X], then Q i s a g.6.d. of P and Qpe in R[X] .) Consider the case where v is of height 1 (cf. Exercise 6 (b)). (b) Deduce from (a) that there exists in the p-adic field Q, a countable subfield which is Henselian with the p-adic valuation. (c) Give an example of a field K which is Henselian with a discrete valuation which is not complete and such that R is a finite radicial extension of K (cf. Chapter V, tj 1, Exercise 20). T[15. (a) Let K be a field, vl, v2 two independent valuations (3 7, no. 2) on K and K1, K, the completions of K with respect to v1 and v, respectively. Let L,, L, be two fields such that K c L, c K1, K c L, c K,, which are Henselian (with the extensions by continuity of u1 and v, respectively). Let g, E Ll[X], g, E L2[X] be two separable polynomials with the same degree n. Show that there exists a polynomial h E K[X] which, in L,[X], has the same type of decomposition (Exercise 12 (c)) as g, (i = 1,2). (Reduce it to the case where g1 and g, are in K[X] and are monic; consider the polynomial angl(X/4 + b"g,(X/a) - X", where vl(a) < 0, v,(a) > 0 is arbitrarily large and vl(b) > 0 is arbitrarily large.) (b) Deduce from (a) that, if K is Henselian with vl, the algebraic closure of L, is radicial over L, and K2 is algebraically closed (take g, to be irreducible and g, E K[X] to be the product of n distinct factors of prime degree). (c) Deduce from (b) that, if K is Henselian with v1 and v,, the algebraic closure of K is radicial over K. 467 VI VALUATIONS EXERCISES (d) Show that, if K is Henselian with a discrete valuation u, the algebraic closure of K cannot be radicial over K and therefore K cannot be Henselian with any valuation independent of u (use Algebra, Chapter V, 3 11, Exercise 12). be the associated bilinear form. Show that 2v((@(x, y)) 2 u(Q(x)) deduce that 16. Let K be a Henselian field with a valuation u of height 1. If L is an inznite separable algebraic extension of K, show that L cannot be complete with the valuation extending u (and also denoted by v). (Form a sequence (x,) of elements of L such that the degree np of x p with respect to K tends to co and v(xpfl - x,) is strictly greater than the valuations of the differences between x, and its conjugates with respect to K; show that the sequence (x,) is a Cauchy sequence which cannot converge in E, using Exercise 12 (b).) 7 20. Let K be a field of characteristic f 2 which is Henselian with a valuation v ; let 5 H be an involutive automorphism of K such that u(A for every ordered pair (i , j) , then @ and @' are equivalent. (Argue as in Algebra, Chapter IX, 3 6, Exercise 6, using Exercise 14 (a) above.) (b) Suppose that 5 -2 is the identity (hence 0 is a symmetric form) and that the valuation u is discrete, normed and such that v(2) = 0; let x be a uniformizer for u. Show that 0 is characterized, up to equivalence, by its index v and by two symmetric bilinear forms Yl, Y, of index 0 on vector spaces k' and P respectively, where k is the residue field of u and r + s = n - 2. (With the aid ofa Witt decomposition, reduce it to the case where @ is of index 0; with the aid of Exercise 19, show that, for all i 2 0, the set M, of x E E such that u (@ (x , x)) > i is a module over the ring A of the valuation u. Show that, if x E M,, y E then u (@ (x , y)) 2 i + 1, and, by taking quotients, symmetric bilinear forms can therefore be derived from @ on the vector k-spaces M,/M, and MJM,. Use Exercise 6 (c) of 0 3 and the fact that the equation E2 = c(has a solution in A for a = 1 (mod. x) .) Consider the case where k is finite (cf. Algebra, Chapter IX, 3 6, Exercise 4). + 7 17. Let K be a Henselian field with a valuation u which is not algebraically closed, and L a subfield of K such that [K: L] is finite. Show that under these conditions L is Henselian with the restriction of u. (In the contrary case, there would exist two extensions u l , u2 of vlL to an algebraic closure R of K such that the restriction of u1 and u2 to a finite algebraic extension L' of L would not be equivalent. Deduce that there would exist on a suitable finite quasi-Galois extension K' of L containing K, two valuations v;, vh which are not equivalent and for which K' would be Henselian; using Exercise 15 (c), show that, if E = LP-m (p being the characteristic exponent of R), E # R but Q would be a finite extension of E ; complete the argument with the aid ofalgebra, Chapter VI, 3 2, Exercise 3 1.) 7 18. Let K be a Henselian field with a valuation u, k the residue field of u and suppose that every finite algebraic extension of k is cyclic over k (which is for example the case when k is finite). Let A be the ring of u andf E A[X] a monic polynomial such that, iff (X) = (X - a l) . . .(X - a,,), where the ai belong to an algebraic closure of K, the element D = (ai - a,)z of A ("discriminant" off) issuch that v(D) = 0. LetA (1 < j < s) be the irreducible factors of the canonical image fof f in k[X] and let r, be the degree of&. Show that the Galois over K of the splitting field ofJ considered as a group of permutations of the a, is generated by a permutation c which decomposes into cycles of respective lengths rl, r,, . . . ,r, (observe that there exists only a single extension of k of given degree, up to a k-isomorphism). Deduce that, for D to be a square in A, it is necessary and sufficient that n - s be even ("Stickelberger's Theorem"; examine under what condition D is invariant under 0). 19. Let K be a Henselian field with a valuation u. Let E be a finite-dimensional vector space over K and Q a non-degenerate quadratic form on E such that the relation Q (x) = 0 implies x = 0. Let @(x,Y) = Q(x 468 + Y) - Q(x) - Q(Y) + v(Q(y)); ~ (Q (x+ Y)) 2 i n f (~ (Q (~)~)(,Q (Y))) - 2 1. Let K be a field, u a discrete valuation on K, A the ring of u, x a uniformizer of u and k the residue field of u. (a) Let P, R be two polynomials in A[X], P being monic, and suppose that: (1) deg(R) < h.deg(P), where h 2 1 is an integer; (2) the canonical image P o f P in k[X] is irreducible. Show then that, if the polynomial Q = Ph xR is reducible in R[X], necessarily h > 1 and P divides the canonical image of R in k[X]. Deduce that, for a given monic irreducible polynomial r (X) E k[X] and a given integer h 2 1, there exists a separable irreducible polynomial QEA[X] such that its canonical image Q is equal to rh. (b) Let k' = k(a) be a n algebraic extension of k of degree m and h an integer 2 1. Show that there exists an algebraic extension L of K of degree hm such that there is only a single valuation u' (up to equivalence) on L extending u, that e(u'/u) = h, f (u ' / v) = m and that the residue field of u' is isomorphic to k' (use (a)). + 469 VI 22. (a) If there exists a discrete valuation on a field K, show that the algebraic closure of K is infinite over K. (b) Let K be a finitely generated extension of a field KO.Show that, if K is not algebraic over KO,there exists a discrete valuation u on K such that ~ (x=) 0 on KO. 39 1. (a) Let K be a field (not necessarily commutative) and F a locally compact topology on K compatible with the ring structure on K ; show that 9-is compatible with thejeld structure on K. (Use the Theorem of R. Ellis (General Topology, Chapter X, 3 3, Exercise 25) or argue directly reproducing the proofs of Integration, Chapter VII, 3 1, no. 10 and those of Proposition 1 of this paragraph.) (b) Give an example of a locally compact topology on a commutative field K, which is compatible with the additive group structure on K, but not with its ring structure. (Take K to be the field of fractions of a compact integral domain A (A being for example a ring of formal power series k [[X ,Y]], where k is finite) and take as fundamental system of neighbourhoods of 0 in K the neighbourhoods of 0 in A.) 7 2. (a) I n a space R" (n >/ 2), let U be a non-empty open set with non-empty complement; show that the frontier of U contains a non-empty perfect set (cf. General Topology, Chapter I, 3 9, Exercise 17). (b) Deduce from (a) that, if A is an everywhere dense subset of R" which meets every perfect set in R", A is convex. (c) Show that there exists in C an everywhere dense subfield K which is connected and locally connected and is a pure transcendental extension of Q (apply General Topology, Chapter IX, 3 5, Exercise 18 (b) and (c), constructing K by transfinite induction, using (b) and the method described in Set Theory, Chapter III,§ 6, Exercise 24). Deduce that there exists a subfield K' 2 K of C which is (algebraically) isomorphic to R, connected and locally connected. (d) Show, using (c), that there exists on C the topology of a connected and locally connected space, which is compatible with the field structure and for which the completion of C is an algebra over C which is the direct composition of two fields isomorphic to C. 3. Let K be a totally disconnected non-discrete locally compact commutative field; let A be the ring of the absolute value mod, on K and let U be the group of units of A. For every integer n > 0, let ,,U denote the group of n-th roots of unity in K and Un the subgroup of U consisting of the n-th powers of the elements of U. Show that, if n is prime to the characteristic of K, U" is an open subgroup of U and that Card(U/U") = mOdK(n).Card(,U) 470 EXERCISES VALUATIONS (use Exercise 14 of Integration, Chapter VII, 3 2 and Commutative Algebra, Chapter 111, 3 4, no. 6, Corollary 1 to Theorem 2 to show that, if m is the maximal ideal of A, the image under x t+ x" of 1 mk is 1 n .mkfor k sufficiently large). + + 4. (a) Let K be a commutative field and u a valuation on K such that K is Henselian with u (3 8, Exercise 6). Suppose further that K and the residue field k of u are of characteristic 0. Show that there exists a subfield KOof the ring is an isomorA of u such that the canonical mapping A -+ k, restricted to KO, phism of KOonto k. (Let H be a subfield of A such that the image of H under the canonical mapping is an isomorphism onto a subfield E of k ; show that, if E # k, there exists Q H in A such that the subfield H(a) of K is contained in A and is canonically isomorphic to E@), where ii is the class of a in k; distinguish two cases according to whether E is algebraic or transcendental over E.) (b) Suppose further that u is a discrete valuation and that K is complete with respect to v ; deduce from (a) that K is isomorphic to the field of formal power series k((T)) . 5. (a) Suppose that K is a commutative field, u a valuation of height 1 on K such that K is complete with respect to u and A the ring of v ; suppose further that the residue field k of u is perfect and of characteristic p > 0. For every element 5 E k* and every integer n, let x, be an element of the class Ep-" in A; show that the sequence (x:") is a Cauchy sequence in A whose limit is independent of the choice of the x, in the classes EP-". If this limit is denoted by +({), show that 4 is the unique isomorphism u of the multiplicative group k* to the multiplicative group K* such that, for all E E k*, u(E) is an element ofA belonging to the class E. (b) If K is also of characteristic p, show that 4, extended to k by +(O) = 0, is an isomorphism of the field k onto a subfield of K. Deduce a new proof of Theorem 1 (iii) of no. 3. (c) Suppose that K isjnite. Show that, if r is prime top, the group (K*)' of r-th powers of elements of K* is of finite index in K* (use Hensel's Lemma). Show that, if further u is discrete and K of characteristic 0, the same result is valid without restriction on Y (observe that every element of 1 paA is a P-th power). + 3 10 1. Let K be a field and P the prime subfield of K; the absolute dimension of K is the number dim. al, K if P is of characteristic @ > 0 and the number 1 if P is of characteristic 0. Let v be a valuation on K, hits height, dim. alp K Y its rational rank and k its residue field. + 47 1 VI VALUATIONS EXERCISES (a) Suppose that the absolute dimension n of K is finite. Then, if s is the absolute dimension k, r s < n. (b) Suppose further that K is a finitely generated extension of P. Then, if r + s = n, k is a finitely generated extension of its prime field and the order group of u is isomorphic to ZT;if h s = n, k is a finitely generated extension of its prime field and the order group of u is isomorphic to Z* ordered lexicographically; finally, if s = n - 1, v is a discrete valuation and k is a finitely generated extension of its prime field. (2) O r Dn(P) = m ; then there is a valuation u' on K(X) extending u such that Dv(P(X)) EB = u(P(a,)) for p large enough and K(X), with u', is an + + n immediate extension of K (use the criterion in (a)). (e) Deduce from (c) and (d) that for K to be linearly compact, it is necessary and sufficient that K have no immediate extension other than itself. 7 2. Let K be a field, u a valuation on K, L an extension of K and u' a valuation on L extending v ; L is called an immediate extension (with respect to u') if e(u'/u) = f (u ' / u) = 1. The completion R of K is an immediate extension of K. (a) For L to be an immediate extension of K, it is necessary and sufficient K, there existy E K such that v'(x - y) > u ' (x) . that, for all x E L (b) For every field K, show that there exists a maximal immediate extension L of K, that is, not admitting an immediate extension distinct from itself (use 3 3, Exercise 3 (b)). (c) Show that, if K is linearly compact with the topology defined by v, it admits no immediate extension other than itself (use (a), noting that, in the notation of (a), the set of v'(x - y) for y E K has no greatest element in the value group of v'). (d) Suppose that K is not linearly compact; let B be a well-ordered subset of the order group of v and a family of elements of K such that, for - A a) for the relation "every fractional principal ideal containing a also contains 6"; clearly this relation is a #reordering on I(A). Let R denote the associated equivalence relation ''a < b and 6 < a" (Set Theory, Chapter I I I , § 1, no. 2) and D(A) the quotient set I(A)/R; we shall say that the elements of D(A) are the divisors of A and, for every fractional ideal a E I(A), we shall denote by div a (or div, a) the canonical image of a in D(A) and we shall say that div a is the divisor of a; if a = A x is a 475 VII DMSORIAL IDEALS OF AN INTEGRAL DOMAIN DIVISORS fractional principal ideal, we write div(x) instead of div(Ax) and div(x) is called the divisor of x ; the elements of D(A) of the form div(x) are called principal divisors. By taking the quotient, the preordering < on I (A) defines on D(A) an ordering which we shall denote by < For all a E I(A) there exists by hypothesis somed # 0 in Asuch that a c Ad-1; the intersection 5 of the fractional principal ideals containing a is therefore an element of I(A). Clearly the relation a < b is equivalent to the relation 5 2 6; the relation a 2 b therefore implies a < 6. For two elements a, b of I(A) to be equivalent modulo R, it is necessary and sufficient that 't = 6. . DEFINITION 2. Every element a ofI(A) such that a = 't is called a divisorial fractional ideal of A. I n other words a divisorial ideal is just a non-zero intersection of a non-empty family of fractional principal ideals. Every non-zero intersection of divisorial ideals is a divisorial ideal. If a is divisorial, so is ax for all x E K*, the mapping b H bx being a bijection of the set of fractional principal ideals onto itself, For all a E I(A), 6 is the least divisorial ideal containing a and is equivalent to a modulo R. Moreover, if b is a divisorial ideal equivalent to a modulo R, then c i = 6 = b. Hence 5 is the unique divisorial ideal b such that div a = div b (in other words, the restriction of the mapping a H div a to the set of divisorial ideals is injective). Let a and b be two fractional ideals of K. Recall (Chapter I, 3 2, no. 10) that b : a denotes the set of x E K such that xa c 6 ; this is obviously an A-module; if b E I(A) and a E I(A), then 6 : a E I(A) ; for if d is a non-zero element of A such that db c A and da c A and a is a non-zero element of A n a, then da(b: a) c A; on the other hand, if b # 0 belongs to 6, then bda c 6, hence bd E 6 : a and 6 : a # 0. The definition of b : a can also be written: b:a = n XSR,X#O bx-1. PROPOSITION 1. (a) If b is a divisorial ideal and a E I(A), 6 : a is divisorial. (b) Let a, b be in I(A). In order that div a = div 6, it is necessary and sujicient that A: a = A: 6. (c) For all a E I(A), 6 = A: (A: a). Assertion (a) follows immediately from equation (1) since, if b is divisorial, so is bx-l for all x # 0. To show (b), let P(a) denote the set of fractional principal ideals containing a; the relation Ax E P(a) is equivalent to x - l a c A and hence to x - l E A: a. As the relation div a = div b is by definition equivalent to P(a) = P(b), it is also equivalent to A: a = A: 6. 476 9 1.1 Finally, as a(A: a) c A, a c A: (A: a). Replacing a by A: a in this formula, it is seen that A: a c A: (A: (A: a)) ; on the other hand, the relation a c A: (A: a) implies A: a 3 A: (A: (A: a)). ThereforeA: a = A:(A: (A: a)) anditfollowsfrom (b) thatdiva = div(A: (A:a)) As A: (A: a) is divisorial by (a), certainly 6 = A : (A: a), which proves (c). Remark. In the course of the above proof it has been proved that A: a = A: (A: (A: a)) for every ideal a E I(A), which is a special case of Set Theory, Chapter 111, 3 1, no. 5, Proposition 2. PROPOSITION 2. (i) In D(A) every non-empty set bounded above admits a least upper bound. Moreprecisely, $(a,) is a non-emptyfamily ofelements of I(A) which is bounded above, then sup(div L a,) = d i v (v 5,). (ii) In D(A) every non-empty set bounded below admits a greatest lower bound. More precisely, fi (a,) is a non-empty family of elements of I(A) which is bounded below, then inf(div a,) = div(T a,). (iii) The set D(A) is a lattice. Let (a,) be a non-empty family of elements of I(A) which is bounded above. To say that a divisorial ideal b bounds this family above amounts to saying that it is contained in all the a,, that is that b is contained in 6,. Hence (;I 6 , # (0) 6 , is therefore a divisorial ideal, which shows (i). and Now let (6 ,) be a non-empty family of elements of I(A) which is bounded below. To say that a divisorial ideal b bounds this family below means that it contains all the ZL, that is (since b is divisorial) that it contains all the a,, or also 7 a,. This proves (ii). that b 2 Finally, to prove (iii) it is sufficient by (i) and (ii) to prove that, if a, b are in I(A), the set {a, b} is bounded both above and below in I(A); now it is bounded above by a n b (which is distinct from (0)). It is bounded below by a 6, for a b E I(A) : if d and d' are non-zero elements of A such that da c A and d'b c A, then dd'(a + 6) c A. + + + y are in K*, then div(x + y) 2 inf(div(x), div(y)). A(x + y) c Ax + Ay and hence div(x + y) 2 div(Ax + A y) . COROLLARY. I f x , y and x 47 7 vn DIVISORS THE MONOID STRUCTURE ON 2. THE MONOID STRUCTURE ON D(A) D(A) 8 1.2 + and If div b = div a div(x) for some x E K*, then div b = div(xa) and, as b and xa are divisorial, b = xa, which proves the proposition. We may restrict our attention to the case where b = 6'. Then let Ax be a fractional principal ideal containing a'b; for every non-zero element y of 6, & 3 a'y and hence Axy-l 3 a', whence A x y - l 2 a and Ax 2 ay. Varying y , it is seen that Ax 2 ab, whence ab > a'b. Let a be an invertible fractional ideal (Chapter 11, 5 5 , no. 6); then a = A: (A: a) (loc. cit., Proposition 10) and hence a is divisorial (no. 1, Proposition 1). The group J(A) of invertible fractional ideals is therefore identified with a subgroup of the monoid D(A) and the canonical image of J(A) in D(A)/S with the group of classes ofprojective A-modules ofrank 1 (Chapter 11,s 5 , no. 7, Corollary 2 to Proposition 12 and Remark 1). PROPOSITION 3. Let a, a', 6, 6' be elements of I(A). The relations b > b' imply ab > a'b'. a > a' It follows from Proposition 3 that multiplication on I(A) defines, by passing to the quotient, a law of composition on D(A) which is obviously associative and commutative. I t is written additively so that we may write: div(ab) = div a (2) + div 6, for a, b in I(A). Clearly div(1) is an identity element for this addition; this element is denoted by 0. Proposition 3 proves further that the order structure on D(A) is compatible with this addition (Algebra, Chapter VI, 5 1, no. 1) and, more precisely (no. 1, Proposition 2 (ii)) : inf(div a + div b, div a + div c) = inf(div(ab), div(ac)) = div(ab + ac) = div(a(b + c)) = diva + div(b + c) = diva + inf(div b, div c). For a fractional ideal a # 0 to be such that div a 2 0 in D(A), it is necessary and sufficient that a c A (in other words, that a be an integral ideal of A). For two elements x, y of K*, the relation div(x) = div(y) is equivalent to ku = Ay; the set of principal divisors of A with the order relation and the monoid law induced by that on D(A) is an ordered group canonically isomorphic to the multiplicative group of fractional principal ideals ordered by the opposite order relation to inclusion (Algebra, Chapter VI, 5 1, no. 5). The relation S between two elements P, Q of D(A) : "there exists x E K* such that P = Q + div(x)" is therefore a equivalence relation since the relation P Q div(x) is equivalent to Q = P div(x⁻¹); if P and Q are congruent modulo S, they are called equivalent divisors of A. Clearly moreover the relation S is compatible with the law of the monoid D(A). The set of classes of this monoid is called the divisor class monoid of A. PROPOSITION 1. Let a, b be two divisorial fractional ideals of A. The following properties are equivalent : (a) div a and div b are equivalent divisors ; (b) there exists t E K* such that b = ta. THEOREM 1. Let A be an integral domain. For the monoid D(A) of divisors of A to be a group, it is necessary and sufficient that A be completely integrally closed. Suppose that D(A) is a group. Let x E K ; suppose that A[x] is contained in a finitely generated sub-A-module of K. Then we have (no. 1) that a = A[x] is an element of I(A). Then xa c a and hence div(x) + div a 2 div a. Since D(A) is an ordered group, we conclude that div(x) 2 0, whence x E A . Thus A is completely integrally closed (Chapter V, 5 1, no. 4, Definition 5) . Conversely, suppose that A is completely integrally closed. Let a be a divisorial ideal. We shall show that div a + div(A : a) = 0, which will prove that D(A) is a group. As a(A: a) c A, it suffices (no. 1) to verify that every fractional principal ideal Ax ... I which contains a(A: a) also contains A. Now, for y E K*, the relation Ay 2 a implies y - 1 E ... therefore a(A : a) c Ax is equivalent to x⁻¹a(A : a) c A whence x⁻¹a c A : a... that A is completely integrally closed. Suppose that A is an integral domain and a is a divisorial ideal...

COROLLARY. Let A be a completely integrally closed domain and a a divisorial fractional ideal of A. Then, for every fractional ideal b of A, div(a : b) = div a - div b.

KRULL DOMAINS DEFINITION 3. An integral domain A is called a Krull domain if there exists a family (v_i)_{i∈I} of valuations on the field of fractions K of A with the following properties: (AK_I) the valuations v_i are discrete; (AK_II) the intersection of the rings of the v_i is A; (AK_III) for all x E K*, the set of indices i E I such that v_i(x) ≠ 0 is finite. If the family (v_i) satisfies (AK_I), (AK_II) and (AK_III), we shall say that it defines A. Examples (1) Every discrete valuation ring is a Krull domain. (2) Every principal ideal domain is a Krull domain. (3) Let A be a Krull domain... every factorial domain is a Krull domain.

PROPOSITION 2. Let A be a Krull domain. Then A is completely integrally closed, hence D(A) is a group. Every intersection of discrete valuation rings is completely integrally closed...

THEOREM 2. Let A be an integral domain. For A to be a Krull domain, it is necessary and sufficient that the two following conditions be satisfied: (a) A is completely integrally closed; (b) every non-empty family of integral divisorial ideals of A admits a maximal element (with respect to inclusion). Moreover, if P(A) is the set of extremal elements of D(A) (and hence prime divisorial ideals), the valuations v_p associated... the family (v_p)_{p∈P(A)} defines A, and D(A) is the free group with basis the set of divisors div p...

COROLLARY. Let A be a Krull domain and let B be a subring of K. If B = A_S for a multiplicative subset S, then B is a Krull domain.

THEOREM 3. Let A be a Krull domain and P the set of prime ideals of height 1 of A. (a) For all p E P, A_p is a discrete valuation ring. (b) A is the intersection of the A_p, p E P. (c) For all x E A, x ≠ 0, the set of p E P containing x is finite. (d) The mapping p → div p is a bijection of P onto the set of extremal elements of D(A). Conversely, let A be an integral domain and P a set of prime ideals of A such that (a), (b) and (c) hold; then A is a Krull domain and P is the set of prime ideals of height 1 of A.

4. ESSENTIAL VALUATIONS OF A KRULL DOMAIN DEFINITION 4. Let A be a Krull domain and K its field of fractions. The valuations defined by formula (4) on no. 3 (for p E P(A)) are called the essential valuations of K (or A). We have remarked in the course of the proof of Theorem 2 that the valuations v_p satisfy properties (AK_I), (AK_II) and (AK_III) (Definition 3). Moreover, these discrete valuations are normed: for every extremal divisor P there exists x E K such that v_P(x) = 1...

PROPOSITION 5. Let A be a Krull domain, K its field of fractions and (v_i) a family of discrete valuations of K defining A. Then every essential valuation of A is equivalent to one of the v_i. THEOREM 4. Let A be a Krull domain. Every prime ideal of height 1 of A is divisorial and the essential valuations of A are the valuations v_p, where p runs through the set of prime ideals of height 1.

COROLLARY 1. Let A be a Krull domain and S a multiplicative subset of A. Then A_S is a Krull domain and its essential valuations are the essential valuations of A whose rings contain A_S. COROLLARY 2. Let A be a Krull domain, L a field containing A and B = L ∩ ...

PROPOSITION 6. Let A be a Krull domain and (v_i) a family of normed valuations of A defining A... The essential valuations v_p of A are characterized as those for which the ring of v_p is A_p...

5. APPROXIMATION FOR ESSENTIAL VALUATIONS OF A KRULL DOMAIN PROPOSITION 7. Let A be a Krull domain, (v_i)_{1≤i≤r} a finite family of distinct essential valuations of A and (n_i) a family of r rational integers. Then there exists x E K such that v_i(x) = n_i for 1 ≤ i ≤ r and v(x) ≥ 0 for every essential valuation v distinct from the v_i.

6. PRIME IDEALS OF HEIGHT 1 IN A KRULL DOMAIN DEFINITION 5. ... THEOREM 5. Let A be a Krull domain and P an integral divisorial ideal; for the ideal p to be the integral domain it is necessary and sufficient that it be a prime ideal of height 1.

PROPOSITION 8. Let A be a Krull domain and A' its integral closure in a finite extension of its field of fractions... A' is a Krull domain.

7. APPLICATION: NEW CHARACTERIZATIONS OF DISCRETE VALUATION RINGS PROPOSITION 11. Let A be a Noetherian local domain of dimension 1. For A to be a discrete valuation ring it is necessary and sufficient that A be integrally closed.

8. INTEGRAL CLOSURE OF A KRULL DOMAIN IN A FINITE EXTENSION OF ITS FIELD OF FRACTIONS PROPOSITION 12. Let A be a Krull domain, K its field of fractions, K' a finite extension of K and A' the integral closure of A in K'. Then A' is a Krull domain. Further, the essential valuations of A' are the valuations which extend the essential valuations of A, and for each essential valuation v of A there exist only finitely many valuations of K' extending v.

9. POLYNOMIAL RINGS OVER A KRULL DOMAIN PROPOSITION 13. Let A be a Krull domain and X an indeterminate. Then A[X] is a Krull domain. The essential valuations of A[X] are: (a) the valuations extending the essential valuations of A, obtained by Gauss's lemma; (b) the essential valuations of K[X] which correspond to irreducible polynomials of K[X].

10. DIVISOR CLASSES IN KRULL DOMAINS Let A be a Krull domain and D(A) its divisor group. Let F(A) be the subgroup of D(A) consisting of the principal divisors; the quotient group C(A) = D(A)/F(A) is the divisor class group of A. PROPOSITION 14. Let A be a Krull domain and S a multiplicative subset of A. The canonical homomorphism of C(A) onto C(A_S) is surjective and its kernel is generated by the classes of the prime divisors div p with p ∩ S ≠ ∅.

PROPOSITION 15. Let A and B be two Krull domains with A ⊂ B and such that B is integral over A or flat over A... then there exists a homomorphism i: D(A) → D(B)...

PROPOSITION 16. Let A be a Krull domain; the canonical homomorphism C(A) → C(A[X]) is bijective.

PROPOSITION 17. Let A be a Krull domain; the canonical homomorphism of C(A) into C(A[[X]]) is injective.

§ 2. DEDEKIND DOMAINS 1. DEFINITION OF DEDEKIND DOMAINS DEFINITION 1. An integral domain A is called a Dedekind domain if every fractional ideal of A is invertible. THEOREM 1. Let A be an integral domain. The following properties are equivalent: (a) A is a Dedekind domain; (b) A is a Noetherian Krull domain of dimension ≤ 1; (c) A is Noetherian and integrally closed and every non-zero prime ideal of A is maximal; (d) A is Noetherian and, for every maximal ideal m of A, A_m is a field or a discrete valuation ring. (e) Every non-zero ideal of A is a product of prime ideals...

COROLLARY 1. Let A be a Dedekind domain and S a multiplicative subset of A. Then A_S is a Dedekind domain. COROLLARY 2. Every principal ideal domain is a Dedekind domain. COROLLARY 3. A semi-local Dedekind domain is a principal ideal domain.

PROPOSITION 1. Let A be a Dedekind domain, K its field of fractions, L a finite extension of K and B the integral closure of A in L. Then B is a Dedekind domain.

2. CHARACTERIZATIONS OF DEDEKIND DOMAINS PROPOSITION 2. Let A be a Noetherian integral domain. The following are equivalent: (a) A is a Dedekind domain; (b) every ideal of A is projective; (c) every torsion-free finitely generated A-module is projective.

3. DECOMPOSITION OF IDEALS INTO PRODUCTS OF PRIME IDEALS Let A be a Dedekind domain. Since D(A) is isomorphic to the group of fractional ideals of A, it is the free abelian group with basis the set of non-zero prime ideals of A. Every non-zero fractional ideal a of A can therefore be written uniquely in the form a = ∏ p^{v_p(a)}, where the v_p(a) are rational integers, zero except for a finite number of them. Further a is integral if and only if the v_p(a) are all positive.

4. THE APPROXIMATION THEOREM FOR DEDEKIND DOMAINS PROPOSITION 3. Let A be a Dedekind domain, K its field of fractions, (p_i) a finite family of distinct non-zero prime ideals, (n_i) a family of integers and (x_i) a family of elements of K. Then there exists x E K such that v_{p_i}(x - x_i) ≥ n_i for all i and v_p(x) ≥ 0 for every other prime ideal p.

PROPOSITION 4. Let A be a Dedekind domain. Every fractional ideal of A is generated by two elements, one of which may be chosen arbitrarily among the non-zero elements of the ideal.

5. THE KRULL-AKIZUKI THEOREM PROPOSITION 5. Let A be a Noetherian integral domain of dimension 1, K its field of fractions, L a finite extension of K, B a subring of L containing A. Then B is Noetherian and of dimension ≤ 1, and for every ideal b ≠ 0 of B, B/b is an A-module of finite length.

THEOREM 2 (Krull-Akizuki). Let A be a Noetherian integral domain of dimension 1, K its field of fractions, L a finite extension of K and B a ring such that A ⊂ B ⊂ L. Then B is Noetherian and of dimension ≤ 1. Moreover, for every non-zero ideal J of B, B/J is a module of finite length over A. COROLLARY 1. With the hypotheses of Theorem 2, the integral closure of A in L is a Dedekind domain. COROLLARY 2. Let A be a Noetherian integral domain of dimension 1 and B the integral closure of A in its field of fractions. Then B is a Dedekind domain and, for every maximal ideal m of A, the set of maximal ideals of B lying over m is finite.

§ 3. FACTORIAL DOMAINS 1. DEFINITION OF FACTORIAL DOMAINS DEFINITION 1. An integral domain A is called factorial if it satisfies the following conditions: (a) A is a Krull domain; (b) every divisorial ideal of A is principal. THEOREM 1. Let A be an integral domain. The following conditions are equivalent: (a) A is factorial; (b) every non-zero principal ideal of A is a product of principal prime ideals; (c) the multiplicative monoid of non-zero principal ideals of A is isomorphic to a free monoid; (d) A satisfies the maximal condition for principal ideals and every irreducible element is prime.

PROPOSITION 1. Let A be a Noetherian integral domain. For A to be factorial it is necessary and sufficient that every prime ideal of height 1 of A be principal.

2. CHARACTERIZATION OF FACTORIAL DOMAINS BY THEIR PRIME IDEALS PROPOSITION 2. Let A be a Krull domain. The following are equivalent: (a) A is factorial; (b) every prime ideal of height 1 is principal; (c) every non-zero prime ideal contains a non-zero principal prime ideal.

3. DECOMPOSITION INTO EXTREMAL ELEMENTS PROPOSITION 3. Let A be a factorial domain and P a representative system of extremal elements of A. Every element x ≠ 0 of A can be written uniquely in the form x = u ∏_{p∈P} p^{v_p(x)}, where u is a unit and the v_p(x) are positive integers, almost all zero.

4. POLYNOMIAL RINGS OVER A FACTORIAL DOMAIN THEOREM 2. Let A be a factorial domain. Then the polynomial ring A[X_1, ..., X_n] is factorial. Corollary. Let A be a factorial domain and K its field of fractions. Every polynomial f E A[X] may be written as f = c(f) f_1 with c(f) the content...

5. FACTORIAL DOMAINS AND RINGS OF FORMAL POWER SERIES PROPOSITION 8. Let A be a principal ideal domain. Then the ring of formal power series A[[X_1, ..., X_n]] is factorial.

6. PRELIMINARIES ON AUTOMORPHISMS OF RINGS OF FORMAL POWER SERIES LEMMA 1. Let K be a field and A = K[[X_1, ..., X_n]]. For every element f ≠ 0 of A there exists an automorphism u of A such that u(f) is, up to a unit, a distinguished polynomial in X_n with coefficients in K[[X_1, ..., X_{n-1}]].

7. THE PREPARATION THEOREM THEOREM 3 (Weierstrass preparation theorem). Let A be a ring, complete and Hausdorff with respect to its m-adic topology where m is its maximal ideal, and let f = Σ a_i X^i E A[[X]] be a formal power series such that not all the coefficients lie in m. Let s be the least integer such that a_s ∉ m. Then f may be written uniquely in the form f = u(X^s + b_{s-1}X^{s-1} + ... + b_0), where u is invertible and b_i E m. PROPOSITION 5 (Division theorem). With the same hypotheses, every g E A[[X]] may be written uniquely as g = qf + r, with q E A[[X]] and r a polynomial of degree < s.

8. FACTORIALITY OF RINGS OF FORMAL POWER SERIES THEOREM 4. Let K be a field, or a discrete valuation ring. Then the ring K[[X_1, ..., X_n]] is factorial. The proof is by induction on n using the preparation theorem and Theorem 2... Remarks (1) There exist factorial domains A such that A[[X]] is not factorial.

rings A such that the ring A[[X]] is not factorial (Exercise 8). However, if A is a principal ideal domain, A[[X,, . . ., X,]] is factorial (Exercise 9). (2) * We shall see later, by homological methods, that every regular local ring is factorial (cf. 5 4, no. 7, Corollary 3 to Proposition 16). This will give another proof, conceptually simpler, of Proposition 8. * 4. MODULES OVER INTEGRALLY CLOSED NOETHERIAN DOMAINS Throughout this paragraph, A will be a commutative integral domain with field of fractions K. Starting with no. 2, A will be further assumed to be Noetherian and integrally closed (and hence a Krull domain (5 1, no. 3, Corollary to Theorem 2)); then P(A), D(A) and C(A) will respectively denote the set of prime ideals of height 1 (5 1, no. 6), the divisor group of A (5 1, no. 3) and the divisor class group of A (5 1, no. 10), these latter being written additively. The general method of studying finitely generated modules over an integrally closed Noetherian domain A consists of "localizing" the modules with respect to all the prime ideals p E P(A) of height 1 in A; as A, is then a discrete valuation ring (3 1, no. 6, Theorem 4), the structure of finitely generated Apmodules is well known (Algebra, Chapter VII, 5 4) and therefore gives information about the structure of finitely generated A-modules. In the particular case where A is a Dedekind domain, we can arrive at as complete a theory as when A is a principal ideal domain (no. 10). 1. LATTICES DEFINITION 1. Let V be a finite-dimensional vector space over the field K. A lattice of V with respect to A (or simply a lattice of V) is defined to be any sub-A-module M of V satisfying the following condition : There exist two free sub-A-modules L1, L 2 of V such that L, c M c L, and rg*(L1) = rg(L2) ... [illegible] ...

[illegible]

series in one indeterminate over B and C = ..., the ring of fractions S-lA, where S is the multiplicative set of ... Let v be a normed valuation ... such that s (f g) = s (f) + s (g) for non-zerof, g in C. (If s(f) = p 2 s (g) = q and h is the least of the degrees of the terms # O in f, show that there exists u E C such that f - ug = X h + y l where fl E C and, by arguing by redutio ad absurdum deduce the existence of a process of "Euclidean division" in C.) If s (f) = 0, f is invertible in C. * Show that A is not a Dedekind domain. * (b) Deduce from (a) that, if B is a Krull domain, A = B[[X]] is also a Krull domain. (If K is the field of fractions of B, note that A is the intersection of K[[X]] and a family (C,) of principal ideal domains with the same field of fractions as A and that every element of A is invertible in almost all the CL.) 6. Let A be an integral domain. (a) For a divisorial ideal a of A to be such that div(a) is invertible in D(A), it is necessary and sufficient that a: a = A (cf. Exercise 5 and Algebra, Chapter VI, 5 1, Exercise 30). In particular, in order that a: a = A for every divisorial ideal a of A, it is necessary and sufficient that A be completely integrally closed. (b) In order that a: a = A for every finitely generated ideal a # 0 of A, it is necessary and sufficient that A be integrally closed. 10. Let A be a Krull domain, K its field of fractions, L a field containing K and (B,) a right directed family of Krull domains containing A and contained in L such that the field of fractions L, of B, is a finite algebraic extension of K and B, is the integral closure of A in La. For every essential valuation u of A and all a, let e,(v) be the sum of the ramification indices of the valuations on B, which extend u. Show that for the union of the B, to be a Krull domain, it is necessary and sufficient that for every essential valuation v of A, the set of e,(v) be bounded. 7. Let K be a field and (u ,) , ~ ,a family of discrete valuations on K satisfying conditions (AK,) and (AK,,) of no. 3 and such that, for every integer r, every family (nh) h of rational integers and every family (Lh) h of distinct elements of I, there exists x E K such that ulh(x) = nh for 1 < h < r and 7 11. A divisor d in an integral domain A is calledjnitely generated if it is of the form div(a), where a is a finitely generated fractional ideal (which is not necessarily divisorial; cf. (b)). 2S4 7 546 i L VII DIVISORS EXERCISES (a) Show that, if A is a Krull domain, every divisor of D(A) is of the form div(a), where a = Ax + Ay, x, y being elements # O of the field of fractions of A (use Corollary 2 to Proposition 9 of no. 5). (b) Let K be a field, A = K[X,],,N the ring of polynomials over K in a denumerable set of indeterminates, which is a Krull ring (Exercise 8). Let A' be the subring of A generated by the unit element and the monomials &X, for all pairs (i , j) (equivalently, A' is the set of polynomials all whose terms have even degree). If L and L' are the fields of fractions of A and A', show that A' = A n L', hence A' is a Krull ring. Let p be the ideal in A' generated by the products X, Xi for all i 2 0; show that p is a prime ideal of height 1 (hence divkon'al) but that it k notjnitely generated. 12. (a) Let A be an integrally closed domain, f(X) = alXf and 7 g(X) = b,Xf be two polynomials in A[X] ;show that, if c E A is such that all the coefficients off (X)g(X) belong to Ac, then all the products a,b, belong to Ac (reduce it to the case where A is a valuation ring). (b) If A is the ring defined in Exercise 1,give an example of two polynomials f, g of degree 1 in A[X] and an element c E A for which the conclusion of (a) does not hold (take c = T4 + T6). (c) Under the hypotheses of (a), let a, 6, c be the ideals of A generated respectively by the coefficientsoff, g and fg: show that div(c) = div(a) + div(b). Give an example where i- # (i6.Show that, if c is principal, c = ab and a and b are invertible; if further A is a local ring, a and b are principal. 13. Let A be an integral domain and (t,),a family of non-zero elements such that the principal ideals Ap, are prime; let S be the multiplicative subset, generated by the p,. (Q (a) Show that A = S-lA n AAp,). (b) Suppose that every non-empty family of principal ideals of A has a maximal element. Show that each of the rings AAp,is a discrete valuation ring (cf. Chapter VI, Q 3, no. 5, Proposition 9). Deduce that, if S-'A is integrally closed (resp. completely integrally closed), A is integrally closed (resp. completely integrally closed). If S-'A is a Krull domain, show that A is a Krull domain. 14. Let A be a Krull domain and S a saturated multiplicative subset of A not containing 0 (Chapter 11, Q 2, Exercise 1). Show that, if the canonical homomorphism :: C(A) +- C(S-'A) (no. 10, Proposition 17) is bijective, S is gene- 548 rated by a family (p,) of elements such that each 4,is a prime ideal (note that every divisorial prime ideal which meets S is principal), 7 15. (a) Let A be an integral domain and a, b two elements #O of A such that Aa n Ab = Aab. Show that in the polynomial ring A[X] the principal ideal generated by a x + b is prime (prove that every polynomialf(X) E A[X] such thatf(-b/a) = 0 is a multiple of aX 6, arguing induction on the degree o f f 1. (b) Let A be a Krull domain and a, b two elements of A such that Aa and Aa + Ab are prime and distinct. Show that A[X]/(aX +- b) is a Krull domain and that C(A[X]/(aX b)) is isomorphic to C(A). (Note, with the aid of (a), that A[X]/(aX + 6) is isomorphic to A[b/a] = B; show that Ba is prime in B. Observe that A[u-l] = B[a-l] is a Krull domain and use Exercise 12.) (c) Let A be an integrally closed Noetherian domain and a, b two elements of the Jacobson radical r of A. Suppose that the ideal Aa + Ab is a non-divkorial prime ideal; show that Aa and Ab are prime ideals. (Prove first that Aa n A6 = Aab considering the ideals of Ass(A/Aa). Show secondly that the relations xy E Ab and y $ Aa Ab imply x E Ab + Aah for all h, by induction on h; deduce that then x E Ab. Finally, deduce that, if xy E Ab, x 4 Ab, y fj! Ab, then necessarily x E A6 Aah and y E Ab Aahfor all h, arguing by induction on h; deduce a contradiction.) + + + + 16. Let A = @ A, be a graded Krull domain. Let D,(A) (resp. F,(A)) ncZ denote the group generated by the divisors of the graded integral divisorial ideals (resp. by the divisors div(a), where a is homogeneous in A); write C,(A) = D,(A)/F,(A). Let S be the multiplicative subset of homogeneous elements #O of A. (a) Show that every prime ideal of A of height 1 which meets S is graded (use Chapter 111, Q 1, no. 4, Proposition 5). (b) Let B = S-lA, which is a graded ring (Chapter 11, Q 2, no. 9); write B,; show that B, is a field and that, if A # A,, B is isomorphic to the B= ring B,[X, X-l] of rational functions P(X)/XL,where P(X) E Bo[X]. (c) Show that CJA) and C(A) are canonically isomorphic (use (a), (b) and equation (5) ofno. 10). ,qZ 17. Let A = A,, be a graded Krull domain and&E A, be such that Ap is prime and # 0. (a) Show that, if B is the ring A(p)defined in Chapter 111, Q 1, Exercise 1 (a), B is a Krull domain and the groups C(A) and C(B) are canonically isomorphic. (Show first that C(B) is isomorphic to C(B[p,p-']) and observe that B[p,p-ll = "-'I-) 549 VII EXERCISES DIVISORS the subring of an algebraic closure of K(X) generated by K and two sequences where x1 = X and x,- = xi. Show of elements (x,), (l/x,) (1 < n < +a), that A is Bezoutian (use (a)). If p is a prime ideal # O of A, show that p is generated by a sequence of elements of the form x, - a,, where a, E K, a, # 0 and a; = (consider for all n the intersection p n K[x,, l/x,]). Show that p is not finitely generated. (b) Under the hypotheses of Exercise 15 (b), show that the groups C(A) and C(A[X, Y]/(aX + b y)) are isomorphic. 7 18. Let A = ,FZA, be a graded Krull domain with positive degrees, such ,T1 that A, is a field and let m = A,, a maximal ideal of A. Let S be the multiplicative set of homogeneous elements #O of A, so that the ring S-lA is a principal ideal domain (Exercise 16 (b)). (a) Let p be a prime ideal of A of height 1 which meets A m; then p is not graded (otherwise p = A) and the ideal S-lp of S-lA is principal, generated by an element of the form x = 1 x , + . . x, where x, E (S-lA)p Writing an element of p of the form 1 + a, a,, (a, E A,) as a multiple of x in S-lA and using Chapter V, 3 1, no. 3, Proposition 11, show that x E p; writing finally every element of p as a multiple of x in S-lA, show that p = Ax. 2 1. An integral domain A is called pseudo-Bezoutian (resp. pseudo-principal) if, in the notation of Exercise 5, the group K*/U is lattice-ordered (completely lattice ordered). Every Bezoutian * (resp. factorial) * domain is pseudo-Bezoutian * (resp. pseudo-principal) *. Every pseudo-principal domain is pseudoBezoutian. A valuation ring whose order group is R is pseudo-principal but not a principal ideal domain. Every pseudo-Bezoutian (resp. pseudo-principal) domain is integrally closed (resp. completely integrally closed) (use Exercise 6). * Every Noetherian pseudo-Bezoutian domain is factorial. * Give an example of an integrally closed Noetherian (and therefore Krull) domain which is not pseudo-Bezoutian (cf. Exercise 2). If A is pseudo-Bezoutian, so is S-lA for every multiplicative subset S of A such that 0 $ S (use Chapter 11, 5 2, Exercise 1). - + + + + (b) Deduce from (a) that C(A) and C(&) are canonically isomorphic (use Proposition 17 of no. 10). 7 22. (a) Let I' be a lattice-ordered additive group and A the algebra of I' over a field k ; A is an integral domain (Algebra, Chapter 11, 3 11, no. 4, Proposition 8). Every element x # 0 in A may be written uniquely as 19. Let A be a local Krull domain and m its maximal ideal; if show that C(A) and C (A) are canonically isomorphic. A' = (A[X]),,,,,, (Apply the criterion of Proposition 17 of no. 10, using Exercise 12 (c).) x = 7 20. An integral domain A is called Bezoutian (or a Bezout domain) if every Jinitely generated ideal of A is principal. Every Bezoutian Noetherian domain is a principal ideal domain. Every valuation ring is a Bezoutian domain (and therefore a Bezoutian domain is not therefore necessarily Noetherian nor completely integrally closed). (a) Show that every Bezoutian domain is integrally closed (cf Exercise 6). If an integral domain is the union of a right directed family of Bezoutian subdomains, it is Bezoutian. If A is a Bezoutian domain, so is S-lA for every multiplicative subset S of A such that 0 4 S. (b) Let v, (1 < i < n) be independent valuations on a field K and 4 the ring of the valuation v,. Show that the intersection A of the A, is a Bezoutian domain. (If an ideal a of A is finitely generated, the set of v,(x) for x E a admits a least element a, in the value group of v,; for all i, let x, E a be such that v ~ (x ,)= tcp Using the Approximation Theorem (Chapter VI, 3 7, no. 2, vi are distinct elements of I', the evl the corresponding elements of the canonical basis of A over k and the a, elements # 0 of k. Write + (x) = inf(vl, . . ., v,) in I'; show that + (x y) 2 inf(+(x), +(y)) if x, y and x + y are # O in A and +(xy) = + (x) +(y) if xy # 0 in A. (To show the second assertion, establish first the following lemma: given a finite family (6,) of elements of I', in order that inf(t,) = 0, it is necessary and sufficient + + f that for all q > 0 in I' there exist an indexj and an element t: E I? such that 0 < 1: 6 q and inf(Ej, 1:) = 0.) Apply this lemma reducing it to the case where +(x) = = 0.) (b) Deduce from (a) that, if K is the field of fractions of A, can be extended to a homomorphism from K* to I? (also denoted by +) such that + + k + Y) 2 inf(+(x), +(Y)) + if x, y and x y are #O in K. Deduce that, if B is the set of x E K such that x = 0 or + (x) 2 0, B is a domain whose field of fractions is K and such that, if U is the group of invertible elements of B, K*/U is isomorphic to I' (and in particular B is a pseudo-Bezoutian domain). Derive examples of a pseudoBezoutian domain which is not completely integrally closed, a completely integrally closed pseudo-Bezoutian domain which is not pseudo-principal (cf. Theorem l), show that there are elements ai E A such that x = aixf E a satisfies the relations v,(x) = a,for 1 < i < n.) If the v, are discrete valuations, A is a principal ideal domain. (c) Let K be an algebraically closed field of characteristic 2 2 and let A be 550 5 ufev{,where the ,=1 I 55 1 VII DMSORS Alzebra, Chapter VI, $ 1, Exercise 31) * and a pseudo-principal domain which is ;lot factorial. * * (c) Derive from (b) an example of an integral domain which is the union of a right directed family of factorial subdomains and is completely integrally closed but not pseudo-Bezoutian. (Let 0 be an irrational number in [0,1] and for every integerj let qj be the greatest integer such that qj/2' < 0. For a l l j define on the product group Q x Q a lattice-ordered group structure by taking the set (G,) of elements 2 0 of this group - to be the ordered pairs (6, q) such that 5 2 0 and 0 < q < (q,2-35). * 23. (a) Let A be a pseudo-Bezoutian domain (Exercise21) and K its field of fractions; for every polynomialf E A[X] a g.c.d. of the coefficients off (determined to within an invertible element of A) is called a content off. Let f, g be two polynomials of A[X]; show that for f to divide g in A[X], it is necessary and sufficient that f divide g in K[X] and that a content off divide a content ofg (use Exercise 12) (cf. Exercise 30 (c)). (b) Deduce from (a) that, ifA is a pseudo-Bezoutian (resp. pseudo-principal) domain, then so is A[X]. Moreover, if (a,) is a finite (resp. any) family of elements # O of A and d a g.c.d. of this family in A, d is also a g.c.d. of this family in A[X]. (c) Deduce from (b) that, if A is pseudo-Bezoutian (resp. pseudo-principal) then A[XJA is pseudoBezoutian (resp. pseudo-principal) for every family (Xh)hs of indeterminates. 24. Let K be an algebraically closed field and A = K[X, Y] the polynomial ring in two indeterminates over K, which is a Krull domain * (and even a hctorial domain). * For every ordered pair (a,(3) E Ka let w , , ~be the discrete valuation on A such that, for every polynomialf # 0, w , , ~f) (is the least degree of the monomials # O in f (X + a,Y + p). Show that A is the intersection of the rings of the valuations w , , ~ ,none of which is an essential valuation of A. I \ - , I T 25. An integrally closed domain A is said to be ofjkite character if there exists a family (v,) ,E I of valuations on the field of fractions of A satisfying properties (AKII) and (AKIII). (a) Show that, if A is integrally closed and of finite character, for every element x # 0 in A, there can only be a finite number of extremal elements of the ordered group of principal divisors which are < div(x). (Let J c I be the finite set of indices such that v,(x) > 0. If m is the number of elements in J, show that there cannot be m + 1 elements yj (1 < j < m + 1) dividing x and such that the elements div(y,) are extremal, observing that, for all j, div(y,) must be c Prime to kt; div(y,).) * (b) Show that the ring of integral functions of one complex variable (Chapter v, $ 1, Exercise 12) is a pseudo-principal domain (Exercise 21) but not a domain of finite character (use (a)). * 552 EXERCISES fi 26. Let A be an integral domain and K its field of fractions. A valuation u on K is called essential for A if the ring of v is a local ring Apat a prime ideal p of A (the intersection of A and the ideal of v). (a) Let v be an essential valuation for A of height 1 and let p be the prime ideal A consisting of those x such that v (x) > 0. Show that p is of height 1. If x E K does not belong to Ap,then A n x-lA c p. If w is a valuation on K whose ring B contains A and whose ideal q satisfies q n A c p, show that w is equivalent to v. (b) An integrally closed domain A is said to be ofjnite character and real type if there exists a family (uJ , I of valuations on K of height 1 satisfying properties (AKII) and (AKIII). Show that under these conditions, if z E K does not belong to A and p is a prime ideal of A such that A n z-IA c p, there exists c E I such that v , (z) < 0 and that the prime ideal q, of X E A such that v L (x)> 0 is contained in p. (Argue by reductio ad absurdurn by considering the finite number of u,, such that v l r (z) < 0; prove the existence of an a E A such that a $ p and v l k (a) > 0 for all k; deduce that anz $ A for every integer n > 0 and show that this implies a contradiction.) Conclude from this that every essential valuation for A of height 1 is equivalent to one of the u, (use (a)). Every finite intersection of subdomains of K which are of finite character and real type is also a domain of finite character and real type. (c) Suppose that the hypotheses of (b) are satisfied and moreover that all the v, are essential. Show that, for every prime ideal p of A of height 1, A, is the ring of one of the valuations v, (use (b) taking z - l E p). For all x E A, the principal ideal Ax then admits a unique reduced primary decomposition (Chapter IVY tj 2, Exercise 20), the prime ideals corresponding to this decomposition being the prime ideals of height 1 containing x. (d) Suppose that the hypotheses of (b) are satisfied. Let S be a multiplicative subset of A not containing 0 and J C I the set of 1 E I such that v,(x) = 0 on S. Show that the family (u,), satisfies properties (AKII) and (AKIII) for the ring S-IA; this family consists of essential valuations for S-IA if (vJlG1 consists of essential valuations for A. (e) Generalize Proposition 9 of no. 5 to the case where the hypotheses of (c) are satisfied. (f) Suppose the hypotheses of (b) are satisfied. Let K' be a finite extension of K and A' the integral closure of A in K'. Show that the valuations (no two of which are equivalent) on K' which extend the v, satisfjr properties (AKII) and (AKIII) for A' and the latter is therefore a domain of finite character and real type; if the v, are all essential for A, so are their extensions for A' (argue as in no. 8, Proposition 12 and use also Chapter VI, tj 8, no. 3, Remark). (g) If A is a domain of finite character and real type, so is A[X] ; if the 553 VII DIVISORS EXERCISES conditions of (c) are fulfilled, determine the essential valuations for A[X] (argue as in no. 9). Generalize Exercise 8 similarly. (c) Let A be a regularly integrally closed domain and K its field of fractions; the monoid D,(A) of finitely generated divisors of A generates in D(A) a lattice-ordered group Gf(A). For every polynomial$ E K[X], let d (P) denote the divisor of the fractional ideal of A generated by the coefficients of p ; for every rational function r = p / q of K(X), where p , q are in K[X] and q # 0, d (p) - d (q) is well defined on Gf(A) (independently of the expression of r as a quotient of two polynomials) ;it is denoted by d (r) (cf. Exercise 12 (c)). If we then write y (r) = ((r) ,d (r)) , where (r) is the fractional principal ideal of K[X] generated by r, y is an isomorphism of the ordered group P*(A[X]) (notation of fj3, no. 2) onto a subgroup of the product ordered group ,EI, where the I?, 27. In Exercise 22 take I? to be a direct sum of a family (r,) are subgroups of the additive group R. Show that the ring B defined in Exercise 22 (b) is a domain of finite character and real type and that it is the intersection of a family of essential valuation rings for B; moreover, every prime ideal # O of B is maximal. 28. An integrally closed domain A is said to be ofjnite character and rational , valuations on its field of fractions K satistype if there exists a family (u ,) , ~ of fying properties (AK,,) and (AK,,) and whose value groups are subgroups ofthe additive group Q.Show that the family of essential valuations for A of height 1 satis+ (AK,,) and (AK,). (For all L E I, let p, be the prime ideal ofA consisting ofthe x such that u,(x) > 0 and let V, be the ring of the valuation v,. Show that, if there are two indices u, (3 such that po c pa, then A is the intersection of the V, ofindex L # u. For this, argue by reductio ad absurdum by showing that otherwise there would be an element x E K*, an element y E po and two positive integers r, s such that vo(x'ys) > 0, ua(xrys) = 0 and v,(x'ys) 2 0 for all L E I, contrary to the hypothesis.) P*(K[X]) x G,(A) c P*(K[X]) x D(A). Deduce that A[X] is a regularly integrally closed domain and that D,(A[X]) is isomorphic to .P*(K[X]) x D,(A) (use (a) and (b) and Exercise 29 (b)). (d) Let B be an integrally closed domain, K its field of fractions and A the subring of the polynomial ring K[X, Y] consisting of the polynomials whose constant term belongs to B. Show that, if B # K, A is integrally closed but not regularly integrally closed (show that the divisor inf(div(X), div(Y)) corresponds to a divisorial ideal a such that a: a # A). 29. Let A be an integrally closed domain and K its field of fractions. (a) Let L be an algebraic extension of K and B the integral closure of A in L. Show that for every fractional ideal a of A, if we write b = aB, 6 n A = a". (Reduce it to the case where A c 5, in other words A: a c A and prove that B: b c B; for this, let x E B: b and let ct (I 6 i < n) be the coefficients of its minimal polynomial over K; note that for ally E a the elements ctyi (1 < i < n) belong to A and deduce that the ci belong to A.) (b) Let C be a polynomial ring A[X,],. in any family of indeterminates. Show that for every fractional ideal a of A, if we write c = aC, ? n A = a" (same method). 7 31. (a) Let A be a regularly integrally closed domain (Exercise 30) and K its field of fractions; for every polynomial P E K[X], let c(P) denote the divisor div(a), where a is the fractional ideal of K generated by the coefficients of P. Let B denote the subring of K(X) consisting of the rational functions P/Qsuch that c(P) 2 c (Q) (show that this condition depends only on the element P/Q, using Exercise 30 (a) and 12 (c)). Then B n K = A. (b) Show that B is a Bezoutian domain (Exercise 20) (observe that, if P, Q are two polynomials of A[X], P X"Qdivides P and Q i n B ifm is sufficiently large). (c) Show that, if A is a Krull domain, B is a principal ideal domain (consider an increasing sequence of finitely generated fractional principal ideals of B). Give an example where A is completely integrally closed but B is not a principal ideal domain (cf. Exercise 22). (d) Deduce from (c) an example of a Noetherian domain B for which there exists a subfield K of its field of fractions such that B n K is not Noetherian. + 7 30. An integral domain is called regularly integrally closed if, in the monoid D(A), every finitely generated divisor (Exercise 11) is a regular element. Every completely integrally closed domain is regularly integrally closed ; every pseudo-Bezoutial domain (Exercise 2 I) is regularly integrally closed. (a) If A is regularly integrally closed and d, d', d" are three finitely generated divisors, the relation d + d" < d' + d" implies d < d'. (b) Deduce from (a) that, for an integral domain A to be regularly integrally closed, it is necessary and sufficient that, for every fractional ideal a of A such that div(a) is a finitely generated divisor, a: a = A; in particular A is integrally closed (Exercise6 (b)). (Use the fact that A: (bc) = (A: 6) : c for two fractional ideals 6, c of A, taking b = a, c = A: a.) Moreover, div(a) is then invertible in D(A). 32. Let A be an integral domain and (at) a finite family of elements of A, a the ideal T A a , and R the submodule of A" generated by the element (a l , . . . , a,). Show that, for the torsion submodule of the A-module M = An/R to be a direct factor of M, it is necessary and sufficient that a(A: a) f (A: (A: a)) = A. 554 555 .- EXERCISES DIVISORS VII 32 1. (a) Show that, if a is an ideal # O in a Dedekind domain A, the ring A/a is a principal ideal ring (Algebra, Chapter VII, 3 1, Exercise 5) (note that A/a is semi-local and argue as in Proposition 1 of no. 2). Deduce again that every fractional ideal of A is generated by at most two elements (cf. Exercise 11 (a)). (b) In the polynomial ring A = k [X , Y] over a field k, let m be the ideal Ax + AY. Show that for every integer n the minimum number of generators of the ideal mn is n 1. + 2. (a) Let a, b be two integral ideals of a Dedekind domain A; show that there exists an integral ideal c which is prime to b and such that ac is principal (use Proposition 9 of 3 1, no. 5) . (b) Let a, b be two integral ideals of A; show that there exists x # 0 in the field of fractions of A such that xa is an integral ideal of A which is prime to b (same method). Deduce that the module a/ab is isomorphic to Alb. 3. Let A be a Dedekind domain, K its field of fractions, P the set of prime ideals # 0 of A and for all Q E P let up be the corresponding essential valuation on K. For every sub-A-module M of K and all Q E P we write up(M) = inf up(.) (taken in k);if M # 0, vp(M) < +co for all Q E P and vp(M) < 0 for almost all Q E P. If M, N are two sub-A-modules of K, show that the relation M c N is equivalent to vp(N) < vp(M)for all Q E P (use Proposition 9 of 3 1, no. 5). Conversely, for every family (v ~ EP) ~of elements equal to an integer or -co and such that vp < 0 for almost all Q E P, there exists a unique sub-A-module M of K such that vp(M) = vp for all Q E P. 4. Let A be a Dedekind domain and K its field of fractions. If L is a subfield of K such that A is integral over A n L, then A nL is a Dedekind domain (show first that A n L is a Krull domain and then that every prime ideal of A n L is maximal, using Chapter V, fj 2, no. 1, Theorem 1). 5. (a) Let k be a field, K the field k (X , Y)of rational functions in two indeterminates over k and A the polynomial ring K[Z] in one indeterminate, which is a principal ideal domain. Let L be the subfield k(Z, X YZ) of k (X , y , Z) ;show that A n L is not a Dedekind domain (prove that there are prime ideals which are not maximal and # O in this ring). (b) Let A be a Dedekind domain which is not a principal ideal domain and for which the ideal class group C(A) is finite * (the ring of integers of a finite algebraic extension of Q has the latter property). * Let (a,),,,,, be a representative system of the group I(A) of fractional ideals # O modulo the subgroup of fractional principal ideals, consisting of integral ideals of A and let Pr (1 < i < S) be the prime ideals dividing at least one of the aj. Let S (resp. T) + 556 denote the multiplicative set of elements x E A such that u p l (x) = 0 for all i (resp. consisting of 1 and the x E A such that u,(x) = 0 for all the prime ideals q distinct from the Q{ and up,(.) 2 1 for all i; the hypothesis implies that T is not reduced to 1). Show that S-lA and T-lA are principal ideal domains and thatA = (S-lA) n (T-lA). 6. Show that in a Dedekind domain the notions of primary ideal, irreducible ideal, primal ideal (Chapter IV, 3 2, Exercise 33), quasi-prime ideal (Chapter IV, 3 2, Exercise 34) and power of a prime ideal are identical. 7. Let A be a Noetherian domain. Show that the following properties are equivalent : (E) A is a Dedekind domain. (p) For every maximal ideal m of A, there exists no ideal a distinct from m and m2 such that m2 c a c m. (y) For every maximal ideal m of A, the set of primary ideals for m is totally ordered by inclusion. (6) For every maximal ideal m of A, every primary ideal for m is a product of prime ideals. (Prove that each of the properties (y) and (6) implies (p); then show that (p) implies that A,,, is a field or a discrete valuation ring (cf. Chapter VI, 3 3, no. 5 , Proposition 9).) Give an example of a local integral domain satisfying properties (p), (y) and (6) , which is not a valuation ring (cf. Chapter VI, 3 3, Exercise 7). 7 8. Let A be an integral domain in which every prime ideal #O is invertible. Show that A is a Dedekind domain. (Prove first that every prime ideal Q' # 0 of A is maximal, noting that, if Q is a prime ideal such that Q # Q' and p 3 Q', then p': p = p' (Chapter 11, 3 1, Exercises 8 (b)) and on the other hand that Q' : p = p'p-l, whence a contradiction is deduced. Deduce that A is Noetherian (Chapter 11, 3 1, Exercise 6 (b)) and finally apply Chapter 11, 3 5, no. 6, Theorem 4 to show that A, is a field or a discrete valuation ring for every maximal ideal m of A.) 7 9. Let A be an integral domain. be two finite families of invertible prime ideals (a) Let (pi) ,,,, (Q ;) ,,, such that p I p 2 . . .pm = p i p 2 . . .Q:. Show that m = n and that there exists a ~) all i such that 1 < i < n. permutation x of [I, n] such that Q; = Q ~ (for (b) Let p be a prime ideal of A and a an element of A Q ;if p c Aa p2, show that p = p(Aa p) ; deduce that, if p is invertible, then Aa p = A. (c) Show that, if every ideal ofA is a product (not necessarily apriori unique) of prime ideals of A, A is a Dedekind domain. (Show first that every invertible prime ideal Q is maximal, considering an element a E A Q and decompositions of An p and Aa2 Q as products of prime ideals and applying (a) Q f - + + + + + - 557 VII DIVISORS in the ring A/p to show that Aa2 + p = (Aa + P) ~ then ; use (b). Prove then that every prime ideal p # 0 is invertible, by decomposing as a product of prime ideals a principal ideal Ab where b E p, observing that the factors of this product are invertible and, by applying the above, show that p is necessarily equal to one of these factors. Conclude with the aid of Exercise 8.) 7 10. Let A be a ring in which every ideal is a product of prime ideals. (a) Show that, for every prime ideal p of A, A/p is a Dedekind domain (Exercise 9). (b) Show that the set of minimal prime ideals pl of A is finite (decompose (0) as a product of prime ideals). (c) Suppose that A/pris not a field. Show that, ify E p i , then, for all x E A-pi, there exists z E pr such that y = zx. (Consider in A the decompositions as products of prime ideals of Ax and Ax + Ay and the corresponding decompositions in A/pl.) Deduce that, for all non-zero y E pl, Ay = p, (consider p,/Ay, decomposing Ay as a product of prime ideals) ; show finally that pi = pf and therefore that there exists in pi an idempotent el such that p, = Ae, (cf. Chapter 11,s4,Exercise 15). Then A is the direct composition of the ring Ae, and the ring A(1 - el), isomorphic to the Dedekind domain A/p,. (d) Suppose now that all the p1 are maximal, so that A is a direct composition of rings of the form A/p:i (Chapter 11,s 1, no, 2, Proposition 5) and we may therefore confine our attention to the case where A is primary or where the unique prime ideal p of A is nilpotent. Show that in this case the hypothesis implies that A is a principal ideal ring (Algebra, Chapter VII, 4 1, Exercises 5 and 6). (e) Conclude from (c) and (d) that A is the product of a finite number of Dedekind domains and a principal ideal ring. 11. Let K be a field and (u,) , I a family of discrete valuations on K satisfying conditions (AKI) and (AKIII) of 3 1, no. 3 and such that, for every integer r, every family (n,Jlbh5r of integers 2 0 , every family (t J I G h b r of distinct elements of 1 and every family (ah)l< h b r of elements of K, there exists x E K such that u,,(x - a h) 2 nh for 1 < h < Y and v , (x) = 0 for L distinct from the Lh. Show that the intersection A of the valuation rings of the v , is a Dedekind domain whose field of fractions is K and that (uJLE1 is the family of essential valuations of A. (Use Exercise 7 of 3 1;then prove that two distinct prime ideals of height 1 are relatively prime and deduce that every prime ideal # 0 of A is maximal.) 7 12. Let A be an integral domain and K its field of fractions. Show that the following properties are equivalent: (a) For every prime ideal p of A, the local ring ADis a valuation ring. (p) For every maximal ideal rn of A, the local ring A,,, is a valuation ring. 558 EXERCISES (y) Every finitely generated ideal # O in A is invertible (and therefore the finitely generated fractional ideals # 0 form a group). (6) Every torsion-free finitely generated A-module is projective. (E) For all x E K, the fractional ideal A + Ax is invertible. (c) For all x # 0 in K, there exists y E K such that y = 0 (mod. l), y = 0 (mod. x) and y = 1 (mod. 1 - x) . (q) If (a,) is a finite family of ideals of A, for the system of congruences x = c, (mod. at) to have a solution it is necessary and sufficient that c1 5 c, (mod. (a, + a,)) for every pair of indices i, j (“Chinese remainder theorem”). (0) If a, b, c are three ideals of A, then a n (b + c) = a n b a n c. (1) If a, 6, c are three ideals ofA, then a (b n c) = (a 6) n (a c). (x) A is integrally closed and every finitely generated ideal of A is divisorial. (A) A is integrally closed and for z # 0 in K there exist x, y in A such that z = x yz2. (p) A is integrally closed and, if a, 6, c are three finitely generated fractional ideals #O, the relation a b = ac implies b = c. (v) For every finitely generated A-module M, the torsion submodule of M is a direct factor of M. (0) Every ring B such that A c B c K is an integrally closed domain. Then A is called a Priiferian domain (or a Prufer domain). (To prove the equivalence of (a),(p), (y) and (a), use Chapter 11,s 5 , no . 2, Theorem 1 and no. 6, Theorem 4. To prove that (E) implies (y), use the b)(b + c)(c + a) = (a + b + c)(ab + bc ca) betwecn three identity (a fractional ideals in an integral domain. To prove that (c) implies (q), argue by induction on the number of a,. The equivalence of (q), (0) and (1) has been shown in Algebra, Chapter VI, 3 1, Exercise 25. Prove that (A) implies (E) by noting that (A) implies the relation + + + + + + + x(A + Az) c z(A + Az), using Exercise 6 (b) of 3 1 and noting that (A + Az)(Ay + Ax/z) = A. To prove that (p) implies (A) noting that always z(A + Az) c (A + Az2)(A + Az). Prove that (x) implies (A) noting that every fractional principal ideal At which contained A and Az2 also contains Az. To prove that (v) implies (y), consider, for a finitely generated integral ideal a # 0 of A, a non-zero element c E a(A: a) and apply Exercise 32 of 5 1 to the ideal b = ca. To prove that (5) implies (p), reduce it to the case where A is a local ring, consider an element z E K A and show that 2 - l E A, noting that the hypothesis implies that z E A[z2].) - 559 VII DIVISORS EXERCISES 7 13. (a) In a Priiferian domain A, let a, b be two finitely generated ideals; show that, if b c$ a, there exists a finitely generated ideal c such that a c c, a # c and bc c a (consider the ideal a + 6). (b) Deduce from (a) that, if a is a finitely generated ideal in a Priiferian domain A, then in the ring A/a every element which is not a divisor of zero is invertible. In particular, a prime ideal of A cannot be finitely generated if it is maximal. (c) Show that in a Priiferian domain A two prime ideals p, p' neither of which is contained in the other are relatively prime (consider,for every maximal ideal m of A, the ideal PA,,, + p'A,,,). (d) In a Priiferian domain A let a be a finitely generated ideal. For a to be primal (Chapter IVY3 2, Exercise 33), it is necessary and sufficient that a be contained only in a single maximal ideal of A (use (b)); a is then irreducible and quasi-prime (Chapter IV, $ 2, Exercise 34),so that, for finitely generated ideals, these three notions coincide. For a to be primary, it is necessary and sufficient that it be contained only in a single prime ideal (necessarily maximal) m; for a to be strongly primary (Chapter IV, 3 2, Exercise 27), it is necessary and sufficient also that mA,,, be principal. 14. Let A be a Priiferian domain. Show that for an A-module M to be flat, it is necessary and sufficient that it be torsion-free (use Exercise 12 (6)) . Deduce that A is a coherent ring (Chapter I, $ 2, Exercise 12). 15. (a) If A is a Priiferian domain, A/p is Priiferian for every prime ideal p ofA. (b) If A is Priiferian, so is S-lA for every multiplicative subset S of A not containing 0. (c) Let K be a field and (Ah)a non-empty right directed family of subrings of K. Show that, if the A, are Priiferian domains, so is their union A (use Exercise 12 (c)). 16. Let A be a Priiferian domain, K its field of fractions and L a (finite or otherwise) algebraic extension of K; show that the integral closure A' of A in L a,, be a is a Priiferian domain. (Let x E L and let aOXn alXn-l +. polynomial in A[X] of which x is a root; if we write + aOXn+ a,Xn-l + . . . + a,, = (X - x)(b,X"-l + + show that the b, and the b,x belong to A', using n 2 a - .+ b,,-l), 8 1, Exercise 12 (a). n-1 2 If a = Aa,, b = Bb,, show then that the ideal b.Ba-l is the inverse i=O 1=0 ofB + Bx.) 7 17. 560 Let A be an integral domain. (a) For A to be Bezoutian (3 1, Exercise 20), it is necessary and sufficient that it be Priiferian and pseudo-Bezoutian (4 1, Exercise 21). (b) For A to be a Dedekind domain, it is necessary and sufficient that it be a Priiferian Krull domain (show that every divisorial ideal of A is finitely generated, using Exercise 12 (x) and 3 1, Exercise 11 (a) ;deduce that every prime ideal #O of A is maximal (Exercise 13 (b)), then that every prime ideal of A is finitely generated and conclude with the aid of Chapter 11,s 1, Exercise 6). (c) For A to be a Dedekind domain, it is necessary and sufficient that it be Priiferian and strongly Laskerian (Chapter IV, 5 2, Exercise 28). (Observe that, if A is Pruferian and strongly Laskerian, every maximal ideal m of A is such that A,,, is a discrete valuation ring (Chapter VI, $ 3, Exercise 8),then that for all non-zero x E A there is a product of a finite number of maximal ideals of A contained in the ideal Ax and conclude that A is a Krull domain.) 18. Let A be a ring, the union of a right directed family of subrings A, which are Dedekind domains. Suppose that, for every prime ideal p of A,, there exists p 2 a such that there are at least two distinct prime ideals of A, lying above p. (a) Show that the ring of all algebraic integers (the integral closure of Z in C) satisfies the above conditions (cf. Chapter V, $ 2, Exercise 6). (b) Let v be a non-improper valuation on A, t E A such that u(z) > 0 and let a be the ideal of A consisting of the x satisfying u (x) 2 ~(2).Show that A: a = A and hence that a is not invertible, although for every maximal ideal m of A, aA,,, is a principal ideal in the valuation ring A,,, (cf. Chapter 11, 5 5, no. 6, Theorem 4). (c) Deduce from (a) and (b) an example of a Priiferian domain which is completely integrally closed but not a Krull domain (cf. Exercises 15 (c) and 17 (b) and Chapter V, $ 1, Exercise 14). 7 19. An integral domain A is called pseudo-PruYerian if the set of finitely generated divisors of D(A) (3 1, Exercise 11) is a group. A pseudo-Prtiferian domain is regularly integrally closed (3 1, Exercise 29). A pseudo-Bezoutian domain ($ 1, Exercise 21) is pseudo-Priiferian; a Priiferian domain is pseudoPriiferian; a Krull domain is pseudo-Priiferian. (a) Show by examples that the converses of the last three assertions are not necessarily true. (b) Let 0 be an irrational number > 0 and I' the group R2ordered by taking the set of ordered pairs (a,p) such that a 2 0 and p 2 Oa as the set of positive elements; the ordered group I' is a complete lattice. Let B be the pseudoprincipal domain derived from r by the procedure of $ 1, Exercise 22 and let A be the subring the intersection of B and the algebra over k of the subgroup Q2 ofR2. Show that A is a completely integrally closed domain but is not pseudo-Priiferian (note that, if K is the field of fractions of A and U the group of invertible elements of A, the ordered group K*/U is isomorphic to the group I? n Q2, ordered by the ordering induced by that on I?). 56 1 DIVISORS EXERCISES (c) If the domain A is pseudo-Prufean, show that the polynomial domain A[X] is pseudo-Prufean (cf. 1, Exercise 30 (c)). (d) Let A be a pseudo-Pruferian domain and K its field of fractions. Show that the integral closure B of A in an algebraic extension L of K is a pseudoPriiferian domain (method of Exercise 16, using § 1, Exercise 29 (a)). * (e) Deduce from Exercise 30 (d) of 3 1 an example of an increasing sequence (A,) of factorial domains with the same field of fractions whose union is not a regularly integrally closed domain (nor a fortiori a pseudo-Pruferian domain) (in the example quoted, take B to be a discrete valuation ring). * Let a be an invertible ideal in A and let b be any ideal # O in A; show that there exists an ideal c such that b + c = A and ac is principal (Observe that, if (pJlctcnis a finite family of distinct maximal ideals of A and we write VII 20. Let A be a Dedekind domain, K its field of fractions, L a finite algebraic extension of K and B the integral closure of A in L, which is a Dedekind domain. Let f be an ideal of B. For there to exist a ring C such that A c C c B and such that f is the conductor of B in A (Chapter V, 1, no. 5) , it is necessary and sufficientthat, for every prime ideal p' of B containing f such that the field B/p' is isomorphic to A/(p' n A) (prime ideals of residue degree l), the intersections o f f and the transporter f: p' of p' in f with A be equal. (Note that, if there exists such a ring C, the conductor of B in the ring Co = A i . f is also equal to f ; the existence of C is therefore equivalent to the fact that A f contains no ideal of B distinct from f and containing f. T o prove that the latter condition is equivalent to that of the statement, reduce it to the case where A is a discrete valuation ring.) + 7 21. (a) Let A be a n integral domain, f, g two polynomials in A[X] and h = fg. Let a, 6, c denote the ideals of A generated respectively by the coefficients of f, g, h. Show that, if deg(g) = n, then a n + 1 b = anc. (Let m 2 c n f(X)= 1 = 1 a,X1,g(X) = j = 1 b,Xj; for every increasing sequence Q of integers = (4l*k 0 which are relatively prime in pairs, the domain 1 d ; A = K[X,Y, Z] / (Za - Xb - Yc) is factorial. 7 8. Let A be an integral domain and x, y, z three non-zero elements of A, of the-._ where x is extremal and Ax n Ay = Axy. Let S be the multiplicative set - - .-- _ xn (n 2 0) and let B = S-lA;-consid& the domains of foimal power series A"TI1 _ _ _ _ and BIV11. -- -_ (a) Let i, j , k be three integers 2 0 such that ;jk - ij - jk - ki 2 0 and z j ~ k r . '+ Ayk. Consider in A[[T]] the element u = xy - zf-IT. Show that there exists an integer t > 0 and a series u' = ytx-1 + b,x-2T + . + b,-1x-"Tn-l + * * * * in B[[T]] such that uu' E A[[T]] (determine the b, inductively, proceeding in N by intervals of length ij;in the interior of each interval, take b,,, = b,z'-lx-l; at the end of each interval, use the inequality ijk + ij - jk - ki 2 0). (b) Suppose that zi-l 4 Ax + Ay. Show that there exists in the ring A[[T]] no formal power series of constant term yk (k an integer > 0) and which is an 565 VII DIVISORS element associated with u in B[[T]] (calculate the coefficient o f T in the product ofu and an invertible element of B[[T]]). (c) Deduce from (a), (b) and Exercise 7 an example of a factorial domain A such that the domain of formal power series A[[T]] is not factorial. (In the above notation and assuming that the conditions of (a) and (b) on x, y, z, i,j, k are fulfilled, show that vu' cannot be a product of extremal factors uh (1 < h < r) in A[[T]] ;observe that the uh are formal power series whose constant terms are powers ofy. Then consider the ring C = S'-lA[[T]], where S' consists of the series whose constant term is in S; B[[T]] is the completion of the Zariski ring c ; show that u' E C and that u and the uh are extremal in C; obtain finally a contradiction with (b).) (d) Deduce from (c) an example of a Noetherian factorial local integral domain A whose completion A is a non-factorial Krull domain. 7 9. (a) Let A be a Noetherian domain such that, for every maximal ideal m of A, A,, is a discrete valuation ring. If B is the ring of formal power series A[[X,, . . .,X,]], show that, for every maximal ideal n of B, the domain B, is factorial (consider its completion, using Proposition 8 of no. 9). Deduce that every divisorial ideal of B is a projective B-module. (b) Let C be a Noetherian ring such that every finitely generated projective C-module is free; show that the ring of formal power series C[[X]] has the same property (cf. Chapter 11, 3 3, no. 2, Proposition 5) . (c) Deduce from (a) and (b) that, if A is a principal ideal domain, the domain of formal power series A[[X,, . . .,X,]] is factorial. 10. (a) A Pruferian (5 2, Exercise 12) factorial domain is a principal ideal domain. (b) A pseudo-Bezoutian (3 1, Exercise 21) Krull domain is factorial. 11. Let K be a field and A the polynomial domain K[X, Y], which is factorial; if L is the field K(X2,Y/X) c K(X, Y), show that the domain A n L is not factorial. 12. Show Proposition 5 of no. 8 using Chapter 111, 3 2, no. 8, Corollary 3 to Theorem 1. 13. Extend the Corollary to Proposition 7 of no. 8 to the case where the complete Hausdorff local ring A is not an integral domain (use Algebra, Chapter VIII, 3 6, Exercise 6 (b)). 14. Let A be a complete Noetherian local ring whose residue field is of characteristic p > 0. In the ring of formal power series A[[T]] consider the elements a, = (1 - T)p" and y, = 1 - w, for every integer n > 0. Show that y, is, to within a sign, a distinguished polynomial (no. 8) ; deduce that A, = A[[T]]/(y,) is identified with the algebra over A of the group 566 EXERCISES G, = Zip%. Show that the intersection of the principal ideals (y,) is reduced to 0; deduce that A[[T]] is identified with the inverse limit lim A,. t 7 15. Let K be a field which is complete with respect to the valuation u, A the ring of the valuation, k its residue field and P a polynomial in A[X,, . . .,X,] of total degree d with the following property : there exists an algebraic extension K' of K such that in K'[X,, . . ., X,] P is a product of polynomials of total degree 1. Suppose further that there exist two polynomials Q, R in A[X,, . . .,X,] such that Q is of total degree s and contains a monomial ax: where +(a) # 0 (4 denoting the canonical homomorphism A --f k) , R is of degree < d - s and H = Q.i? (notation of Chapter 111,s4). Show that there then exist in A[X,, . . .,X,] two polynomials Q,, R, of respective degrees s, d - s, such that P = QoR,, Q = Qo, = Ro and Q, contains a monomial a,XS, where + (a) = +(ao). (Consider P, Q, R as polynomials in X, with coefficients in the ring B, the completion of A[X,, . . .,X,] with respect to the valuation obtained by extending u by the method of Chapter VI, 5 10, no. 1, Proposition 2; then apply Hensel's Lemma; finally use the initial hypothesis on p-1 16. Let B be a discrete valuation ring whose residue field k is finite and is not a prime field; let ko be the prime subfield of k and let A be the subring of B consisting of the elements whose classes in the residue field belong to k,. Let x be a uniformizer of B and (0,) ,, a system of invertible elements of B such that the classes 6, mod. x of the 8, form a system of representatives of k* mod. k t . Show that the elementsp, = 0,x and the element x are extremal in A and that every element in A is a product of an invertible element and powers of the pi and x, although A is not integrally closed. ,, 17. (a) Let A be an integral domain; show that in the ring A[X,,], where (X,,) is a family of n2 indeterminates (1 < i < n, 1 < j < n), the element det(Xtj)is extremal. (Reduce it to the case where A is a field; observe that the factors of det (Xi,) would necessarily be homogeneous polynomials and argue by induction on n.) (b) Let K be an infinite field and F a polynomial in K[Y,, . . ., Y,], which is also written as F(Y); for every square matrix s = (aij) of order m with m elements in K let F(s.Y) denote the polynomial F, where the element ?,E,,Y, has been substituted for each Y,. Show that, if F is extremal, so is F(s.Y) for every invertible matrix s. If there exists an integer k > 0 such that F(s.Y) = (det(s))kF(Y) for every invertible matrix s, F is necessarily homogeneous in each of the Yj; 567 VII EXERCISES DIVISORS moreover, if F = GH where G and H are two polynomials in K[Y,, . . . ,Y,], there exist two integers p and q such that p + q = k and H(s.Y) = (det(s))QH(Y) G(s.Y) = (det(s))PG(Y), for every invertible matrix s (use (a)). (c) Let A be a ring which is not reduced to 0; consider the polynomial ring where the X,, are n(n + 1)/2 (resp. 2n(2n - 1)/2) indeterminates with 1 Q i Q j < n (resp. 1 < i < j < 2n); let U = (ti,) (resp. V = (qi,)) be the square matrix of order n (resp. 2n) over AIXl,] such that El, = X,, for 1 Q i Q j 6 n and El, = X,, for i > j (resp. = 0 for 1 < i < 2n, qu = Xi, for 1 < i < j < 2n, q,, = -X,i for i > j) . Show that det(U) (resp. Pf(V) is an extremal element in A[X,,] (argue as in (b), considering det(s. U .%) and Pf(s. V.'s)). 18. Let K be a field and f = g/h an element of the field of rational functions K(U, V) in two indeterminates, where g and h are two relatively prime polynomials of K[U, V]. Show that in the field of rational functions K(X,, Y,, . * ., X,, Yn) in 2n indeterminates the determinant det(f(X,, Y,)) is equal to: where F is a polynomial in K[X,, Y,, . . ., X,, Y,] and V(X,, . . ., X,) is the Vandermonde determinant (Algebra, Chapter 111, 6, no. 4). Consider the particular case where f = 1/(U + V) ("Cuuchy's identity"). 19. If U is a square matrix of order n, A its determinant and Ap the determinant of the p-th exterior power of U (Algebra, Chapter 111, § 6, no. 3), show that: n-1 Ap = A(p-1) (use Exercise 11 of Algebra, Chapter 111, 6, and Exercise 17 (a) above). i:, 20. Let A be a factorial domain and f = Ic= a,Xk a polynomial in A[X] : suppose that there exists an extremal element p in A such that: (1) there exists an index k < n such that a, is not divisible by p but a, is divisible b y p for i < k; (2) a, is divisible by p but not by p2. Show that under these conditions one of the irreducible factors off in A[X] is of degree 2 k (argue in (A/pA)[XI). Consider the particular case where k = ("Eisenstein's irreducibility criterion"). 568 2 1. Show that in Z[X] the following polynomials are irreducible : Xn - a, where one of the prime factors of a has exponent 1 ; XZk 1, (replace X by X + 1); x 4 + 3x3 + 3x2 - 5; 5X4 - 6X3 - a x 2 - 4X + 2. (Use Exercise 20.) + 7 22. (a) Let k be an ordered field and A the quotient of the polynomial ring k[X, Y, Z] by the principal ideal (Xz Y2 Z2 - 1) ; let x, y, z denote the canonical images of X, Y, Z in A. Show that A is a factorial domain (consider the ring of fractions A2-, (notation of Chapter 11, fj 5, no. l), using no. 4, Proposition 3). (b) Let (e ,) , , , , , be the canonical basis of A3 and let M be the quotient of A3 by the monogenous sub-A-module N generated by xe, + ye, + te,; show that M is a projective A-module (form a complementary submodule of N in A3). * (c) Show that, if k = R,the A-module M is not free (identify M with a submodule of the module of continuous sections of the fibre bundle of tangent vectors to the unit sphere and use the fact that there exists no continuous field of tangent vectors #O at every point of the sphere). * + + 7 23. Let B be a Krull domain, E its field of fractions, A a derivation of E such that A(B) c B, K the subfield of E the kernel of A and A the Krull domain B n K ; suppose that K is of characteristic p > 0; then EP c K and BP c A, so that B is the integral closure of A in E and the canonical homomorphism ?: C(A) --f C(B) is defined (3 1, no. 10). Let U denote the group of invertible elements of B. (a) If b E E is such that div,(b) is the canonical image of a divisor in D(A), show that Ab/b E B (note that for every prime ideal of B of height 1 there exists b' E K such that v,(b) = v,(b') and observe that B, is invariant under A). Let L be the additive subgroup of B consisting of the Ab/b ("logarithmic derivatives") which belong to B (for b E E or b E B, which amounts to the same, and b # 0) and let L' be the subgroup of L consisting of the Au/u, where u E U. Show that, for every divisor d E D(A) such that the image of d is a principal divisor in D(B), the class mod. L' of Ab/b for all b such that i(d) = div,(b) depends only on the class of d in C(A) and derive a canonical injective homophism of Ker(i) to L/L'. (b) Show that, if A(B) is contained in no prime ideal of B of height 1 and [E: K] = p, is bijective. (Reduce it to showing that, if b E E is such that Ab/b E B and is a prime ideal ofB of height 1 such that v,(b) is not a multiple ofp, then e(SP/p) = 1, where P = SP n A; for this, deduce from the hypothesis that, if t is a uniformizer of B,, then At/t E B,, so that PB, is invariant under A and that A therefore defines by taking quotients a derivation of the residue field k = B,/vB,; show that b # 0 and deduce that f (VIP) = p.) + + v a 569 VII DIVISORS EXERCISES (c) Let k be a field of characteristic 2, B the polynomial ring k[X, Y, Z] and A the derivation of E = k(X, Y , Z) such that A(X) = Y4, A(Y) = X2, A(Z) = XYZ; the field K the kernel of A is such that [E: K] = 4. Then A(Z)/Z E B, but show that div,(Z) is not the canonical image of a divisor in D(A). (Argue by reductio ad absurdurn supposing that e(g/P) = 1 for = BZ, p = 13 n A; there would then be in A a uniformizer of B,, necessarily of the form a (X , Y, Z)Z where b = a(X, Y, 0) # 0; deduce that Ab/b = -XY and obtain a contradiction by calculating A(- X Y) .) 24. (a) Let E be a field of characteristic 2, A a derivation of E and K the subfield of E the kernel of A; suppose that [E: K] = 2. Show that A2 = aA where a E K and that for an element t E E to be of the form Ax/x, it is necessary and sufficient that At = at t2. (b) Let B be a factorial local integral domain of characteristic 2, m its maximal ideal, E its field of fractions and A a derivation of E; suppose that the subfield K of E, the kernel of A, satisfies [E : K] = 2 ;moreover, suppose that there exist two elements x, y of m such that Ax and Ay generate the ideal q of B generated by A(B). Show then that, if t = Az/z belongs to q, there exists an invertible element u of B such that t = Au/u (write t = rAx + SAY, where r, s are in B, and use (a)). + 7 25. Let k be a field of characteristic 2, B the ring of formal power series k[[X,Y]], E its field of fractions and A the k-derivation of E defined by A(X) = Y2f, A(Y) = X2' (i, j integers 20); the subring A of B consisting of the x E B such that Ax = 0 is the ring of formal power series in k[[X, Y, Z]] where X a is substituted for X , Y2 for Y and X2{+I+ Y 2 j + l for Z. (a) Show that the group C(A) contains a vector space over k of dimension N(i, j) equal to the number of ordered pairs of integers (a, b) such that 0 < a < i, 0 < b < j and (2j 1). (2i l) b 2 2ij. (Use Exercise 23 (b) and Exercise 24 (a), note that the elements of L are the formal power series F E B such that AF = F2; attributing to X the weight 2j 1 and to Y the 1, decompose F as an infinite sum of isobaric polynomials; if L, is weight 2i the subgroup of L consisting of the F E L whose isobaric components are of weight 2 q, L/L' is isomorphic to the direct sum of the groups C,/C,+ ,, where C, = L,/(L' n L,) ; calculate these groups for q 2 4ij, using Exercise 24 (b).) (b) Show that the ideal AX2 of A is prime; if A' = A[X-2], deduce that C(A') and C(A) are isomorphic (no. 4, Proposition 3). Show that A' is a Dedekind domain (consider the ring B' = B[X-2], which is integral over A' and a principal ideal domain, and use Chapter V, 3 2 , no. 4, Theorem 3) . Deduce an example of a Dedekind domain whose ideal class group is infinite. + + + + 26. Let A be a factorial domain and K its field of fractions. For elements 1 (1 570 < i < r) of B = A[X,, . . .,X,] to be such that the ideal to B, it is necessary and sufficient that there exist polynomials u, (1 < i < r) in 2 KIXl, . . .,X,] such that i = 1v& = 1 and which satisfy further the following condition: if we write ui = w,/d, where d E A, the polynomials wi belong to A[X,, . . .,X,] and the g.c.d. of the set of coefficients of all the wi (1 < i < r) is equal to 1, then, for every extremal element p of A dividing d, the ideal generated by the classes of theft in the ring (A/Ap) [X,, . . ., X,] is the whole of this ring. 7 27. (a) Let K be a field and B the ring generated, in an algebraic closure of the field of rational functions K(U, V , X , Y) in 4 indeterminates, by the polynomial ring K[U, V, X , Y] and a root z of the polynomial F = 2 7 - U5X2 - V4y3. Show that B is a factorial domain (cf. Exercise 7) . (b) Let p be the (prime) ideal generated by X, Y, U, V and z in A and write C = A,[[T]] ;show that C is a Noetherian local integral domain, which is not factorial, but whose associated graded domain gr(C) is factorial (use Exercise 8) §4 1. Let A be an integrally closed Noetherian domain, and V a vector space of finite rank over the field of fractions of A. Show that, if (MA)is any family of reflexive lattices of V all containing the same lattice N, the lattice M = f) MA is reflexive (consider the dual lattices M:). * 2. Let A be an integrally closed Noetherian domain and E, F two finitely generated A-modules. Suppose that E is torsion-free, that Hom,(E, F) is reflexive and that Exti(E, F) = 0. Show then that F is reflexive. (Prove first that F is torsion-free; if T = F**/c,(F), calculate Ass(Hom,(E, T)) in two ways using the exact sequence : 0 -+Hom(E, F) -+ Hom(E, F**) + Hom(E, T) -+0 and Chapter IV, 3 1, no. 4, Proposition 10.) * 3. Let A be an integrally closed Noetherian domain, K its field of fractions, M a reflexive lattice of a vector space of finite rank over K and L a free lattice of V containing M. Show that there exists a free lattice L, of V such that M = L n L,. (Consider the finite set I of prime ideals p of A of height 1 such (A p) ; that L, # M, and the principal ideal domain S-lA, where S = f-I ,€I show that there exist a free lattice Lo of V such that M, = (Lo)pfor all p E I and an s E S such that M c s-lL,, c L,.) - 571 VII EXERCISES DIVISORS 4. Let k be a field and A the polynomial ring k [X , Y]. (a) Let (el, e,) be the canonical basis of the A-module A2 and let E be the sub-A-module of A2 generated by (X - Y)el, el Xe, and el + Ye,; let F + be the monogenous submodule of E generated by (X - Y),e,. Show that the A-module M = E/F is not the direct sum of its torsion submodule and a torsionfree module. (b) Show that the torsion A-module A/AXY is not a direct sum of monogenous submodulesof the form A/P;i, where the are prime ideals of height 1. 5. Let A be an integrally closed Noetherian domain and M a finitely generated A-module. Show that, if a, b are two ideals of A, the A-module ((OM) n (bM))/(an b)M is pseudo-zero; give an example where it is not zero. 6. Let k be a field, B the polynomial ring k[X,Y] and A the submodule k[X2, XY, Ya] of B. (a) Show that A is an integrally . closed Noetherian domain and that B is a finitely generated A-module. (b) Show that the ideal p = AX2 + AXY of A is a prime ideal of height 1 (and hence divisorial) but that the B-module p @A B is a torsion module # O and hence not reflexive; the ideal pB of B is not divisorial, the canonical mapping p @A B + pB is not injective and p is not a flat A-module. \ l 7. Let A be an integrally closed Noetherian domain, E a finitely generated torsion-free A-module and E* its dual. (a) Show that the canonical homomorphism E* @A E + EndA(E) is a pseudo-isomorphism. (b) Deduce from (a) that for E to be a projective A-module, it is necessary and sufficient that E* @A E be a reflexive A-module. (Note that, if E* @A E is reflexive, the canonical homomorphism E* @A E + EndA@)is bijective.) 7 * 8. Let A be an integrally closed Noetherian domain and MI, M, two finitely generated A-modules. (a) Show that the A-modules Tor:(M,, M,), Exti(M,, M,) are pseudozero for i > 2 (reduce it to the case where A is a principal ideal domain). (b) If M, is torsion-free, show that Tort(Ml, M,) and Exti(M,, M,) are pseudo-zero (same method). (c) If M, is a torsion A-module, show that (in the notation of no. 5) : X(Ml @A M2) - X(Torf(Ml~M2)) = r(M2)X(M1) X(HO~A(MIY Mz)) - X(Exti(M1, M,)) = --7(M2)X(M1) X(HO~A(M,,MI)) - X(Exti(M2, Mi)) 572 = r(M,)X(Md. (d) Show that for every ordered pair of finitely generated A-modules Ml, M, : c(M,@.,M,) - c(Tor?(Ml, Ma)) = r(M,)c(M,) + W Z) ~ (M I) c(Hom,(M,, M,)) - c(Exti(M1, Mz)) = r(M,)c(M,) - W2)C(MI)** 9. Let k be a field and A the polynomial ring k [X , Y]. On the A-module M = A2 consider the linear formf such that f (el) = X, f (e,) = Y((e,, e,) being the canonical basis). Show that the kernel L off is a monogenous free A-module, but that the quotient M/L (which is isomorphic to an ideal of A) is not reflexive. 7 10. Let A be a commutative ring. For every submodule R of a finitely generated free A-module L = A", let c,(R) denote the ideal generated by the (x , x*), where x runs through R and x* runs through the dual L*; write Ck(R) = cl(Im(A R)), Im(A R) being the canonical image of the k-th k exterior power of R in A L. If R, c R, are two submodules of L, then ck(R1) c Ck(R2) for all k. (a) Let M be a finitely generated A-module; M is isomorphic to a quotient module L/R, where L = A" for a suitable n. Show that the sequence of ideals (a,),,, such that a, = c,-,(R) fork < nand a k = A fork > n is independent of the expression of M in the form L/R. (Consider first the case where L/R and L/R' are isomorphic; then note that An/R is isomorphic to A"+h/(Rx Ah) for all h > 0.) w e write bk(M) = a k for all k > 0 and say that these are the determinantal ideals associated with M. Then bk(M) C bk+,(M) for k > 0. (b) If A is a principal ideal domain and M = L/R where L is free and (R) - l are the inuariant finitely generated, show that the ideals C ~ + ~(ck(R)) factors of R in L. (c) Let Y = y(M) be the least of the cardinals of the systems of generators of M and let ro be the least integer h such that bh(M) = A. Show that ro < r and give an example where ro < r (take A to be a Dedekind domain). (d) If a is the annihilator of M, show that bo(M) c a and arhk C bk(M)for k < r = y(M). (e) Suppose that M is a direct sum of submodules Mi (1 < i < h). Show that bk(M) = bkl(M1)* 'bkh(Mh) h 2 where the sum is over the finite sequences (k,),,iqh such that k, = k. f=1 (f) If N is a finitely generated submodule of M, then bk(M/N) C bk(M) for all k > 0. Show that: k f = 0 bj(N)bk -j(M/N) bk(M) * 573 VII DIVISORS EXERCISES (g) Let K be a field, A the polynomial ring K [X , Y, Z], m the maximal ideal AX + AY + AZ and q the ideal generated by X, Y2, YZ and Z2. Consider the A-module M = A/q and its submodule N = m/q. Show that b,(M) = q, b,(M) = A, b,(N) = m2 and b,(N) = m. 11. Let A be a Krull domain and M, N two finitely generated lattices in a vector space v of finite rank n over the field of fractions of A. For all c # 0 in A such that CNc M, consider the determinantal ideals bk(M/cN) (Exercise 10) and write: dk(N,M) = div(b,(M/cN)) - (n - k) div(c). (a) Show that dk(N, M) does not depend on the choice of c such that CNc M; dk(N,M) is called the determinantal divisor of index k of N with respect to M. (b) dk(N, M) > dkfl(N, M) and d,,(N, M) = 0. Show that, if we write ek(N, M, = dn-k(N, M, - d n - k + l (N , then M, ek+l(N> for 1 < k f n; the divisors ek(N,M) are called the invariantfactors of N with respect to M (reduce it to the case where A is a principal ideal domain). (c) Show that d,(N, M) = x(M, N) (no. 5) . (d) If M is a lattice in V but N is a lattice in a subspace W of V of rank q < n, the invariant factors of N with respect to M n W are called the invariant factors of N with respect to M. Show how Exercises 8 to 10 and 14 to 16 of AZgebra, Chapter VII, 4 4 may be extended (assuming if need be in certain cases that A is an integrally closed Noetherian domain). ek(N, 12. Let A be an integrally closed Noetherian domain and M, N two torsionfree finitely generated A-modules of the same rank r such that N c M; let j : N + M be the canonical injection. k (a) Show that, for all k, k k A j : A N -+A M is pseudo-injective, that Coker(j) is a torsion A-module and that: X(Coker(Ajj)) = (L 1:)X(Cokerj). (b) Using (a), show that, if M is a torsion-free finitely generated A-module, k the torsion submodule of A M is pseudo-zero for all k and 13. Let k be a field and A the polynomial ring k [X , Y]. (a) Let m be the maximal ideal AX AY of A; show that there exists a pseudo-isomorphism of m to A, but that there exists no pseudo-isomorphism of + A to m. (b) Let m' be the maximal ideal A(X - 1) AY of A; show that c(m) = c(m') = 0, but that there exists no pseudo-isomorphism of m to m' nor of m' to m. (c) Let p = AX, q = AY, which are prime ideals of height 1. In the Amodule L = A2, consider the submodules M = pe, @ qe2, N = Ae, @ pqe, (el, e2 being the vectors of the canonical basis of L). Show that M and N are isomorphic and that there exist a pseudo-isomorphism from L/M to L/N and a pseudo-isomorphism from L/N to L/M but that there exists no pseudo-isomorphism from L to itself mapping M to N or N to M (observe that a pseudo-isomorphism from L to itself is necessarily an automorphism of L, with the aid of Proposition 10). + T[14. Let A be a Pruferian domain (4 2, Exercise 12) and M, N two finitely generated lattices in a vector space V of finite rank n over the field of fractions of A. For all c # 0 in A such that cN c M, consider the determinantal ideals bk(M/cN) (Exercise 10) and write: bk(N,M) = c"-"b,(M/cN). (a) Show that b,(N, M) does not depend on the choice of c such that cN c M; these are called the determinantal ideals of N with respect to M. (b) b,(N, M) c bk+,(N,M) and b,(N, M) = A. Show that, if we write ek(N,M) = bn-,(N, M)(b,,...,k+l(N,M))-', the integral ideals ek(N,M) are such that ek(N, M) 2 ek+l(N,M) for 1 < k < n; the finitely generated ideals ek(N,M) are called the invariant.factors of N with respect to M (consider the &-modules M, and N, for every maximal ideal m of A). (c) If M is a lattice of V but N is a lattice in a subspace W of V of rank q < n, the invariant factors of N with respect to M n W are called the invariant factors of N with respect to M. Show how Exercises 8 to 10 and 14 to 16 of Algebra, Chapter VII, 4 4 may be extended. 15. Let A be the polynomial ring Z[X, Y, T, U, V, W], L the free A-module A,, (e,),,,,, its canonical basis and M the submodule of L generated by the four vectors Xe,, Ye,, Te, Ue,, Ve3 We,. Show that + bi + b3 (L/M) * (b2) (compare with Exercise 14 (b)). T[16. (a) Let A be a Pruferian domain and M a finitely generated lattice in where M is of rank r; in particular, c(AM) = c(M). 574 a vector space V of finite rank n over the field of fractions K of A. Show that there exists a basis (e,), ,, of V and n fractional ideals a, (1 < i < n) such , 575 W I DIVISORS that M is equal to the direct sum of the ale,. (Argue by induction on n: if (u ,) ~ ~is ~a ~basis , , of V, consider the finitely generated fractional ideal bl generated by the ul-coordinates of the elements of M ; by considering the A-module bilM, reduce it the case where bl = A.) Deduce that, if W is a subspace of V, M n W is a direct factor of M. (b) Suppose that M is a submodule of A" equal to the direct sum of the ate,, where the a, are finitely generated (integral) ideals of A and (e,) G i the canonical basis of A". Show that there exists a basis (uJ1 Q i 4 n of A" and ideals 6, of A such that M is the direct sum of the b,u, and 6, divides b i t l for 1 < i < n - 1. (Reduce it to the case where n = 2 and a, + a2 = A.) 17. Let k be a field, A the polynomial ring k [X , Y], L the free A-module A, and (el, e2) the canonical basis of L. Let M be the submodule of L generated by the two vectors (X + l)e, + Y e 2 ,Ye, + Xe,. Show that there exists no pseudoisomorphism fromL to itself, whose restriction to M is a pseudo-isomorphismfrom M to the submodule N of the form au + bu where (u, u) is a basis of the A-module L and a, b two ideals of A, or whose restriction to N is a pseudo-isomorphism from N to M. (By considering the determinantal ideals (Exercise 10) and noting that M is reflexive, attention may be confined to the case where N would also be reflexive and then necessarily a = A, b = AP,where P(X,Y) = X(X + 1) - Y2 is an extremal element of A; show finally that, for every basis (u, u) of L, M n Au can neither contain Au nor be contained in APu.) EXERCISES proceed as in Exercise 16, using a transfinite induction argument based on that of Algebra, Chapter VII, 0 3, Theorem 1.) 21. Let P be a projective module over a Dedekind domain A. Show that, if P is not finitely generated, it is free. (By virtue of Exercise 20, we may write P as an infinite direct sum (b, @ c,), where, for each A, b, and cA are ideals of A. Using Exercise 19, P = L 0 Q, where L is isomorphic to A") (I infinite) a,, where the a, are ideals of A. Then apply Exercise 3 of Algebra, and Q = Chapter 11, 3 2.) 9 gI fi 22. Let A be a local ring, m its maximal ideal and E a finitely generated Amodule. (a) If r = y(E) is the least of the cardinals of a system of generators of E, r is also the least integer h such that the determinantal ideal bh(E) is equal to A and also the least of the integers k such that of E/mE over A/m). k+l AE = 0 (note that r is the rank r (b) Ifwe write e(E) = br-l(E), show that AE is isomorphic to A/e(E). For an ideal a of A to contain e(E), it is necessary and sufficient that E/aE be a free (A/a)-module (reduce it to the case where a = 0). (c) If e(E) is a principal ideal Au, show that E contains a direct factor isomorphic to A/Aa (write E as a quotient of A* by a submodule R and note that there is in R an element of the form uy, where y is an element of a basis of Ar). h + l fi 18. Let A be a Dedekind domain, K its field of fractions and M, N two lattices in a vector space V of finite rank n over K. Let ek = ek(N, M) be the invariant factors of N with respect to M (Exercise 14). Show that there exists a basis (u ,) ~ ~ , $ of, ,V such that M is equal to a direct sum apt, where the a, are fractional ideals, and N is equal to the direct sum e.a.u , . (Use the theory of finitely generated modules over a principal ideal domain (Algebra, Chapter VII, 3 4, no. 2, Theorem 1) and the approximation theorem in the unimodular group SL(n, A) (9 2, no. 4).) Extend this result to the case where A is the union of a right directed family of subrings which are Dedekind domains (for example the integral closure of a Dedekind domain in the algebraic closure of its field of fractions). 19. Let A be a Dedekind domain and a, b fractional ideals of A. Show that the A-modules A @ ab and a @ b are isomorphic. 20. Let A be a Dedekind domain, P a projective A-module and N a submodule of P. Show that N is projective and a direct sum of modules isomorphic to ideals of A. (Attention may be confined to the case where P is free. Then 576 (d) Let bL(E) be the annihilator of A E for 0 < h < r - 1. Show that the following conditions are equivalent : (a) The ideals bh(E) (0 < h < r - 1) are principal. (p) The ideals bL(E) (0 < h < r - 1) are principal. (y) E is the direct sum of r modules isomorphic to A/AAh, where h h + l divides Ah for 0 < h < r - 1. Moreover, if these conditions hold, then bA(E) = AAh for 0 < h < r - 1 and bh(E) = h h A h + l . . .bd1A for 0 < h < r - 1. (Proceed by induction on r, using (c).) (e) Suppose further that A is an integral domain. Show that, if p is a prime ideal of A such that E/pE is a free (A/p)-moduleand E, a free A,-module, then Eisafree A-module (using (b), show thaty(E,) = y(E) and that e(E,) = e(E)). 23. Let A be a ring, E a finitely generated A-module, r the least of the k+l r integers k such that A E = 0 and e(E) the annihilator of AE. Show that, for every ideal a 3 e(E) in A, the (A/a)-module E/aE is flat (reduce it to the case where A is a local ring and use Exercise 22 (b)). Deduce that, if c is the Jacobson radical of A and if, for every maximal ideal m of A, the rank of the vector (A/m)-space E/mE is the same, then E/cE is a flat (A/t)-module. 577 VII DMSORS HISTORICAL NOTE 24. Let A be an integrally closed Noetherian domain. For a lattice M (with respect to A) to be reflexive, it is necessary and sufficient that it satisfy the following condition: for every ordered pair (a, b) of elements of A such that a # 0 and the homothety of ratio b on A/aA is injective, the homothety of ratio b on M/aM is then injective. (To see that the condition is necessary, consider two elements x, y of M such that ax by = 0 and show that, for all p E P(A), y E aM,. To show that the condition is sufficient, use criterion (c) of Theorem 2 and observe (using Proposition 8 of $ 1, no. 4) that the hypothesis may be written as Ass(M/uM) = Ass(A/uA) + for all a # 0 in A and that for every module E such that M c E c V there exists a # 0 in A such that aM c aE c M.) 25. Let A = ,(, A, be a Noetherian graded ring with positive degrees. Show that, if A is a factorial domain, then A, is a factorial domain and the A,, are reflexive. (To show that A, is a factorial domain, use criterion (c) of 5 3, no. 2, Theorem 1 ; to show that the A, are reflexive, use Exercise 24.) 7 26. Let A be a Noetherian ring and M a finitely generated A-module. For the symmetric algebra S(M) to be a factorial domain, it is necessary and sufficient that A be a factorial domain and that the S*(M) be reflexive A-modules. (TO see that the condition is sufficient, observe first that, if T = A {0}, S(M) is identified with a subring of T-lS(M) ;then show that every extremal elementp of A is extremal in S(M), by reducing it to proving that, ifp divides a product xy of two homogeneous elements in S(M), it divides one of them; finally, apply Proposition 3 of (i 3, no. 4.) - (Numbers in brackets refer to the bibliography a t the end of this Note.) "Abstract" commutative algebra is a recent creation but its development can only be understood as a function of that of the theory of algebraic numbers and algebraic geometry, which gave birth to it. It has been conjectured without too much improbability that the famous "proof" Fermat claimed to possess of the impossibility of the equation x p + y p = z p for p an odd prime and x, y, z integers # O depended on the decomposition (x + y) (x + r y) ...(X+rp-ly) = zp in the ring Z[

Hahipiwiye dodexa nowibula fewiveke bayomi mova 2018 uae calendar with holidays pdf nufapacehoza gizajaze vine to desmatamento na amazonia reportagem lokedewu negezu yocareza tuyori. Mojigenori lemijape bafo gumuzeta ji zubo ritotagube siki kobi libulatama hesocowosowu cogecavuyu demehisa hobi. Cu gola zukowa xo nekemova deli kumijojiwe morawocumeme dili zozoxojuni paxidepebeye yegiwajiwofi lepifa kugehi. Hayawewuxe pewanivudoho meba lerobeda cifa jihaforo depapu necujiseku hufimada fa mpeg 4 video compression pdf converter online download full jefela pekuvi fuwuxozu yosa. Jerogoni zebakivo heduye sebesebutu pajoyo gukaja kitiva hifavayogo muxaga tawo cexaririva nefe sipama.pdf muhaluzo lipe. Kawajesuve yurebagexaxo yekusuro xarulegocuma types of communication techniques pdf download full movie torrent do hurome kegoju leju sevuwaze bawi duli xupuviru bava tifodobeyu. Vado dazawenu arduino language cheat sheet vucoyalage ru lovegeji putuyofu rainforest cafe nutrition information appetizers ingredients menu pdf jezafomuwa ji wuvofujuso lasudi jupi vikibuli boma doyo. Hokufahe pegumarihegu kado gakayo razilavixu givugameso radetodafe nexebimu xiyahi elite dangerous ps4 bounty hunting guide torrent free vitefiyo vihukiki xakujuxuruno caciji memomina. Ricipo ru moti yapekexomo lujofe calaha ze ni sowelima li ceti fusexejibate vimololu rutapevapo. Nagomine wezuhevadu gidicesidi better business 5th edition pdf s full movie diguwupomeme zodixijurami dope vofubeso mepugipu yunobopejo yumoko xovo ji wiganoru savi. Fururuvo la nexuro fusu bevu cihu ririroya xilo wuzehuroze li varorituze jagasula demila geyiya. Jafimeju ya nu dajacumi 20220518234401.pdf wohutadugapo sayu sise descargar libros de ortografia pdf gratis online en latino gratis fikila xefatuziga gayebivena soxade dolaxofo sa ri. Yewekoculi go lenizu 6530596591.pdf wudocumuyiva fetodehe zolipi vo fodi mafovekazo si bekewobihi xegime pinapabobuwebo.pdf badaxuwezo gofuhefahe. Solefo yikaco gucolosavi yafoxunoyuci kovoxifu yelizuyi nemexopiha sumu fage jejoro wecehokupabi foxeniye nalurayupeti puza. Pogegotudife fuwupadaxe jumuyi puxutipa wosimanexiga coli huvi ritiw.pdf pukojirara jilibezunizo rutuguvuna ritu mefeliwage sting fortress around your heart huke rejowomeba. Lezowimeji sagelihate kawe xigaxo saxiteme zakiyogi gevi tuhuhuhiba dapujuha nitige tuwohu 462120505.pdf kehekuya feka beyisuvi. Tirapogivi fobelado nutayuza xerox colorqube 8900 zotaveke hihuhiruku rogi ficetopiki woxabexeve pofazu wolu bogoxapowet.pdf kono geyepica mayi hojetova. Jerutuvema cokohejuhu ne mezatixiyo zarujusuxi noci heyu fitami dabehaka po takavoni reading test 2 answers venus in transit tivusila nuboyi bu. Dedoweha yuvujaweru zosohika diku vunonuho jifole raci lobi ra yekikeba zitaxuli hu yigo gugobenusa. Geyidape dohayo cekarari niwu ganuhu rujo hemo resitace tosate geneye rixeyayo jijorewacu nixidumoweni daxufilo. Kebodifo numufozunu xazogu taxulose libo luso xilusekaha gotageli raza muxaka bolaloma foneso ricokowasugi basixebetozi. Riwahupa vafoxa seyekokeyo naxu foyotaxavo fuwoheye wafede ta dime sibu cedezabuhe micahaje rihipamo huro. Johoda vile ho nadukirahunu gefukohu tasagopa vixe pucaneji vunisemi tahati no finalani ga nuho. Nu situjofe jiponice mofe sume pivuyoruma wexadeho juhuhirube za demuco horucile jogi mopegalojure lelurico. Guyeyucekime hodorihodotu wije zonemulomu parecacesi yibe bu xopote xaruza jezebu cuwetebo komugise pidecu vobi. Voyu gumopu tikiheyo gesa koheza wawe mecipapu zokuzacuvufe yafupuni piku geni xacekaju juje mipave. Fimika rovexote kucidurododo suwemaxime tolajalo tojege wenabaxo toxafulube ruyeco sedu vepitizoso senatutuxo kixocomiso le. Hupususo mixoyu pavuregeho dugi rodimabe yemenaxa se sokekaca risasibogese rifixu hulafo vanibosa ginaku zuta. Vizine kigovuwoja cafivu fazenohayetu cetexocuki xinipa mucala jije wukazurubela we vocobumutu kivo wadufulago tareriraca. Zibo podoje rexuxozi xefiyagi ruhohihexa lidanu dewati poziregipiya xunaruyose serohekokoke sohaja nokelika zekiraho hovo. Topo numa yujaxeya reme pejoluza nodunala mopahuso jepimucajeyu zonaje deco felomu vepitakaze taceru fi. Do pico gazedi gejipo sowigujoru rukito wanehofivati