Hideyuki Matsumura,
Professor of Mathematics at Nagoya University, received his graduate training at Kyoto University and was awarded his Ph.D. in 1959. Formerly Associate Professor of Mathematics at this university, Professor Matsumura was a research associate at the University of Pisa during 1962 and 1963. He was also Visiting Associate Professor at the University of Chicago (1962), at Johns Hopkins University (1963), at Columbia University (1966-1967), and at Brandeis University (1967-1968).

The author spent 1973 and 1974 as Visiting Professor at the University of Pennsylvania, 1974 and 1975 as Visiting Professor at the Politecnic of Torino, and 1977 as Visiting Professor at the University of Münster.

Commutative Algebra
This book, based on the author's lectures at Brandeis University in 1967 and 1968, is designed for use as a textbook on commutative algebra by students of modern algebraic geometry or abstract algebra.

Part I is devoted to basic concepts such as dimension, depth, normal rings, and regular local rings; Part II deals with the finer structure theory of noetherian rings initiated by Zariski and developed by Nagata and Grothendieck.

In this second edition, the chapter on Depth has been completely rewritten. There is also a new Appendix consisting of several sections, which are almost independent of each other. The Appendix has two purposes: to prove the theorems used but not proved in the text; to record some of the recent achievements in the areas connected with Part II.

For specialists in commutative algebra, this book will serve as an introduction to the more difficult and detailed books of Nagata and Grothendieck.
To geometers, it will be a convenient handbook of algebra.

Review of the First Edition:
"This is an excellent book which contains a wealth of material...Part I, for which the prerequisites are minimal, develops the main concepts, central to modern commutative algebra...Part II, is considerably more advanced..."
– American Mathematical Monthly

The Benjamin/Cummings Publishing Company
Advanced Book Program

Matsumura

Commutative Algebra
SECOND EDITION

MATHEMATICS
LECTURE NOTE SERIES

MATHEMATICS LECTURE NOTE SERI

Commutative Algel

SECOND EDITION

Hideyuki Matsumura

QA
251.3
M37
1980

E BENJAMIN/CUMMINGS PUBLISHING COMP.
Advanced Book Program

MATHEMATICS LECTURE NOTE SERIES

Volumes of the Series published from 1961 to 1973 are not officially numbered. The parenthetical numbers shown are designed to aid librarians and bibliographers to check the completeness of their holdings.

ISBN			
0-8053-5801-3	(1)	S. Lang	Algebraic Functions, 1965
0-8053-8703-X	(2)	J. Serre	Lie Algebras and Lie Groups, 1965 (3rd printing, with corrections, 1974)
0-8053-2327-9	(3)	P. J. Cohen	Set Theory and the Continuum Hypothesis, 1966 (4th printing, 1977)
0-8053-5808-0 0-8053-5809-9	(4)	S. Lang	Rapport sur la cohomologie des groupes, 1966
0-8053-8750-1 0-8053-8751-X	(5)	J. Serre	Algèbres de Lie semi-simples complexes, 1966
0-8053-0290-5 0-8053-0291-3	(6)	E. Artin and J. Tate	Class Field Theory, 1967 (2nd printing, 1974)
0-8053-0300-6 0-8053-0301-4	(7)	M. F. Atiyah	K-Theory, 1967
0-8053-2434-8 0-8053-2435-6	(8)	W. Feit	Characters of Finite Groups, 1967
0-8053-3555-4	(9)	Marvin J. Greenberg	Lectures on Algebraic Topology, 1966 (6th printing, with corrections, 1979)
0-8053-3757-1	(10)	Robin Hartshorne	Foundations of Projective Geometry, 1967 (3rd printing, 1978)
0-8053-0660-9	(11)	H. Bass	Algebraic K-Theory, 1968
0-8053-0668-4	(12)	M. Berger and M. Berger	Perspectives in Nonlinearity: An Introduction to Nonlinear Analysis, 1968
0-8053-5208-2 0-8053-5209-0	(13)	I. Kaplansky	Rings of Operators, 1968
0-8053-6690-3 0-8053-6691-1	(14)	I. G. MacDonald	Algebraic Geometry: Introduction to Schemes, 1968
0-8053-6698-9 0-8053-6699-7	(15)	G. W. Mackey	Induced Representation of Groups and Quantum Mechanics, 1968
0-8053-7710-7 0-8053-7711-5	(16)	R. S. Palais	Foundations of Global Non-linear Analysis, 1968
0-8053-7818-9 0-8053-7819-7	(17)	D. Passman	Permutation Groups, 1968
0-8053-8725-0	(18)	J. Serre	Abelian *l*-Adic Representations and Elliptic Curves, 1968
0-8053-0116-X	(19)	J. F. Adams	Lectures on Lie Groups, 1969
0-8053-0550-5	(20)	J. Barshay	Topics in Ring Theory, 1969
0-8053-1021-5	(21)	A. Borel	Linear Algebraic Groups, 1969
0-8053-1050-9	(22)	R. Bott	Lectures on K(X), 1969
0-8053-1430-X 0-8053-1431-8	(23)	A. Browder	Introduction to Function Algebras, 1969
		G. Choquet	Lectures on Analysis (3rd printing, 1976)
0-8053-6955-4	(24)		Volume I. Integration and Topological Vector Spaces, 1969
0-8053-6957-0	(25)		Volume II. Representation Theory, 1969
0-8053-6959-7	(26)		Volume III. Infinite Dimensional Measures and Problem Solutions, 1969
0-8053-2366-X 0-8053-2367-8	(27)	E. Dyer	Cohomology Theories, 1969

MATHEMATICS LECTURE NOTE SERIES *(continued)*

ISBN			
0-8053-2420-8 0-8053-2421-6	(28)	R. Ellis	Lectures on Topological Dynamics, 1969
0-8053-2570-0 0-8053-2571-9	(29)	J. Fogarty	Invariant Theory, 1969
0-8053-3080-1 0-8053-3081-X	(30)	William Fulton	Algebraic Curves: An Introduction to Algebraic Geometry, 1969 (5th printing, with corrections, 1978)
0-8053-3552-8 0-8053-3553-6	(31)	M. J. Greenberg	Lectures on Forms in Many Variables, 1969
0-8053-3940-X 0-8053-3941-8	(32)	R. Hermann	Fourier Analysis on Groups and Partial Wave Analysis, 1969
0-8053-4551-5	(33)	J. F. P. Hudson	Piecewise Linear Topology, 1969
0-8053-5212-0 0-8053-5213-9	(34)	K. M. Kapp and H. Schneider	Completely O-Simple Semigroups: An Abstract Treatment of the Lattice of Congruences, 1969
0-8053-5240-6 0-8053-5241-4	(35)	J. B. Keller and S. Antman, (eds.)	Bifurcation Theory and Nonlinear Eigenvalue Problems, 1969
		O. Loos	Symmetric Spaces
0-8053-6620-2 0-8053-6621-0	(36)		Volume I. General Theory, 1969
0-8053-6622-9 0-8053-6623-7	(37)		Volume II. Compact Spaces and Classification, 1969
0-8053-7024-2 0-8053-7025-0	(38)	H. Matsumura	Commutative Algebra, 1970 (2nd Edition—cf. Vol. 56)
0-8053-7574-0 0-8053-7575-9	(39)	A. Ogg	Modular Forms and Dirichlet Series, 1969
0-8053-7812-X 0-8053-7813-8	(40)	W. Parry	Entropy and Generators in Ergodic Theory, 1969
0-8053-8350-6 0-8053-8351-4	(41)	W. Rudin	Function Theory in Polydiscs, 1969
0-8053-9100-2 0-8053-9101-0	(42)	S. Sternberg	Celestial Mechanics Part I, 1969
0-8053-9102-9	(43)	S. Sternberg	Celestial Mechanics Part II, 1969
0-8053-9254-8 0-8053-9255-6	(44)	M. E. Sweedler	Hopf Algebras, 1969
0-8053-3946-9 0-8053-3947-7	(45)	R. Hermann	Lectures in Mathematical Physics Volume I, 1970
0-8053-3942-6	(46)	R. Hermann	Lie Algebras and Quantum Mechanics, 1970
0-8053-8364-6 0-8053-8365-4	(47)	D. L. Russell	Optimization Theory, 1970
0-8053-7080-3 0-8053-7081-1	(48)	R. K. Miller	Nonlinear Volterra Integral Equations, 1971
0-8053-1875-5 0-8053-1876-3	(49)	J. L. Challifour	Generalized Functions and Fourier Analysis, 1972
0-8053-3952-3	(50)	R. Hermann	Lectures in Mathematical Physics Volume II, 1972
0-8053-2342-2 0-8053-2343-0	(51)	I. Kra	Automorphic Forms and Kleinian Groups, 1972
0-8053-8380-8 0-8053-8381-6	(52)	G. E. Sacks	Saturated Model Theory, 1972
0-8053-3103-4	(53)	A. M. Garsia	Martingale Inequalities: Seminar Notes on Recent Progress, 1973
0-8053-5664-3 0-8053-5666-5	(54)	T. Y. Lam	The Algebraic Theory of Quadratic Forms, 1973 (2nd printing, with revisions, 1980)
0-8053-6702-0 0-8053-6703-9	55	George W. Mackey	Unitary Group Representations in Physics, Probability, and Number Theory, 1978

MATHEMATICS LECTURE NOTE SERIES *(continued)*

ISBN			
0-8053-7026-9	56	Hideyuki Matsumura	Commutative Algebra, Second Edition, 1980
0-8053-0360-X		Richard Bellman	Analytic Number Theory: An Introduction, 1980

Other volumes in preparation

COMMUTATIVE ALGEBRA

Second Edition

HIDEYUKI MATSUMURA

Nagoya University, Nagoya, Japan

1980

THE BENJAMIN/CUMMINGS PUBLISHING COMPANY, INC.
ADVANCED BOOK PROGRAM
Reading, Massachusetts

London · Amsterdam · Don Mills, Ontario · Sydney · Tokyo

Hideyuki Matsumura

Commutative Algebra

First Edition, 1969
Second Edition, 1980

Library of Congress Cataloging in Publication Data

Matsumura, Hideyuki, 1930-
Commutative algebra.

(Mathematics lecture note series ; 56)
Includes indexes.
1. Commutative algebra. I. Title.
QA251.3.M37 1980 512'.24 80-11958
ISBN 0-8053-7026-9

Main body of the text reproduced by The Benjamin/Cummings Publishing Company, Inc., Advanced Book Program, Reading, Massachusetts, from camera-ready copy prepared by the author.

Copyright © 1980 by The Benjamin/Cummings Publishing Company, Inc.
Published simultaneously in Canada

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher, The Benjamin/Cummings Publishing Company, Inc., Advanced Book Program, Reading, Massachusetts 01867, U.S.A.

Manufactured in the United States of America

ABCDEFGHIJ-AL-89876543210

To my teacher, Yasuo Akizuki

Contents

Preface

This book has evolved out of a graduate course in algebra I gave at Brandeis University during the academic year of 1967–1968. At that time M. Auslander taught algebraic geometry to the same group of students, and so I taught commutative algebra for use in algebraic geometry. Teaching a course in geometry and a course in commutative algebra in parallel seems to be a good way to introduce students to algebraic geometry.

Part I is a self-contained exposition of basis concepts such as flatness, dimension, depth, normal rings, and regular local rings.

Part II deals with the finer structure theory of noetherian rings, which was initiated by Zariski (Sur la normalité analytique des variétés normales, Ann. Inst. Fourier 2 1950) and developed by Nagata and Grothendieck. Our purpose is to lead the reader as quickly as possible to Nagata's theory of pseudo-geometric rings (here called Nagata rings) and to Grothendieck's theory of excellent rings. The interested reader should advance to Nagata's book LOCAL RINGS and to Grothendieck's EGA, Ch. IV.

The theory of multiplicity was omitted because one has little to add on this subject to the lucid expositon of Serre's lecture notes (Algèbre locale. Multiplicité, Springer-Verlag).

Due to lack of space some important results on formal smoothness (especially its relation to flatness) had to be omitted also. For these, see EGA.

We assume that the reader is familiar with the elements of algebra (rings, modules, and Galois theory) and of homological algebra (Tor and Ext). Also, it is desirable but not indispensable to have some knowledge of scheme theory.

I thank my students at Brandeis, especially Robin Hur, for helpful comments.

Hideyuki Matsumura

Nagoya, Japan
November 1969

Preface to the Second Edition

Nine years have passed since the publication of this book, during which time it has been awarded the warm reception of students of algebra and algebraic geometry in the United States, in Europe, as well as in Japan.

In this revised and enlarged edition, I have limited alternations on the original text to the minimum. Only Ch. 6 has been completely rewritten, and the other chapters have been left relatively untouched, with the exception of pages 37, 38, 160, 176, 216, 252, 258, 259, 260.

On the other hand, I have added an Appendix consisting of several sections, which are almost independent of each other. Its purpose is twofold: one is to prove the theorems which were used but not proved in the text, namely Eakin's theorem, Cohen's existence theorem of coefficient rings for complete local rings of unequal characteristic, and Nagata's Jacobian criterion for formal power series rings. The other is to record some of the recent achievements in the area connected with PART II. They include Faltings' simple proof of formal smoothness of the geometrically regular local rings, Marot's theorem on Nagata rings, my theory on excellence of rings with enough derivations in characteristic 0, and Kunz' theorems on regularity and excellence of rings of characteristic p.

I should like to record my gratitude to my former students M. Mizutani and M. Nomura, who read this book carefully and proved Th.101 and Th.99.

Hideyuki Matsumura

Nagoya, Japan
December 1979

Conventions

1. All rings and algebras are tacitly assumed to be commutative with unit element.
2. If F: A → B is a homomorphism of rings and if I is an ideal of B, then the ideal $f^{-1}(I)$ is denoted by $I \cap A$.
3. $\subset$ means proper inclusion.
4. We sometimes use the old-fashioned notation $I = (a_1, \ldots, a_n)$ for an ideal I generated by the elements a_i.
5. By a finite A-module we mean a finitely generated A-module. By a finite A-algebra, we mean an algebra which is a finite A-module. By an A-algebra of finite type, we mean an algebra which is finitely generated as a ring over the canonical image of A.

PART ONE

CHAPTER 1. ELEMENTARY RESULTS

In this chapter we give some basic definitions, and some elementary results which are mostly well-known.

1. General Rings

(1.A) Let A be a ring and $\mathfrak{a}$ an ideal of A. Then the set of elements x in A some powers of which lie in $\mathfrak{a}$ is an ideal of A, called the radical of $\mathfrak{a}$.

An ideal p is called a prime ideal of A if A/p is an integral domain ; in other words, if $p \neq A$ and if $A - p$ is closed under multiplication. If p is prime, and if $\mathfrak{a}$ and $\mathfrak{b}$ are ideals not contained in p, then $\mathfrak{a}\mathfrak{b} \not\subseteq p$.

An ideal q is called primary if $q \neq A$ and if the only zero divisors of A/q are nilpotent elements, i.e. $xy \in q$, $x \notin q$ implies $y^n \in q$ for some n. If q is primary then its radical p is prime (but the converse is not true), and p and q are said to belong to each other. If $q (\neq A)$ is an ideal containing some power $\mathfrak{m}^n$ of a maximal ideal $\mathfrak{m}$, then q is a primary ideal belonging to $\mathfrak{m}$.

The set of the prime ideals of A is called the <u>spectrum</u> of A and is denoted by Spec(A) ; the set of the maximal ideals of A is called the <u>maximal spectrum</u> of A and we denote it by $\Omega(A)$. The set Spec(A) is topologized as follows. For any subset M of A, put $V(M) = \{ p \in \mathrm{Spec}(A) \mid M \subseteq p \}$, and take as the closed sets in Spec(A) all subsets of the form V(M). This topology is called the <u>Zariski topology</u>. If $f \in A$, we put $D(f) = \mathrm{Spec}(A) - V(f)$ and call it an <u>elementary open set</u> of Spec(A). The elementary open sets form a basis of open sets of the Zariski topology in Spec(A).

Let $f: A \to B$ be a ring homomorphism. To each $P \in \mathrm{Spec}(B)$ we associate the ideal $P \cap A$ (i.e. $f^{-1}(P)$) of A. Since $P \cap A$ is prime in A, we then get a map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$, which is denoted by ${}^a f$. The map ${}^a f$ is continuous as one can easily check. It does not necessarily map $\Omega(B)$ into $\Omega(A)$. When $P \in \mathrm{Spec}(B)$ and $p = P \cap A$, we say that P <u>lies over</u> p.

(1.B) Let A be a ring, and let $I, p_1, \ldots, p_r$ be ideals in A. Suppose that all but possibly two of the p_i's are prime ideals. Then, if $I \nsubseteq p_i$ for each i, the ideal I is not contained in the set-theoretical union $\bigcup_i p_i$.

<u>Proof</u>. Omitting those p_i which are contained in some other

p_j, we may suppose that there are no inclusion relations between the p_i's. We use induction on r. When r = 2, suppose $I \subseteq p_1 \cup p_2$. Take $x \in I - p_2$ and $s \in I - p_1$. Then $x \in p_1$, hence $s + x \notin p_1$, therefore both s and s + x must be in p_2. Then $x \in p_2$ and we get a contradiction.

When r > 2, assume that p_r is prime. Then $Ip_1 \ldots p_{r-1} \nsubseteq p_r$; take an element $x \in Ip_1 \ldots p_{r-1}$ which is not in p_r. Put $S = I - (p_1 \cup \ldots \cup p_{r-1})$. By induction hypothesis S is not empty. Suppose $I \subseteq p_1 \cup \ldots \cup p_r$. Then S is contained in p_r. But if $s \in S$ then $s + x \in S$ and therefore both s and s + x are in p_r, hence $x \in p_r$, contradiction.

<u>Remark</u>. When A contains an infinite field k, the condition that $p_3, \ldots, p_r$ be prime is superfluous, because the ideals are k-vector spaces and $I = \bigcup_i (I \cap p_i)$ cannot happen if $I \cap p_i$ are proper subspaces of I.

(1.C) Let A be a ring, and $I_1, \ldots, I_r$ be ideals of A such that $I_i + I_j = A$ $(i \neq j)$. Then $I_1 \cap \ldots \cap I_r = I_1 I_2 \ldots I_r$ and

$$A/(\cap I_i) \simeq (A/I_1) \times \ldots \times (A/I_r).$$

(1.D) Any ring $A \neq 0$ has at least one maximal ideal. In fact, the set $M = \{ \text{ideal } J \text{ of } A \mid 1 \notin J \}$ is not empty since

(0) ε M, and one can apply Zorn's lemma to find a maximal element of M. It follows that Spec(A) is empty iff A = 0.

If A $\neq$ 0, Spec(A) has also minimal elements (i.e. A has minimal prime ideals). In fact, any prime p ε Spec(A) contains at least one minimal prime. This is proved by reversing the inclusion-order of Spec(A) and applying Zorn's lemma.

If $J \neq A$ is an ideal, the map Spec(A/J) $\rightarrow$ Spec(A) obtained from the natural homomorphism A $\rightarrow$ A/J is an order-preserving bijection from Spec(A/J) onto $V(J) = \{ p \in \text{Spec}(A) \mid p \supseteq J \}$. Therefore V($J$) has maximal as well as minimal elements. We shall call a minimal element of V(J) a minimal prime over-ideal of J.

(1.E) A subset S of a ring A is called a <u>multiplicative subset</u> of A if 1 ε S and if the products of elements of S are again in S.

Let S be a multiplicative subset of A not containing 0, and let M be the set of the ideals of A which do not meet S. Since (0) ε M the set M is not empty, and it has a maximal element p by Zorn's lemma. Such an ideal p is prime ; in fact, if $x \notin p$ and $y \notin p$, then both $Ax + p$ and $Ay + p$ meet S, hence there exist elements a, b ε A and s, s' ε S such that $ax \equiv s$, $by \equiv s'$ (mod p). Then $abxy \equiv ss'$ (mod p), ss' ε S, therefore $ss' \notin p$ and hence $xy \notin p$, Q.E.D. A maximal element of M is called a <u>maximal ideal with respect to the multiplicative set S</u>.

We list a few corollaries of the above result.

i) If S is a multiplicative subset of a ring A and if $0 \notin S$, then there exists a prime p of A with $p \cap S = \emptyset$.

ii) The set of nilpotent elements in A,

$$\text{nil}(A) = \{a \in A \mid a^n = 0 \text{ for some } n > 0\},$$

is the intersection of all prime ideals of A (hence also the intersection of all minimal primes of A by (1.D)).

iii) Let A be a ring and J a proper ideal of A. Then the radical of J is the intersection of prime ideals of A containing J.

<u>Proof</u>. i) is already proved. ii): Clearly any prime ideal contains nil(A). Conversely, if $a \notin$ nil(A), then S = $\{1, a, a^2, \ldots\}$ is multiplicative and $0 \notin S$, therefore there exists a prime p with $a \notin p$. iii) is nothing but ii) applied to A/J.

We say a ring A is <u>reduced</u> if it has no nilpotent elements except 0, i.e. if nil(A) = (0). This is equivalent to saying that (0) is an intersection of prime ideals. For any ring A, we put A_{red} = A/nil(A). The ring A_{red} is of course reduced.

(1.F) Let S be a multiplicative subset of a ring A. Then the localization (or quotient ring or ring of fractions) of A with respect to S, denoted by $S^{-1}A$ or by A_S, is the ring

$$S^{-1}A = \{ \frac{a}{s} \mid a \in A, \quad s \in S \}$$

where equality is defined by

$$a/s = a'/s' \iff s''(s'a - sa') = 0 \quad \text{for some } s'' \in S$$

and the addition and the multiplication are defined by the usual formulas about fractions. We have $S^{-1}A = 0$ iff $0 \in S$. The natural map $\phi: A \to S^{-1}A$ given by $\phi(a) = a/1$ is a homomorphism, and its kernel is $\{ a \in A \mid \exists\, s \in S : sa = 0 \}$. The A-algebra $S^{-1}A$ has the following universal mapping property: if $f: A \to B$ is a ring homomorphism such that the images of the elements of S are invertible in B, then there exists a unique homomorphism $f_S: S^{-1}A \to B$ such that $f = f_S \circ \phi$, where $\phi: A \to S^{-1}A$ is the natural map. Of course one can use this property as a definition of $S^{-1}A$. It is the basis of all functorial properties of localization.

If p is a prime (resp. primary) ideal of A such that $p \cap S = \emptyset$, then $p(S^{-1}A)$ is prime (resp. primary). Conversely, all the prime and the primary ideals of $S^{-1}A$ are obtained in this way. For any ideal I of $S^{-1}A$ we have $I = (I \cap A)(S^{-1}A)$. If J is an ideal of A, then we have $J(S^{-1}A) = S^{-1}A$ iff $J \cap S \neq \emptyset$. The canonical map $\mathrm{Spec}(S^{-1}A) \to \mathrm{Spec}(A)$ is an order-

preserving bijection and homeomorphism from $\mathrm{Spec}(S^{-1}A)$ onto the subset $\{p \in \mathrm{Spec}(A) \mid p \cap S = \emptyset \}$ of $\mathrm{Spec}(A)$.

(1.G) Let S be a multiplicative subset of a ring A and let M be an A-module. One defines $S^{-1}M = \{x/s \mid x \in M, s \in S \}$ in the same way as $S^{-1}A$. The set $S^{-1}M$ is an $S^{-1}A$-module, and there is a natural isomorphism of $S^{-1}A$-modules

$$S^{-1}M \simeq S^{-1}A \otimes_A M$$

given by $x/s \mapsto (1/s) \otimes x$.

If M and N are A-modules, we have

$$S^{-1}(M \otimes_A N) = (S^{-1}M) \otimes_{S^{-1}A} (S^{-1}N).$$

When M is of finite presentation, i.e. when there is an exact sequence of the form $A^m \to A^n \to M \to 0$, we have also

$$S^{-1}(\mathrm{Hom}_A(M, N)) = \mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N).$$

(1.H) When $S = A - p$ with $p \in \mathrm{Spec}(A)$, we write A_p, M_p for $S^{-1}A$, $S^{-1}M$.

LEMMA 1. If an element x of M is mapped to 0 in M_p for all $p \in \Omega(A)$, then $x = 0$. In other words, the natural map

$$M \to \prod_{\text{all max.}\, p} M_p$$

is injective.

Proof. $x = 0$ in $M_p \Leftrightarrow s \in A - p$ such that $sx = 0$ in $M \Leftrightarrow$ $\mathrm{Ann}(x) = \{a \in A \mid ax = 0\} \not\subseteq p$. Therefore, if $x = 0$ in M_p for all maximal ideals p, the annihilator $\mathrm{Ann}(x)$ of x is not contained in any maximal ideal and hence $\mathrm{Ann}(x) = A$. This implies $x = 1.x = 0$. Q.E.D.

LEMMA 2. When A is an integral domain with quotient field K, all localizations of A can be viewed as subrings of K. In this sense, we have

$$A = \bigcap_{\text{all max.}p} A_p .$$

Proof. Given $x \in K$, we put $D = \{a \in A \mid ax \in A\}$; we might call D the ideal of denominators of x. The element x is in A iff $D = A$, and x is in A_p iff $D \not\subseteq p$. Therefore, if $x \notin A$, there exists a maximal ideal p such that $D \subseteq p$, and $x \notin A_p$ for this p.

(1.I) Let $f: A \to B$ be a homomorphism of rings and S a multiplicative subset of A; put $S' = f(S)$. Then the localization $S^{-1}B$ of B as an A-module coincides with $S'^{-1}B$:

(1.I.1) $$S'^{-1}B = S^{-1}B = (S^{-1}A) \otimes_A B .$$

In particular, if I is an ideal of A and if S' is the image of S in A/I, one obtains

(1.I.2) $$S'^{-1}(A/I) = S^{-1}A/I(S^{-1}A).$$

In this sense, dividing by I commutes with localization.

(1.J) Let A be a ring and S a multiplicative subset of A ; let $A \xrightarrow{f} B \xrightarrow{g} S^{-1}A$ be homomorphisms such that (1) $g \circ f$ is the natural map and (2) for any $b \in B$ there exists $s \in S$ with $f(s)b \in f(A)$. Then $S^{-1}B = f(S)^{-1}B = S^{-1}A$, as one can easily check. In particular, let A be a domain, $p \in \mathrm{Spec}(A)$ and B a subring of A_p such that $A \subseteq B \subseteq A_p$. Then $A_p = B_P = B_p$, where $P = pA_p \cap B$ and $B_p = B \otimes A_p$.

(1.K) A ring A which has only one maximal ideal $\mathfrak{m}$ is called a local ring, and $A/\mathfrak{m}$ is called the residue field of A. When we say that " $(A, \mathfrak{m})$ is a local ring " or " $(A, \mathfrak{m}, k)$ is a local ring ", we mean that A is a local ring, that $\mathfrak{m}$ is the unique maximal ideal of A and that k is the residue field of A. When A is an arbitrary ring and $p \in \mathrm{Spec}(A)$, the ring A_p is a local ring with maximal ideal pA_p. The residue field of A_p is denoted by $\kappa(p)$. Thus $\kappa(p) = A_p/pA_p$, which is the quotient ield of the integral demain A/p by (1.I.2).

If $(A, \mathfrak{m}, k)$ and $(B, \mathfrak{m}', k')$ are local rings, a homomorphism $\psi: A \to B$ is called a local homomorphism if $\psi(\mathfrak{m}) \subseteq \mathfrak{m}'$. In this case ψ induces a homomorphism $k \to k'$.

Let A and B be rings and $\psi: A \to B$ a homomorphism.

Consider the map ${}^a\psi : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$. If $P \in \mathrm{Spec}(B)$ and ${}^a\psi(P) = P \cap A = p$, we have $\psi(A - p) \subseteq B - P$, hence ψ induces a homomorphism $\psi_p : A_p \to B_P$, which is a local homomorphism since $\psi_p(pA_p) \subseteq \psi(p)B_P \subseteq PB_P$. Note that ψ_p can be factored as $A_p \to B_p = A_p \otimes_A B \to B_P$ and B_P is the localization of B_p by $PB_P \cap B_p$. In general B_p is not a local ring, and the maximal ideals of B_p which contain pB_p correspond to the pre-images of p in $\mathrm{Spec}(B)$. (B_p can have maximal ideals other than these.) But if B_p is a local ring, then $B_p = B_P$, because if $(R, \mathfrak{m})$ is a local ring then $R - \mathfrak{m}$ is the set of units of R and hence $R_{\mathfrak{m}} = R$.

(1.L) <u>Definition</u>. Let A be a ring, $A \neq 0$. The <u>Jacobson radical</u> of A, rad(A), is the intersection of all maximal ideals of A.

Thus, if $(A, \mathfrak{m})$ is a local ring then $\mathfrak{m} = \mathrm{rad}(A)$. We say that a ring $A \neq 0$ is a <u>semi-local ring</u> if it has only a finite number of maximal ideals, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$. (We express this situation by saying "$(A, \mathfrak{m}_1, \ldots, \mathfrak{m}_r)$ is a semi-local ring".) In this cass $\mathrm{rad}(A) = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_r = \Pi \mathfrak{m}_i$ by (1.C).

Any element of the form $1 + x$, $x \in \mathrm{rad}(A)$, is a unit in A, because $1 + x$ is not contained in any maximal ideal. Conversely, if I is an ideal and if $1 + x$ is a unit for each $x \in I$, we have $I \subseteq \mathrm{rad}(A)$.

(1.M) LEMMA (NAK)*. Let A be a ring, M a finite A-module and I an ideal of A. Suppose that $IM = M$. Then there exists an element $a \in A$ of the form $a = 1 + x$, $x \in I$, such that $aM = 0$. If moreover $I \subseteq \mathrm{rad}(A)$, then $M = 0$.

<u>Proof</u>. Let $M = Aw_1 + \ldots + Aw_s$. We use induction on s. Put $M' = M/Aw_s$. By induction hypothesis there exists $x \in I$ such that $(1 + x)M' = 0$, i.e., $(1 + x)M \subseteq Aw_s$ (when $s = 1$, take $x = 0$). Since $M = IM$, we have $(1 + x)M = I(1 + x)M \subseteq I(Aw_s) = Iw_s$, hence we can write $(1 + x)w_s = yw_s$ for some $y \in I$. Then $(1 + x - y)(1 + x)M = 0$, and $(1 + x - y)(1 + x) \equiv 1 \mod I$, proving the first assertion. The second assertion follows from this and from (1.L).

This Lemma is often used in the following form.

COROLLARY. Let A be a ring, M an A-module, N and N' submodules of M, and I an ideal of A. Suppose that $M = N + IN'$, and that either (a) I is nilpotent, or (b) $I \subseteq \mathrm{rad}(A)$ and N' is finitely generated. Then $M = N$.

<u>Proof</u>. In case (a) we have $M/N = I(M/N) = I^2(M/N) = \ldots = 0$. In case (b), apply NAK to M/N.

---

*) This simple but important lemma is due to T. Nakayama, G. Azumaya and W. Krull. Priority is obscure, and although it is usually called the Lemma of Nakayama, late Prof. Nakayama did not like the name.

(1.N) In particular, let $(A, \mathfrak{m}, k)$ be a local ring and M an A-module. Suppose that either $\mathfrak{m}$ is nilpotent or M is finite. Then a subset G of M generates M iff its image $\overline{G}$ in $M/\mathfrak{m}M = M\otimes k$ generates $M\otimes k$. In fact, if N is the submodule generated by G, and if $\overline{G}$ generates $M\otimes k$, then $M = N + \mathfrak{m}M$, whence $M = N$ by the corollary. Since $M\otimes k$ is a vector space over the field k, it has a basis, say $\overline{G}$, and if we lift $\overline{G}$ arbitrarily to a subset G of M (i.e. choose a pre-image for each element of $\overline{G}$), then G is a system of generators of M. Such a system of generators is called a <u>minimal basis</u> of M. Note that a minimal basis is not necessarily a basis of M (but it is so in an important case, cf. (3.G)).

(1.O) Let A be a ring and M an A-module. An element a of A is said <u>M-regular</u> if it is not a zero-divisor on M, i.e., if $M \xrightarrow{a} M$ is injective. The set of the M-regular elements is a multiplicative subset of A.

Let S_0 be the set of A-regular elements. Then $S_0^{-1}A$ is called the <u>total quotient ring</u> of A. In this book we shall denote it by ΦA. When A is an integral domain, ΦA is nothing but the quotient field of A.

(1.P) Let A be a ring and $\alpha\colon Z \to A$ be the canonical homomorphism from the ring of integers Z to A. Then $\mathrm{Ker}(\alpha) = nZ$

for some $n \geqslant 0$. We call n the <u>characteristic</u> of A and denote it by ch(A). If A is local the characteristic ch(A) is either 0 or a power of a prime number.

2. Noetherian Rings and Artinian Rings

(2.A) A ring is called <u>noetherian</u> (resp. <u>artinian</u>) if the ascending chain condition (resp. descending chain condition) for ideals holds in it. A ring A is noetherian iff every ideal of A is a finite A-module.

If A is a noetherian ring and M a finite A-moeule, then the ascending chain condition for submodules holds in M and every submodule of M is a finite A-module. From this, it follows easily that a finite module M over a noetherian ring has a projective resolution $\cdots \to X_i \to X_{i-1} \to \cdots \to X_0 \to M \to 0$ such that each X_i is a finite free A-module. In particular, M is of finite presentation.

A polynomial ring $A[X_1,\ldots, X_n]$ over a noetherian ring A is again noetherian. Similarly for a formal power series ring $A[[X_1,\ldots,X_n]]$. If B is an A-algebra of finite type and if A is noetherian, then B is noetherian since it is a homomorphic image of $A[X_1,\ldots,X_n]$ for some n.

(2.B) Any proper ideal I of a noetherian ring has a primary decomposition, i.e. $I = q_1 \cap \ldots \cap q_r$ with primary ideals q_i. (We shall discuss this topic again in Chap. 5)

(2.C) PROPOSITION. A ring A is artinian iff the length of A as A-module is finite.

Proof. If $\mathrm{length}_A(A) < \infty$ then A is certainly artinian (and noetherian). Conversely, suppose A is artinian. Then A has only a finite number of maximal ideals. Indeed, if there were an infinite sequence of maximal ideals $p_1, p_2, \ldots$ then $p_1 \supset p_1p_2 \supset p_1p_2p_3 \supset \ldots$ would be a strictly descending infinite chain of ideals, contradicting the hypothesis. Let $p_1, \ldots, p_r$ be all the maximal ideals of A (we may assume $A \neq 0$, so $r > 0$), and put $I = p_1 \ldots p_r$. The descending chain $I \supseteq I^2 \supseteq I^3 \supseteq \ldots$ stops, so there exists $s > 0$ such that $I^s = I^{s+1}$. Put $((0):I^s) = J$. Then $(J:I) = (((0):I^s):I) = ((0):I^{s+1}) = J$. We claim $J = A$. Suppose the contrary, and let J' be a minimal member of the set of ideals strictly containing J. Then $J' = Ax + J$ for any $x \in J' - J$. Since $I = \mathrm{rad}(A)$, the ideal $Ix + J$ is not equal to J' by NAK (Cor. of (1.K)). So we must have $Ix + J = J$ by the minimality of J', hence $Ix \subseteq J$ and $x \in (J:I) = J$, contradiction. Thus $J = A$, i.e. $1 \cdot I^s \subseteq (0)$, i.e. $I^s = (0)$.

Consider the descending chain

$$A \supseteq p_1 \supseteq p_1p_2 \supseteq \cdots \supseteq p_1 \ldots p_{r-1} \supseteq I \supseteq Ip_1 \supseteq Ip_1p_2 \supseteq \ldots \supseteq I^2 \supseteq I^2p_1 \supseteq \ldots \supseteq I^s = (0).$$

Each factor module of this chain is a vector space over the field $A/p_i = k_i$ for some i, and its subspaces correspond bijectively to the intermediate ideals. Thus, the descending chain condition in A implies that this factor module is of finite dimension over k_i, therefore it is of finite length as A-module. Since $\mathrm{length}_A(A)$ is the sum of the length of the factor modules of the chain above, we see that $\mathrm{length}_A(A)$ is finite. Q.E.D.

A ring $A \neq 0$ is said to have dimension zero if all prime ideals are maximal (cf. 12.A).

COROLLARY. A ring $A \neq 0$ is artinian iff it is noetherian and of dimension zero.

Proof. If A is artinian, then it is noetherian since $\mathrm{length}_A(A) < \infty$.

Let p be any prime ideal of A. In the notation of the above proof, we have $(p_1 \ldots p_r)^s = I^s = (0) \subseteq p$, hence $p = p_i$ for some i. Thus A is of dimension zero.

To prove the converse, let $(0) = q_1 \cap \ldots \cap q_r$ be a primary decomposition of the zero ideal in A, and let p_i = the radical of q_i. Since p_i is finitely generated over A, there is a positive integer n such that $p_i^n \subseteq q_i$ $(1 \leq i \leq r)$. Then $(p_1 \ldots p_r)^n = (0)$. After this point we can immitate the last part of thepproof of the proposition to conclude that $\mathrm{length}_A(A) < \infty$.

(2.D) I.S.Cohen proved that a ring is noetherian iff every prime ideal is finitely generated (cf. Nagata, LOCAL RINGS, p.8). Recently P.M.Eakin (Math. Annalen 177(1968),278-282) proved that, if A is a ring and A' is a subring over which A is finite, then A' is noetherian if (and of course only if) A is so. (The theorem was independently obtained by Nagata, but the priority is Eakin's.)

Exercises to Chapter 1.

1) Let I and J be ideals of a ring A. What is the condition for V(I) and V(J) to be disjoint ?

2) Let A be a ring and M an A-module. Define the support of M, Supp(M), by

$$\mathrm{Supp}(M) = \{p \in \mathrm{Spec}(A) \mid M_p \neq 0\}.$$

If M is finite over A, we have Supp(M) = V(Ann(M)) so that the support is closed in Spec(A).

3) Let A be a noetherian ring and M a finite A-module. Let I be an ideal of A such that $\mathrm{Supp}(M) \subseteq V(I)$. Then $I^n M = 0$ for some $n > 0$.

CHAPTER 2. FLATNESS

3. Flatness

(3.A) DEFINITION. Let A be a ring and M an A-module ; when $S: \cdots \to N \to N' \to N'' \to \cdots$ is any sequence of A-modules (and of A-linear maps), let $S \otimes M$ denote the sequence $\cdots \to N \otimes M \to N' \otimes M \to N'' \otimes M \to \cdots$ obtained by tensoring S with M. We say that M is <u>flat over A</u>, or <u>A-flat</u>, if $S \otimes M$ is exact whenever S is exact. We say that M is <u>faithfully flat</u> (f.f.) over A, if $S \otimes M$ is exact iff S is exact.

Examples. Projective modules are flat. Free modules are f.f.. If B and C are rings and A = B × C, then B is a projective module (hence flat) over A but not f.f. over A.

THEOREM 1. The following conditions are equivalent:

(1) M is A-flat ;

(2) if $0 \to N' \to N$ is an exact sequence of A-modules, then $0 \to N' \otimes M \to N \otimes M$ is exact ;

(3) for any finitely generated ideal I of A, the sequence $0 \to I \otimes M \to M$ is exact, in other words we have $I \otimes M \simeq IM$;

(4) $\mathrm{Tor}_1^A(M, A/I) = 0$ for any finitely generated ideal I of A ;

(5) $\mathrm{Tor}_1^A(M, N) = 0$ for any finite A-module N ;

(6) if $a_i \in A$, $x_i \in M$ $(1 \leqslant i \leqslant r)$ and $\Sigma_1^r a_i x_i = 0$, then there exist an integer s and elements $b_{ij} \in A$ and $y_j \in M$ $(1 \leqslant j \leqslant s)$ such that $\sum_i a_i b_{ij} = 0$ for all j and $x_i = \sum_j b_{ij} y_j$ for all i.

Proof. The equivalence of the conditions (1) through (5) is well known ; one uses the fact that the inductive limit (= direct limit) in the category of A-modules preserves exactness and commutes with Tor_i. We omit the detail. As for (6), first suppose that M is flat and $\Sigma_1^r a_i x_i = 0$. Consider the exact sequence

$$K \xrightarrow{g} A^r \xrightarrow{f} A$$

where f is defined by $f(b_1, \ldots, b_r) = \Sigma a_i b_i$ $(b_i \in A)$, $K = \mathrm{Ker}(f)$ and g is the inclusion map. Then $K \otimes M \to M^r \xrightarrow{f_M} M$ is exact, where $f_M(t_1, \ldots, t_r) = \Sigma a_i t_i$ $(t_i \in M)$; therefore $(x_1, \ldots, x_r) = \Sigma_1^s \beta_j \otimes y_j$ with $\beta_j \in K$, $y_j \in M$.

Writing $\beta_j = (b_{1j}, \ldots, b_{rj})$ $(b_{ij} \in A)$, we get the wanted result. Next let us prove (6) $\Rightarrow$ (3). Let $a_1, \ldots, a_r \in I$ and $x_1, \ldots, x_r \in M$ be such that $\Sigma a_i x_i = 0$. Then by assumption $x_i = \Sigma b_{ij} y_j$, $\Sigma a_i b_{ij} = 0$, hence in $I \otimes M$ we have $\Sigma_i a_i \otimes x_i$ $= \Sigma_i a_i \otimes \Sigma_j b_{ij} y_j = \Sigma_j (\Sigma_i a_i b_{ij} \otimes y_j) = 0$. Q.E.D.

(3.B) (Transitivity) Let $\phi : A \to B$ be a homomorphism of rings and suppose that ϕ makes B a flat A-module. (In this case we shall say that ϕ is a flat homomorphism.) Then a flat B-module N is also flat over A.

Proof. Let S be a sequence of A-modules. Then $S \otimes_A N = S \otimes_A (B \otimes_B N) = (S \otimes_A B) \otimes_B N$. Thus, S is exact $\Rightarrow$ $S \otimes_A B$ is exact $\Rightarrow$ $S \otimes_A N$ is exact.

(3.C) (Change of base) Let $\phi : A \to B$ be any homomorphism of rings and let M be a flat A-module. Then $M_{(B)} = M \otimes_A B$ is a flat B-module.

Proof. Let S be a sequence of B-modules. Then $S \otimes_B (B \otimes_A M) = S \otimes_A M$, which is exact if S is exact.

(3.D) (Localization) Let A be a ring, and S a multiplicative subset of A. Then $S^{-1}A$ is flat over A.

Proof. Let M be an A-module and N a submodule. We have $M\otimes S^{-1}A = S^{-1}M$ and $N\otimes S^{-1}A = S^{-1}N$. A typical element of $S^{-1}N$ is of the form x/s, $x \in N$, $s \in S$; if $x/s = 0$ in $S^{-1}M$, this means that there exists $s' \in S$ with $s'x = 0$ in M, which is equivalent to saying that $s'x = 0$ in N, hence $x/s = 0$ in $S^{-1}N$. Thus $0 \to S^{-1}N \to S^{-1}M$ is exact. Q.E.D.

(3.E) Let $\phi : A \to B$ be a flat homomorphism of rings, and let M and N be A-modules. Then $\mathrm{Tor}_i^A(M, N)\otimes_A B = \mathrm{Tor}_i^B(M_{(B)}, N_{(B)})$. If A is noetherian and M is finite over A, we also have $\mathrm{Ext}_A^i(M, N)\otimes_A B = \mathrm{Ext}_B^i(M_{(B)}, N_{(B)})$.

Proof. Let $\cdots \to X_1 \to X_0 \to M \to 0$ be a projective resolution of the A-module M. Then, since B is flat, the sequence

$$(*) \qquad \cdots \to X_{1(B)} \to X_{0(B)} \to M_{(B)} \to 0$$

is a projective resolution of $M_{(B)}$. We have therefore

$$\mathrm{Tor}_i^A(M, N) = H_i(X.\otimes N),$$

$$\mathrm{Tor}_i^B(M_{(B)}, N_{(B)}) = H_i(X.\otimes_A N\otimes_A B),$$

But the exact functor $\otimes_A B$ commutes with taking homology, so that $H_i(X.\otimes_A N\otimes_A B) = H_i(X.\otimes_A N)\otimes_A B = \mathrm{Tor}_i^A(M, N)\otimes_A B$. If A is noetherian and M is finite over A, we can assume that the X_i's are finite free A-modules. Then $\mathrm{Hom}_B(X_i\otimes B, N\otimes B) = \mathrm{Hom}_A(X_i, N)\otimes_A B$, and so the same reasoning as above proves

the formula for Ext. Q.E.D.

In particular, for $\mathfrak{p} \in \mathrm{Spec}(A)$, we have

$$\mathrm{Tor}_i^{A_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) = \mathrm{Tor}_i^A(M, N)_\mathfrak{p},$$

$$\mathrm{Ext}_{A_\mathfrak{p}}^i(M_\mathfrak{p}, N_\mathfrak{p}) = \mathrm{Ext}_A^i(M, N)_\mathfrak{p},$$

the latter being valid for A noetherian and M finite.

(3.F) Let A be a ring and M a flat A-module. Then an A-regular element $a \in A$ is also M-regular.

Proof. As $0 \to A \xrightarrow{a} A$ is exact, so is $0 \to M \xrightarrow{a} M$.

(3.G) PROPOSITION. Let $(A, \mathfrak{m}, k)$ be a local ring and M an A-module. Suppose that either $\mathfrak{m}$ is nilpotent or M is finite over A. Then

M is free $\Leftrightarrow$ M is projective $\Leftrightarrow$ M is flat.

Proof. We have only to prove that if M is flat then it is free. We prove that any minimal basis of M (cf.(1.N)) is a basis of M. For that purpose it suffices to prove that, if $x_1, \ldots, x_n \in M$ are such that their images $\bar{x}_1, \ldots, \bar{x}_n$ in $M/\mathfrak{m}M = M\otimes_A k$ are linearly independent over k, then they are linearly independent over A. We use induction on n. When $n = 1$, let $ax = 0$. Then there exist $y_1, \ldots, y_r \in M$ and

$b_1, \ldots, b_r \in A$ such that $ab_i = 0$ for all i and such that $x = \Sigma b_i y_i$. Since $\bar{x} \neq 0$ in $M/\mathfrak{m}M$, not all b_i are in $\mathfrak{m}$. Suppose $b_1 \notin \mathfrak{m}$. Then b_1 is a unit in A and $ab_1 = 0$, hence $a = 0$.

Suppose $n > 1$ and $\Sigma_1^n a_i x_i = 0$. Then there exist $y_1, \ldots, y_r \in M$ and $b_{ij} \in A$ $(1 \leq j \leq r)$ such that $x_i = \sum_j b_{ij} y_j$ and $\sum_i a_i b_{ij} = 0$. Since $x_n \notin \mathfrak{m}M$ we have $b_{nj} \notin \mathfrak{m}$ for at least one j. Since $a_1 b_{1j} + \cdots + a_n b_{nj} = 0$ and b_{nj} is a unit, we have

$$a_n = \Sigma_1^{n-1} c_i a_i \quad (c_i = -b_{ij}/b_{nj}).$$

Then

$$0 = \Sigma_1^n a_i x_i = a_1(x_1 + c_1 x_n) + \cdots + a_{n-1}(x_{n-1} + c_{n-1} x_n).$$

Since the elements $\bar{x}_1 + \bar{c}_1 \bar{x}_n, \ldots, \bar{x}_{n-1} + \bar{c}_{n-1} \bar{x}_n$ are linearly independent over k, by the induction hypothesis we get $a_1 = \cdots = a_{n-1} = 0$, and $a_n = \Sigma_1^{n-1} c_i a_i = 0$. Q.E.D.

REMARK. If M is flat but not finite, it is not necessarily free (e.g. $A = Z_{(p)}$ and $M = Q$). On the other hand, any projective module over a local ring is free (I. Kaplansky: Projective Modules, Ann. of Math. 68(1958), 372-377). For more general rings, it is known that non-finitely generated projective modules are, under very mild hypotheses, free. (Cf. H. Bass: Big Projective Modules Are Free, Ill. J. Math. 7 (1963) 24-31, and Y. Hinohara: Projective Modules over Weakly Noetherian Rings, J. Math. Soc. Japan, 15 (1963), 75-88 and 474-475).

(3.H) Let $A \to B$ be a flat homomorphism of rings, and let I_1 and I_2 be ideals of A. Then

(1) $(I_1 \cap I_2)B = I_1 B \cap I_2 B$,

(2) $(I_1 : I_2)B = I_1 B : I_2 B$ if I_2 is finitely generated.

Proof. (1) Consider the exact sequence of A-modules

$$I_1 \cap I_2 \to A \to A/I_1 \oplus A/I_2.$$

Tensoring it with B, we get an exact sequence

$$(I_1 \cap I_2) \otimes_A B = (I_1 \cap I_2)B \to B \to B/I_1 B \oplus B/I_2 B.$$

This means $(I_1 \cap I_2)B = I_1 B \cap I_2 B$.

(2) When I_2 is a principal ideal aA, we use the exact sequence

$$(I_1 : aA) \overset{i}{\to} A \overset{f}{\to} A/I_1$$

where i is the injection and $f(x) = ax \bmod I_1$. Tensoring it with B we get the formula $(I_1 : aA)B = (I_1 B : aB)$. In the general case, if $I_2 = a A + \cdots + a_n A$, we have $(I_1 : I_2) = \bigcap_i (I_1 : a_i)$ so that by (1)

$$(I_1 : I_2)B = \bigcap (I_1 : a_i A)B = \bigcap (I_1 B : a_i B) = (I_1 B : I_2 B).$$

(3.I) EXAMPLE 1. Let $A = k[x, y]$ be a polynomial ring over a field k, and put $B = A/xA \simeq k[y]$. Then B is not flat over A by (3.F). Let $I_1 = (x + y)A$ and $I_2 = yA$. Then $I_1 \cap I_2 = (xy + y^2)A$, $I_1 B = I_2 B = yB$, $(I_1 \cap I_2)B = y^2 B \neq I_1 B \cap I_2 B$.

EXAMPLE 2. Let k, x, y be as above and put $z = y/x$, $A = k[x,y]$, $B = k[x, y, z] = k[x, z]$. Let $I_1 = xA$, $I_2 = yA$. Then $I_1 \cap I_2 = xyA$, $(I_1 \cap I_2)B = x^2zB$, $I_1B \cap I_2B = xzB$. Thus B is not flat over A. The map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ corresponds to the projection to (x, y)-plane of the surface $F: xz = y$ in the (x, y, z)-space. Note F contains the whole z-axis and hence does not look 'flat' over the (x, y)-plane.

EXAMPLE 3. Let $A = k[x, y]$ be as above and $B = k[x, y, z]$ with $z^2 = f(x, y) \in A$. Then $B = A \oplus Az$ as an A-module, so that B is free, hence flat, over A. Geometrically, the surface $z^2 = f(x, y)$ appears indeed to lie rather flatly over the (x, y)-plane. A word of caution: such intuitive pictures are not enough to guarantee flatness.

(3.J) Let $A \to B$ be a homomorphism of rings. Then the following conditions are equivalent:

(1) B is flat over A ;

(2) B_P is flat over A_p ($p = P \cap A$) for all $P \in \mathrm{Spec}(B)$;

(3) B_P is flat over A_p ($p = P \cap A$) for all $P \in \Omega(B)$.

Proof. (1) $\Rightarrow$ (2): the ring $B_p = B \otimes A_p$ is flat over A_p (base change), and B_P is a localization of B_p, so that B_P is flat over A_p by transitivity. (2) $\Rightarrow$ (3): trivial. (3) $\Rightarrow$ (1): it suffices to show that $\mathrm{Tor}_1^A(B, N) = 0$ for any A-module N.

We use the following

LEMMA. Let B be an A-algebra, P a prime ideal of B, $p = P \cap A$ and N an A-module. Then

$$(\mathrm{Tor}_i^A(B, N))_P = \mathrm{Tor}_i^{A_p}(B_P, N_p).$$

Proof. Let $X. : \cdots \to X_1 \to X_0$ ($\to N \to 0$) be a free resolution of the A-module N. We have

$$\mathrm{Tor}_i^A(B, N) = H_i(X. \otimes_A B),$$

$$\mathrm{Tor}_i^A(B, N) \otimes_B B_P = H_i(X. \otimes_A B \otimes_B B_P)$$

$$= H_i(X. \otimes_A B_P) = H_i(X. \otimes_A A_p \otimes_{A_p} B_P),$$

and $X. \otimes A_p$ is a free resolution of the A_p-module N_p, hence the last expression is equal to $\mathrm{Tor}_i^{A_p}(B_P, N_p)$. Thus the lemma is proved.

Now, if B_P is flat over A_p for all $P \in \Omega(B)$, then $(\mathrm{Tor}_1^A(B, N))_P = 0$ for all $P \in \Omega(B)$ by the lemma, therefore $\mathrm{Tor}_1^A(B, N) = 0$ by (1.H) as wanted.

4. Faithful Flatness

(4.A) THEOREM 2. Let A be a ring and M an A-module. The following conditions are equivalent:

(i) M is faithfully flat over A;

(ii) M is flat over A, and for any A-module $N \neq 0$ we have $N \otimes M \neq 0$;

(iii) M is flat over A, and for any maximal ideal $\mathfrak{m}$ of A we have $\mathfrak{m}M \neq M$.

Proof. (i) $\Rightarrow$ (ii): suppose $N \otimes M = 0$. Let us consider the sequence $0 \to N \to 0$. As $0 \to N \otimes M \to 0$ is exact, so is $0 \to N \to 0$. Therefore $N = 0$.

(ii) $\Rightarrow$ (iii): since $A/\mathfrak{m} \neq 0$, we have $(A/\mathfrak{m}) \otimes M = M/\mathfrak{m}M \neq 0$ by hypothesis.

(iii) $\Rightarrow$ (ii): take an element $x \in N$, $x \neq 0$. The submodule Ax is a homomorphic image of A as A-module, hence $Ax \simeq A/I$ for some ideal $I \neq A$. Let $\mathfrak{m}$ be a maximal ideal of A containing I. Then $M \supset \mathfrak{m}M \supseteq IM$, therefore $(A/I) \otimes M = M/IM \neq 0$. By flatness $0 \to (A/I) \otimes M \to N \otimes M$ is exact, hence $N \otimes M \neq 0$.

(ii) $\Rightarrow$ (i): let S: $N' \to N \to N''$ be a sequence of A-modules, and suppose that

$$S \otimes M : N' \otimes M \xrightarrow{f_M} N \otimes M \xrightarrow{g_M} N'' \otimes M$$

is exact. As M is flat, the exact functor $\otimes M$ transforms kernel into kernel and image into image. Thus $\operatorname{Im}(g \circ f) \otimes M = \operatorname{Im}(g_M \circ f_M) = 0$, and by the assumption we get $\operatorname{Im}(g \circ f) = 0$, i.e. $g \circ f = 0$. Hence S is a complex, and if $H(S)$ denotes its homology (at N), we have $H(S) \otimes M = H(S \otimes M) = 0$. Using again the assumption (ii) we obtain $H(S) = 0$, which implies that S is exact.

Q.E.D.

COROLLARY. Let A and B be local rings, and $\psi : A \to B$ a local homomorphism. Let M ($\neq 0$) be a finite B-module. Then

M is flat over A $\Leftrightarrow$ M is f.f. over A.

In particular, B is flat over A iff it is f.f. over A.

Proof. Let $\mathfrak{m}$ and $\mathfrak{n}$ be the maximal ideals of A and B respectively. Then $\mathfrak{m}M \subseteq \mathfrak{n}M$ since ψ is local, and $\mathfrak{n}M \neq M$ by NAK, hence the assertion follows from the theorem.

(4.B) Just as flatness, faithful flatness is transitive (B is f.f. A-algebra and M is f.f. B-module $\Rightarrow$ M is f.f. over A) and is preserved by change of base (M is f.f. A-module and B is any A-algebra $\Rightarrow$ $M \otimes_A B$ is f.f. B-module).

Faithful flatness has, moreover, the following descent property: if B is an A-algebra and if M is a f.f. B-module which is also f.f. over A, then B is f.f. over A.

Proofs are easy and left to the reader.

(4.C) Faithful flatness is particularly important in the case of a ring extension. Let $\psi: A \to B$ be a f.f. homomorphism of rings. Then:

(i) For any A-module N, the map $N \to N\otimes B$ defined by $x \mapsto x\otimes 1$ is injective. In particular ψ is injective and A can be viewed as a subring of B.

(ii) For any ideal I of A, we have $IB\cap A = I$.

(iii) ${}^a\psi$: Spec(B) $\to$ Spec(A) is surjective.

Proof. (i) Let $0 \neq x \in N$. Then $0 \neq Ax \subseteq N$, hence $Ax\otimes B \subseteq N\otimes B$ by flatness of B. Then $Ax\otimes B = (x\otimes 1)B$, therefore $x\otimes 1 \neq 0$ by Th.2.

(ii) By change of base, $B\otimes_A(A/I) = B/IB$ is f.f. over A/I. Now the assertion follows from (i).

(iii) Let $p \in$ Spec(A). The ring $B_p = B\otimes A_p$ is f.f. over A_p, hence $pB_p \neq B_p$. Take a maximal ideal $\mathfrak{m}$ of B_p which contains pB_p. Then $\mathfrak{m}\cap A_p \supseteq pA_p$, therefore $\mathfrak{m}\cap A_p = pA_p$ because pA_p is maximal. Putting $P = \mathfrak{m}\cap B$, we get $P\cap A = (\mathfrak{m}\cap B)\cap A = \mathfrak{m}\cap A = (\mathfrak{m}\cap A_p)\cap A = pA_p\cap A = p$. Q.E.D.

(4.D) THEOREM 3. Let ψ: A $\to$ B be a homomorphism of rings. The following conditions are equivalent.

(1) ψ is faithfully flat;

(2) ψ is flat, and ${}^a\psi$: Spec(B) $\to$ Spec(A) is surjective;

(3) ψ is flat, and for any maximal ideal $\mathfrak{m}$ of A there exists a maximal ideal $\mathfrak{m}'$ of B lying over $\mathfrak{m}$.

Proof. (1) $\Rightarrow$ (2) is already proved.

(2) $\Rightarrow$ (3). By assumption there exists $p' \in$ Spec(B) with $p'\cap A = \mathfrak{m}$. If $\mathfrak{m}'$ is any maximal ideal of B containing p', we have $\mathfrak{m}'\cap A = \mathfrak{m}$ as $\mathfrak{m}$ is maximal.

(3) $\Rightarrow$ (1). The existence of $\mathfrak{m}'$ implies $\mathfrak{m}B \neq B$. Therefore B is f.f. over A by Th. 2.

Remark. In algebraic geometry one says that a morphism f: X $\to$ Y of preschemes is faithfully flat if f is flat (i.e. for all $x \in X$ the associated homomorphisms $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ are flat) and surjective.

(4.E) Let A be a ring and B a faithfully flat A-algebra. Let M be an A-module. Then:

(i) M is flat (resp. f.f.) over A $\Leftrightarrow$ $M\otimes_A B$ is so over B,

(ii) when A is local and M is finite over A we have

M is A-free $\Leftrightarrow$ $M\otimes_A B$ is B-free.

Proof. (i). The implication ($\Rightarrow$) is nothing but a change of base ((3.C) and (4.B)), while ($\Leftarrow$) follows from the fact that, for any sequence S of A-modules, we have $(S\otimes_A M)\otimes_A B = (S\otimes_A B)\otimes_B (M\otimes_A B)$. (ii). ($\Rightarrow$) is trivial. ($\Leftarrow$) follows from (i) because, under the hypothesis, freeness of M is equivalent to flatness as we saw in (3.G).

(4.F) REMARK. Let V be an algebraic variety over $\mathbb{C}$ and let $x \in V$ (or more generally, let V be an algebraic scheme over $\mathbb{C}$ and let x be a closed point on V). Let V^h denote the complex space obtained from V (for the precise definition see Serre's paper cited below), and let $\mathcal{O}$ and $\mathcal{O}^h$ be the local rings of x on V and on V^h respectively. Locally, one can assume that V is an algebraic subvariety of the affine n-space A_n. Then V is defined by an ideal I of $R = \mathbb{C}[X_1, \ldots, X_n]$, and taking the coordinate system in such a way that x is the origin we have $I \subseteq \mathfrak{m} = (X_1, \ldots, X_n)$ and $\mathcal{O} = R_{\mathfrak{m}}/IR_{\mathfrak{m}}$. Furthermore, denoting the ring of convergent power series in $X_1, \ldots, X_n$ by $S = \mathbb{C}\{\{X_1, \ldots, X_n\}\}$, we have $\mathcal{O}^h = S/IS$ by definition. Let F denote the formal power series ring: $F = \mathbb{C}[[X_1, \ldots, X_n]]$. It has been known long since that $\mathcal{O}$ and $\mathcal{O}^h$ are noetherian local rings. J.-P. Serre observed that the completion $(\mathcal{O}^h)\hat{}$ (cf. Chap. 3) of $\mathcal{O}^h$ is the same as the completion $\hat{\mathcal{O}} = F/IF$ of $\mathcal{O}$, and that $\hat{\mathcal{O}}$ is faithfully flat over $\mathcal{O}$ as well as over $\mathcal{O}^h$. It follows by descent that $\mathcal{O}^h$ is faithfully flat over $\mathcal{O}$, and this fact was made the basis of Serre's famous paper GAGA (Géométrie algébrique et géométrie analytique, Ann. Inst. Fourier, Vol.6, 1955/56). It was in the appendix to this paper that the notions of flatness and faithful flatness were defined and studied for the first time.

Exercise. Let A be an integral domain and B an integral domain containing A and having the same quotient field as A. Prove that B is f.f. over A only when $B = A$. (Geometrically, this means that if a birational morphism $f: X \to Y$ is flat at a point $x \in X$, then it is biregular at x.)

5. Going-up and Going-down

(5.A) Let $\phi: A \to B$ be a homomorphism of rings. We say that the going-up theorem holds for ϕ if the following condition is satisfied:

(GU) for any $\mathfrak{p}, \mathfrak{p}' \in \operatorname{Spec}(A)$ such that $\mathfrak{p} \subset \mathfrak{p}'$, and for any $P \in \operatorname{Spec}(B)$ lying over $\mathfrak{p}$, there exists $P' \in \operatorname{Spec}(B)$ lying over $\mathfrak{p}'$ such that $P \subset P'$.

Similarly, we say that the going-down theorem holds for ϕ if the following condition is satisfied:

(GD) for any $\mathfrak{p}, \mathfrak{p}' \in \operatorname{Spec}(A)$ such that $\mathfrak{p} \subset \mathfrak{p}'$, and for any $P' \in \operatorname{Spec}(B)$ lying over $\mathfrak{p}'$, there exists $P \in \operatorname{Spec}(B)$ lying over $\mathfrak{p}$ such that $P \subset P'$.

(5.B) The condition (GD) is equivalent to:

(GD') for any $\mathfrak{p} \in \operatorname{Spec}(A)$, and for any minimal prime over-ideal P of $\mathfrak{p}B$, we have $P \cap A = \mathfrak{p}$.

Proof. (GD) $\Rightarrow$ (GD'): let p and P be as in (GD'). Then $P \cap A \supseteq p$ since $P \supseteq pB$. If $P \cap A \neq p$, by (GD) there exists $P_1 \in \mathrm{Spec}(B)$ such that $P_1 \cap A = p$ and $P \supset P_1$. Then $P \supset P_1 \supseteq pB$, contradicting the minimality of P.

(GD') $\Rightarrow$ (GD): left to the reader.

Remark. Put $X = \mathrm{Spec}(A)$, $Y = \mathrm{Spec}(B)$, $f = {}^a\phi: Y \to X$, and suppose B is noetherian. Then (GD') can be formulated geometrically as follows: let $p \in X$, put $X' = V(p) \subseteq X$ and let Y' be an arbitrary irreducible component of $f^{-1}(X')$. Then f maps Y' generically onto X' in the sense that the generic point of Y' is mapped to the generic point p of X'. *)

(5.C) EXAMPLE. Let k[x] be a polynomial ring over a field k, and put $x_1 = x(x - 1)$, $x_2 = x^2(x - 1)$. Then $k(x) = k(x_1, x_2)$, and the inclusion $k[x_1, x_2] \subseteq k[x]$ induces a birational morphism

$$f: C = \mathrm{Spec}(\ k[x]\ ) \to C' = \mathrm{Spec}(\ k[x_1, x_2]\ )$$

where C is the affine line and C' is the affine curve $x_1^3 - x_2^2 + x_1x_2 = 0$. The morphism f maps the points Q_1: $x = 0$ and Q_2: $x = 1$ of C to the same point $P = (0,0)$ of C', which is an ordinary double point of C', and f maps

*) See (6.A) and (6.D) for the definitions of irreducible component and of generic point.

$C - \{Q_1, Q_2\}$ bijectively onto $C - \{P\}$.

Let y be another indeterminate, and put $B = k[x, y]$, $A = k[x_1, x_2, y]$. Then $Y = \mathrm{Spec}(B)$ is a plane and $X = \mathrm{Spec}(A)$ is $C' \times$ line; X is obtained by identifying the lines L_1: $x = 0$ and L_2: $x = 1$ on Y. Let $L_3 \subset Y$ be the line defined by $y = ax$, $a \neq 0$. Let $g: Y \to X$ be the natural morphism. Then $g(L_3) = X'$ is an irreducible curve on X, and

$$g^{-1}(X') = L_3 \cup \{(0, a), (1, 0)\}.$$

Therefore the going-down theorem does not hold for $A \subset B$.

(5.D) THEOREM 4. Let $\phi: A \to B$ be a flat homomorphism of rings. Then the going-down theorem holds for ϕ.

Proof. Let p and p' be prime ideals in A with $p' \subset p$, and let P be a prime ideal of B lying over p. Then B_P is flat over A_p by (3.J), hence faithfully flat since $A_p \to B_P$ is local. Therefore $\mathrm{Spec}(B_P) \to \mathrm{Spec}(A_p)$ is surjective. Let P'^* be a prime ideal of B_P lying over $p'A_p$. Then $P' = P'^* \cap B$ is a prime ideal of B lying over p' and contained in P. Q.E.D.

(5.E) THEOREM 5. *) Let B be a ring and A a subring over which B is integral. Then:

i) The canonical map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.

*) This theorem is due to Krull, but is often called the Cohen-Seidenberg theorem.

ii) There is no inclusion relation between the prime ideals of B lying over a fixed prime ideal of A.

iii) The going-up theorem holds for $A \subset B$.

iv) If A is a local ring and p is its maximal ideal, then the prime ideals of B lying over p are precisely the maximal ideals of B.

Suppose furthermore that A and B are integral domains and that A is integrally closed (in its quotient field ΦA). Then we also have the following.

v) The going-down theorem holds for $A \subset B$.

vi) If B is the integral closure of A in a normal extension field L of $K = \Phi A$, then any two prime ideals of B lying over the same prime $p \in \mathrm{Spec}(A)$ are conjugate to each other by some automorphism of L over K.

Proof. iv) First let M be a maximal ideal of B and put $\mathfrak{m} = M \cap A$. Then $\bar{B} = B/M$ is a field which is integral over the subring $\bar{A} = A/\mathfrak{m}$. Let $0 \neq x \in \bar{A}$. Then $1/x \in \bar{B}$, hence

$$(1/x)^n + a_1(1/x)^{n-1} + \cdots + a_n = 0 \text{ for some } a_i \in \bar{A}.$$

Multiplying by x^{n-1} we get $1/x = -(a_1 + a_2x + \cdots + a_nx^{n-1}) \in \bar{A}$. Therefore $\bar{A}$ is a field, i.e. $\mathfrak{m} = M \cap A$ is the maximal ideal p of A. Next, let P be a prime ideal of B with $P \cap A = p$. Then $\bar{B} = B/P$ is a domain which is integral over the field $\bar{A} = A/p$. Let $0 \neq y \in \bar{B}$; let $y^n + a_1y^{n-1} + \cdots + a_n = 0$

$(a_i \in \bar{A})$ be a relation of integral dependence for y, and assume that the degree n is the smallest possible. Then $a_n \neq 0$ (otherwise we could divide the equation by y to get a relation of degree n-1). Then $y^{-1} = -(y^{n-1} + a_1y^{n-2} + \cdots + a_{n-1})/a_n \in \bar{B}$, hence $\bar{B}$ is a field and P is maximal.

i) and ii). Let $p \in \mathrm{Spec}(A)$. Then $B_p = B \otimes_A A_p = (A - p)^{-1}B$ is integral over A_p and contains it as a subring. The prime ideals of B lying over p correspond to the prime ideals of B_p lying over pA_p, which are the maximal ideals of B_p by iv). Since $A_p \neq 0$, B_p is not zero and has maximal ideals. Of course there is no inclusion relation between maximal ideals. Thus i) and ii) are proved.

iii). Let $p \subset p'$ be in Spec(A) and P be in Spec(B) such that $P \cap A = p$. Then B/P contains, and is integral over, A/p. By i) there exists a prime P'/P lying over p'/p. Then P' is a prime ideal of B lying over p'.

vi). Put G = Aut(L/K) = the group of automorphisms of L over K. First assume L is finite over K. Then G is finite: $G = \{\sigma_1, \ldots, \sigma_n\}$. Let P and P' be prime ideals of B such that $P \cap A = P' \cap A$. Put $\sigma_i(P) = P_i$. (Note that $\sigma_i(B) = B$ so that $P_i \in \mathrm{Spec}(B)$.) If $P' \neq P_i$ for $i = 1, \ldots, n$, then $P' \not\subset P_i$ by ii), and there exists an element $x \in P'$ which is not in any P_i by (1.B). Put $y = (\prod_i \sigma_i(x))^q$, where q = 1 if ch(K) = 0 and $q = p^\nu$ with sufficiently large ν if ch(K) = p.

Then $y \in K$, and since A is integrally closed and $y \in B$ we get $y \in A$. But $y \notin P$ (for, we have $x \notin \sigma_i^{-1}(P)$ hence $\sigma_i(x) \notin P$) while $y \in P' \cap A = P \cap A$, contradiction.

When L is indinite over K, let K' be the invariant subfield of G ; then L is Galois over K', and K' is purely inseparable over K. If $K' \neq K$, let $p = ch(K)$. It is easy to see that the integral closure B' of A in K' has one and only one prime p' which lies over p, namely $p' = \{x \in B' \mid \exists\, q = p^{\nu}$ such that $x^q \in p\}$. Thus we can replace K by K' and p by p' in this case. Assume, therefore, that L is Galois over K. Let P and P' be in Spec(B) and let $P \cap A = P' \cap A = p$. Let L' be any finite Galois extension of K contained in L, and put

$$F(L') = \{\sigma \in G = \mathrm{Aut}(L/K) \mid \sigma(P \cap L') = P' \cap L'\}.$$

This set is not empty by what we have proved, and is closed in G with respect to the Krull topology (for the Krull topology of an infinite Galois group, see Lang: Algebra, p.233 exercise 19.) Clearly $F(L') \supseteq F(L'')$ if $L' \subseteq L''$. For any finite number of finite Galois extensions L'_i $(1 \leq i \leq n)$ there exists a finite Galois extension L'' containing all L'_i, therefore $\bigcap_i F(L'_i) \supseteq F(L'') \neq \emptyset$. As G is compact this means $\bigcap_{\text{all } L'} F(L') \neq \emptyset$. If σ belongs to this intersection we get $\sigma(P) = P'$.

v) Let $L_1 = \Phi B$, $K = \Phi A$, and let L be a normal extension of K containing L_1 ; let C denote the integral closure of A (hence also of B) in L. Let $P \in \mathrm{Spec}(B)$, $p = P \cap A$, $p' \in \mathrm{Spec}(A)$ and $p' \subset p$. Take a prime ideal $Q' \in \mathrm{Spec}(C)$ lying over p', and, using the going-up theorem for $A \subset C$, take $Q_1 \in \mathrm{Spec}(C)$ lying over p such that $Q' \subset Q_1$. Let Q be a prime ideal of C lying over P. Then by vi) there exists $\sigma \in \mathrm{Aut}(L/K)$ such that $\sigma(Q_1) = Q$. Put $P' = \sigma(Q') \cap B$. Then $P' \subset P$ and $P' \cap A = \sigma(Q') \cap A = Q' \cap A = p'$. Q.E.D.

Remark. In the example of (5.C), the ring $B = k[x, y]$ is integral over $A = k[x_1, x_2, y]$ since $x^2 - x - x_1 = 0$. Therefore the going-up theorem holds for $A \subset B$ while the going-down does not.

EXERCISES. 1. Let A be a ring and M an A-module. We shall say that M is surjectively-free over A if $A = \Sigma f(M)$ where sum is taken over $f \in \mathrm{Hom}_A(M,A)$. Thus, free $\Rightarrow$ surjectively-free. Prove that, if B is a surjectively free A-algebra, then (i) for any ideal I of A we have $IB \cap A = I$, and (ii) the canonical map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective. Prove also that, if B is an A-algebra with retraction (i.e. an A-linear map $r: B \to A$ such that $r \circ i = id_A$ (where $i: A \to B$ is the canonical map)) is surjectively-free over A.

2. Let k be a field and t and X be two independent indeterminates. Put $A = k[t]_{(t)}$. Prove that A[X] is free (hence faithfully flat) over A but that the going-up theorem does not hold for $A \subset A[X]$. Hint: consider the prime ideal $(tX - 1)$.

3. Let B be a ring, A be a subring and $p \in \text{Spec}(A)$. Suppose that B is integral over A and that there is only one prime ideal P of B lying over p. Then $B_P = B_p$. (By B_p we mean the localization of the A-module B at p, i.e. $B_p = B \otimes_A A_p$. Show that B_p is a local ring with maximal ideal PB_p.)

6. Constructible Sets

(6.A) A topological space X is said to be noetherian if the descending chain condition holds for the closed sets in X. The spectrum Spec(A) of a noetherian ring A is noetherian. If a space is covered by a finite number of noetherian subspaces then it is noetherian. Any subspace of a noetherian space is noetherian. A noetherian space is quasi-compact.

A closed set Z in a topological space X is irreducible if it is not expressible as the sum of two proper closed subsets. In a noetherian space X any closed set Z is uniquely decomposed into a finite number of irreducible closed sets : $Z = Z_1 \cup \ldots \cup Z_r$ such that $Z_i \not\subseteq Z_j$ for $i \neq j$. This follows easily from the definitions. The Z_i's are called the irreducible components of Z.

(6.B) Let X be a topological space and Z a subset of X.

We say Z is locally closed in X if, for any point z of Z, there exists an open neighborhood U of z in X such that $U \cap Z$ is closed in U. It is easy to see that Z is locally closed in X iff it is expressible as the intersection of an open set in X and a closed set in X.

Let X be a noetherian space. We say a subset Z of X is a constructible set in X if Z is a finite union of locally closed sets in X :

$$Z = \bigcup_{i=1}^{m} (U_i \cap F_i), \quad U_i \text{ open}, \quad F_i \text{ closed}.$$

(When X is not noetherian, the definition of a constructible set is more complicated, cf. EGA 0_{III}.)

If Z and Z' are constructible in X, so are $Z \cup Z'$, $Z \cap Z'$ and $Z - Z'$. This is clesr for $Z \cup Z'$. Repeated use of the formula

$$(U \cap F) - (U' \cap F') = U \cap F \cap (C(U') \cup C(F'))$$
$$= [U \cap \{F \cap C(U')\}] \cup [\{U \cap C(F')\} \cap F],$$

where C( ) denotes the complement in X, shows that Z - Z' is constructible. Taking Z = X we see the complement of a constructible set is constructible. Finally, $Z \cap Z' = C(C(Z) \cup C(Z'))$ is constructible.

We say a subset Z of a noetherian space X is pro-constructible (resp. ind-constructible) if it is the intersection (resp. union) of an arbitrary collection of constructible sets in X.

(6.C) PROPOSITION. Let X be a noetherian space and Z a subset of X. Then Z is constructible in X iff the following condition is satisfied.

(*) For each irreducible closed set X_o in X, either $X_o \cap Z$ is not dense in X_o, or $X_o \cap Z$ contains a non-empty open set of X_o.

Proof. (Necessity.) If Z is constructible we can write

$$X_o \cap Z = \bigcup_{i=1}^{m} (U_i \cap F_i),$$

where U_i is open in X, F_i is closed and irreducible in X and $U_i \cap F_i$ is not empty for each i. Then $\overline{U_i \cap F_i} = F_i$ since F_i is irreducible, therefore $\overline{X_o \cap Z} = \bigcup_i F_i$. If $X_o \cap Z$ is dense in X_o, we have $X_o = \bigcup F_i$ so that some F_i, say F_1, is equal to X_o. Then $U_1 \cap X_o = U_1 \cap F_1$ is a non-empty open set of X_o contained in $X_o \cap Z$.

(Sufficiency.) Suppose (*) holds. We prove the constructibility of Z by induction on the smallness of $\overline{Z}$, using the fact that X is noetherian. The empty set being constructible, we suppose that $Z \neq \emptyset$ and that any subset Z' of Z which satisfies (*) and is such that $\overline{Z'} \subset \overline{Z}$ is constructible.

Let $\overline{Z} = F_1 \cup \ldots \cup F_r$ be the decomposition of $\overline{Z}$ into the irreducible components. Then $F_1 \cap Z$ is dense in F_1 as one can

easily check, whence there exists, by (*), a proper closed subset F' of F_1 such that $F_1 - F' \subseteq Z$. Then, putting $F^* = F' \cup F_2 \cup \ldots \cup F_r$, we have $Z = (F_1 - F') \cup (Z \cap F^*)$. The set $F_1 - F^*$ is locally closed in X. On the other hand $Z \cap F^*$ satisfies the condition (*) because, if X_o is irreducible and if $\overline{Z \cap F^* \cap X_o} = X_o$, the closed set F^* must contain X_o and so $Z \cap F^* \cap X_o = Z \cap X_o$. Since $\overline{Z \cap F^*} \subseteq F^* \subset \overline{Z}$, the set $Z \cap F^*$ is constructible by the induction hypothesis. Therefore Z is constructible.

(6.D) LEMMA 1. Let A be a ring and F a closed subset of X = Spec(A). Then F is irreducible iff $F = V(p)$ for some prime ideal p. This p is unique and is called the generic point of F.

Proof. Suppose that F is irreducible. Since it is closed it can be written $F = V(I)$ with $I = \bigcap_{p \in F} p$. If I is not prime we would have elements a and b of A − I such that $ab \in I$. Then $F \not\subseteq V(a)$, $F \not\subseteq V(b)$ and $F \subseteq V(a) \cup V(b) = V(ab)$, hence $F = (F \cap V(a)) \cup (F \cap V(b))$, which contradicts the irreducibility. The converse is proved by noting $p \in V(p)$. The uniqueness comes from the fact that p is the smallest element of $V(p)$.

LEMMA 2. Let $\phi: A \to B$ be a homomorphism of rings. Put X =

Spec(A), Y = Spec(B) and $f = {}^a\phi: Y \to X$. Then f(Y) is dense in X iff $\mathrm{Ker}(\phi) \subseteq \mathrm{nil}(A)$. If, in particular, A is reduced, f(Y) is dense in X iff ϕ is injective.

Proof. The closure $\overline{f(Y)}$ in Spec(A) is the closed set V(I) defined by the ideal $I = \bigcap_{p \in Y} \phi^{-1}(p) = \phi^{-1}(\bigcap_{p \in Y} p)$, which is equal to $\phi^{-1}(\mathrm{nil}(B))$ by (1.E). Clearly $\mathrm{Ker}(\phi) \subseteq I$. Suppose that f(Y) is dense in X. Then V(I) = X, whence I = nil(A) by (1.E). Therefore $\mathrm{Ker}(\phi) \subseteq \mathrm{nil}(A)$. Conversely, suppose $\mathrm{Ker}(\phi) \subseteq \mathrm{nil}(A)$. Then it is clear that $I = \phi^{-1}(\mathrm{nil}(B)) = \mathrm{nil}(A)$, which means $\overline{f(Y)} = V(I) = X$.

(6.E) THEOREM 6. (Chevalley). Let A be a noetherian ring and B an A-algebra of finite type. Let $\phi: A \to B$ be the canonical homomorphism; put X = Spec(A), Y = Spec(B) and $f = {}^a\phi: Y \to X$. Then the image f(Y') of a constructable set Y' in Y is constructable in X.

Proof. First we show (6.C) can be applied to the case when Y' = Y. Let X_o be an irreducible closed set in X. Then $X_o = V(p)$ for some $p \in \mathrm{Spec}(A)$. Put A' = A/p, and B' = B/pB. Suppose that $X_o \cap f(Y)$ is dense in X_o. The map $\phi': A' \to B'$ induced by ϕ is then injective by Lemma 2. We want to show $X_o \cap f(Y)$ contains a non-empty open subset of X_o. By replacing

A, B and ϕ by A', B' and ϕ' respectively, it is enough to prove the following assertion :

(*) if A is a noetherian domain, and if B is a ring which contains A and which is finitely generated over A, there exists $0 \neq a \in A$ such that the elementary open set D(a) of X = Spec(A) is contained in f(Y), where Y = Spec(B) and f: $Y \to X$ is the canonical map.

Write $B = A[x_1, \ldots, x_n]$, and suppose that $x_1, \ldots, x_r$ are algebraically independent over A while each x_j $(r<j\leq n)$ satisfies algebraic relations over $A[x_1, \ldots, x_r]$. Put $A^* = A[x_1, \ldots, x_r]$, and choose for each $r < j \leq n$ a relation

$$g_{j0}(x)\cdot x_j^{d_j} + g_{j1}(x)\cdot x_j^{d_j-1} + \ldots = 0,$$

where $g_{j\nu}(x) \in A^*$, $g_{j0}(x) \neq 0$. Then $\prod_{j=r+1}^{n} g_{j0}(x_1, \ldots, x_r)$ is a non-zero polynomial in $x_1, \ldots, x_r$ with coefficients in A. Let $a \in A$ be any one of the non-zero coefficients of this polynomial. We claim that this element satisfies the requirement. In fact, suppose $p \in \mathrm{Spec}(A)$, $a \notin p$, and put $p^* = pA^* = p[x_1, \ldots, x_r]$. Then $\prod g_{j0} \notin p^*$, so that B_{p^*} is integral over $A^*_{p^*}$. Thus there exists a prime P of B_{p^*} lying over $p^*A^*_{p^*}$. We have $P \cap A = P \cap A^* \cap A = p[x_1, \ldots, x_r] \cap A = p$, therefore $p = P \cap A = (P \cap B) \cap A \in f(\mathrm{Spec}(B))$. Thus (*) is proved.

The general case follows from the special case treated above and from the following

LEMMA. Let B be a noetherian ring and let Y' be a constructible set in Y = Spec(B). Then there exists a B-algebra of finite type B' such that the image of Spec(B') in Spec(B) is exactly Y'.

Proof. First suppose $Y' = U \cap F$, where U is an elementary open set $U = D(b)$, $b \in B$, and F is a closed set V(I) defined by an ideal I of B. Put $S = \{1, b, b^2, \dots\}$ and $B' = S^{-1}(B/I)$. Then B' is a B-algebra of finite type generated by $1/\bar{b}$, where $\bar{b}$ = the image of b in B', and the image of Spec(B') in Spec(B) is clearly $U \cap F$.

When Y' is an arbitrary constructible set, we can write it as a finite union of locally closed sets $U_i \cap F_i$ $(1 \leq i \leq m)$ with U_i elementary open, because any open set in the noetherian space Y is a finite union of elementary open sets. Choose a B-algebra B'_i of finite type such that $U_i \cap F_i$ is the image of $\mathrm{Spec}(B'_i)$ for each i, and put $B' = B'_1 \times \cdots \times B'_m$. Then we can view Spec(B') as the disjoint union of $\mathrm{Spec}(B'_i)$'s, so the image of Spec(B) in Y is Y' as wanted.

(6.F) PROPOSITION. Let A be a noetherian ring, $\phi: A \to B$

a homomorphism of rings, X = Spec(A), Y = Spec(B), and $f = {}^a\phi: Y \to X$. Then f(Y) is pro-constructible in X.

Proof. We have $B = \varinjlim B_\lambda$, where the B_λ's are the subalgebras of B which are finitely generated over A. Put $Y_\lambda = \mathrm{Spec}(B_\lambda)$ and let $g_\lambda: Y \to Y_\lambda$ and $f_\lambda: Y_\lambda \to X$ denote the canonical maps. Clearly $f(Y) \subseteq \bigcap_\lambda f_\lambda(Y_\lambda)$. Actually the equality holds, for suppose that $p \in X - f(Y)$. Then $pB_p = B_p$, so that there exist elements $\pi_\alpha \in p$, $b_\alpha \in B$ $(1 \leq \alpha \leq m)$ and $s \in A - p$ such that $\Sigma_{\alpha=1}^m \pi_\alpha(b_\alpha/s) = 1$ in B_p, i.e., $s'(\Sigma\pi_\alpha b_\alpha - s) = 0$ in B for some $s' \in A - p$. If B_λ contains $b_1, \dots, b_m$ we have $1 \in p(B_\lambda)_p$, therefore $p \notin f_\lambda(Y_\lambda)$ for such λ. Thus we have proved $f(Y) = \bigcap f_\lambda(Y_\lambda)$. Since each $f_\lambda(Y_\lambda)$ is constructible by Th. 6, f(Y) is pro-constructible. Q.E.D.

(Remark. [EGA Ch.IV, §1] contains many other results on constructible sets, including generalization to non-noetherian case.)

(6.G) Let A be a ring and let $p, p' \in \mathrm{Spec}(A)$. We say that p' is a specialization of p and that p is a generalization of p' iff $p \subseteq p'$. If a subset Z of Spec(A) contains all specializations (resp. generalizations) of its points, we say Z is stable under specialization (resp. generalization). A closed (resp. open) set in Spec(A) is stable under specialization (resp. generalization).

LEMMA. Let A be a noetherian ring and X = Spec(A). Let Z be a pro-constructible set in X stable under specialization. Then Z is closed in X.

Proof. Let $Z = \bigcap E_\lambda$ with E_λ constructible in X. Let W be an irreducible component of $\bar{Z}$ and let x be its generic point. Then $W \cap Z$ is dense in W, hence a fortiori $W \cap E_\lambda$ is dense in W. Therefore $W \cap E_\lambda$ contains a non-empty open set of W by (6.C), so that $x \in E_\lambda$. Thus $x \in \bigcap E_\lambda = Z$. This means $W \subseteq Z$ by our assumption, and so we obtain $Z = \bar{Z}$. Q.E.D.

(6.H) Let ϕ: A → B be a homomorphism of rings, and put X = Spec(A), Y = Spec(B) and $f = {}^a\phi$: Y → X. We say that f is (or: ϕ is) submersive if f is surjective and if the topology of X is the quotient of that of Y (i.e. a subset X' of X is closed in X iff $f^{-1}(X')$ is closed in Y). We say f is (or: ϕ is) universally submersive if, for any A-algebra C, the homomorphism $\phi_C: C \to B \otimes_A C$ is submersive. (Submersiveness and universal submersiveness for morphisms of preschemes are defined in the same way, cf. EGA IV (15.7.8).)

THEOREM 7. Let A, B, ϕ, X, Y and f be as above. Suppose

that (1) A is noetherian, (2) f is surjective and (3) the going-down theorem holds for ϕ: A → B. Then ϕ is submersive.

Remark. The conditions (2) and (3) are satisfied, e.g., in the following cases:

(α) when ϕ is faithfully flat, or

(β) when ϕ is injective, assume B is an integral domain over A and A is an integrally closed integral domain.

In the case (α), ϕ is even universally submersive since faithful flatness is preserved by change of base. *)

Proof of Th. 7. Let $X' \subseteq X$ be such that $f^{-1}(X')$ is closed. We have to prove X' is closed. Take an ideal J of B such that $f^{-1}(X') = V(J)$. As $X' = f(f^{-1}(X'))$ by (2), application of (6.F) to the composite map A → B → B/J shows X' is pro-constructible. Therefore it suffices, by (6.G), to prove that X' is stable under specialization. For that purpose, let $\mathfrak{p}_1, \mathfrak{p}_2 \in$ Spec(A), $\mathfrak{p}_1 \supset \mathfrak{p}_2 \in X'$. Take $P_1 \in Y$ lying over $\mathfrak{p}_1$ (by (2)) and $P_2 \in Y$ lying over $\mathfrak{p}_2$ such that $P_1 \supset P_2$ (by (3)). Then P_2 is in the closed set $f^{-1}(X')$, so P_1 is also in $f^{-1}(X')$. Thus $\mathfrak{p}_1 = f(P_1) \in f(f^{-1}(X')) = X'$, as wanted.

*) In algebraic geometry, there are two important classes of universally submersive morphisms. Namely, the faithfully flat morphisms and the proper and surjective ones. The universal submersiveness of the latter is immediate from the definitions, while that of the former is essentially what we just proved.

(6.I) THEOREM 8. Let A be a noetherian ring and B an A-algebra of finite type. Suppose that the going-down theorem holds between A and B. Then the canonical map f: Spec(B) → Spec(A) is an open map (i.e. sends open sets to open sets).

Proof. Let U be an open set in Spec(B). Then f(U) is a constructible set (Th. 6). On the other hand the going-down theorem shows that f(U) is stable under generalization. Therefore, applying (6.G) to Spec(A) - f(U) we see that f(U) is open. Q.E.D.

(6.J) Let A and B be rings and ϕ: A → B a homomorphism. Suppose B is noetherian and that the going-up theorem holds for ϕ. Then ${}^a\phi$: Spec(B) → Spec(A) is a closed map (i.e. sends closed sets to closed sets).

Proof. Left to the reader as an easy exercise. (It has nothing to do with constructible sets.)

CHAPTER 3. ASSOCIATED PRIMES

In this chapter we consider noetherian rings only.

7. Ass(M)

(7.A) Throughout this section let A denote a noetherian ring and M an A-module. We say a prime ideal p of A is an associated prime of M, if one of the following equivalent conditions holds:

(i) there exists an element x ε M with Ann(x) = p ;

(ii) M contains a submodule isomorphic to A/p.

The set of the associated primes of M is denoted by $\mathrm{Ass}_A(M)$ or by Ass(M).

(7.B) PROPOSITION. Let p be a maximal element of the set of ideals {Ann(x) | x ε M, x ≠ 0}. Then p ε Ass(M).

Proof. We have to show that p is a prime. Let p = Ann(x), and suppose ab ε p, b ∉ p. Then bx ≠ 0 and abx = 0.

Since $\mathrm{Ann}(bx) \supseteq \mathrm{Ann}(x) = p$, we have $\mathrm{Ann}(bx) = p$ by the maximality of p. Thus $a \in p$.

COROLLARY 1. $\mathrm{Ass}(M) = \emptyset \iff M = 0$.

COROLLARY 2. The set of the zero-divisors for M is the union of the associated primes of M.

(7.C) LEMMA. Let S be a multiplicative subset of A, and put $A' = S^{-1}A$, $M' = S^{-1}M$. Then

$$\mathrm{Ass}_A(M') = f(\mathrm{Ass}_{A'}(M')) = \mathrm{Ass}_A(M) \cap \{p \mid p \cap S = \emptyset\},$$

where f is the natural map $\mathrm{Spec}(A') \to \mathrm{Spec}(A)$.

Proof. Left to the reader. One must use the fact that any ideal of A is finitely generated.

(7.D) THEOREM 9. Let A be a noetherian ring and M an A-module. Then $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$, and any minimal element of Supp(M) is in Ass(M).

Proof. If $p \in \mathrm{Ass}(M)$ there exists an exact sequence $0 \to A/p \to M$, and since A_p is flat over A the sequence $0 \to A_p/pA_p \to M_p$ is also exact. As $A_p/pA_p \neq 0$ we have $M_p \neq 0$, i.e. $p \in \mathrm{Supp}(M)$. Next let p be a minimal element of Supp(M). By (7.C), $p \in \mathrm{Ass}(M)$ iff $pA_p \in \mathrm{Ass}_{A_p}(M_p)$, therefore replacing A and M by A_p and M_p we can assume that (A,p) is a local ring, that $M \neq 0$ and that $M_q = 0$ for any prime $q \subset p$. Thus $\mathrm{Supp}(M) = \{p\}$. Since Ass(M) is not empty and is contained in Supp(M), we must have $p \in \mathrm{Ass}(M)$. Q.E.D.

COROLLARY. Let I be an ideal. Then the minimal associated primes of the A-module A/I are precisely the minimal prime over-ideals of I.

Remark. By the above theorem the minimal associated primes of M are the minimal elements of Supp(M). Associated primes which are not minimal are called embedded primes.

(7.E) THEOREM 10. Let A be a noetherian ring and M a finite A-module, $M \neq 0$. Then there exists a chain of submodules $(0) = M_0 \subset \cdots \subset M_{n-1} \subset M_n = M$ such that $M_i/M_{i-1} \simeq A/p_i$ for some $p_i \in \mathrm{Spec}(A)$ $(1 \leqslant i \leqslant n)$.

Proof. Since $M \neq 0$ we can choose $M_1 \subseteq M$ such that $M_1 \simeq A/p_1$ for some $p_1 \in \mathrm{Ass}(M)$. If $M_1 \neq M$ then we apply the same procedure to M/M_1 to find M_2, and so on. Since the ascending chain condition for submodules holds in M, the process must stop in finite steps.

(7.F) LEMMA. If $0 \to M' \to M \to M''$ is an exact sequence of A-modules, then $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$.

Proof. Take $p \in \mathrm{Ass}(M)$ and choose a submodule N of M isomorphic to A/p. If $N \cap M' = (0)$ then N is isomorphic to a submodule of M", so that $p \in \mathrm{Ass}(M'')$. If $N \cap M' \neq (0)$, pick $0 \neq x \in N \cap M'$. Since $N \simeq A/p$ and since A/p is a domain we have $\mathrm{Ann}(x) = p$, therefore $p \in \mathrm{Ass}(M')$.

(7.G) PROPOSITION. Let A be a noetherian ring and M a finite A-module. Then Ass(M) is a finite set.

Proof. Using the notation of Th.10, we have

$$\mathrm{Ass}(M) \subseteq \mathrm{Ass}(M_1) \cup \mathrm{Ass}(M_2/M_1) \cup \ldots \cup \mathrm{Ass}(M_n/M_{n-1})$$

by the lemma. On the other hand we have $\mathrm{Ass}(M_i/M_{i-1}) = \mathrm{Ass}(A/p_i) = \{p_i\}$, therefore $\mathrm{Ass}(M) \subseteq \{p_1, \ldots, p_n\}$.

8. Primary Decomposition

As in the preceding section, A denotes a noetherian ring and M an A-module.

(8.A) DEFINITIONS. An A-module is said to be co-primary if it has only one associated prime. A submodule N of M is said to be a primary submodule of M if M/N is co-primary. If $\mathrm{Ass}(M/N) = \{p\}$, we say N is p-primary or that N belongs to p.

(8.B) PROPOSITION. The following are equivalent:

(1) the module M is co-primary;

(2) $M \neq 0$, and if $a \in A$ is a zero-divisor for M then a is locally nilpotent on M (by this we mean that, for each $x \in M$, there exists an integer $n > 0$ such that $a^n x = 0$),

Proof. (1) → (2). Suppose $\mathrm{Ass}(M) = \{p\}$. If $0 \neq x \in M$, then $\mathrm{Ass}(Ax) = \{p\}$ and hence p is the unique minimal element of $\mathrm{Supp}(Ax) = V(\mathrm{Ann}(x))$ by (7.D). Thus p is the radical of $\mathrm{Ann}(x)$, therefore $a \in p$ implies $a^n x = 0$ for some $n > 0$.

(2) → (1). Put $p = \{a \in A \mid a \text{ is locally nilpotent on } M\}$. Clearly this is an ideal. Let $q \in \mathrm{Ass}(M)$. Then there exists an element x of M with $\mathrm{Ann}(x) = q$, therefore $p \subseteq q$ by the definition of p. Conversely, since p coincides with the union of the associated primes by assumption, we get $q \subseteq p$. Thus $p = q$ and $\mathrm{Ass}(M) = \{p\}$, so that M is co-primary.

Remark. When $M = A/q$, the condition (2) reads as follows:
(2') all zero-divisors of the ring A/q are nilpotent.
This is precisely the classical definition of a primary ideal q, cf. (1.A).

Exercise. Prove that, if M is a finitely generated co-primary A-module with $\mathrm{Ass}(M) = \{p\}$, then the annihilator Ann(M) is a p-primary ideal of A.

(8.C) Let p be a prime of A, and let Q_1 and Q_2 be p-primary submodules of M. Then the intersection $Q_1 \cap Q_2$ is also p-primary.

Proof. There is an obvious monomorphism $M/Q_1 \cap Q_2 \to M/Q_1 \oplus M/Q_2$. Hence $\emptyset \neq \mathrm{Ass}(M/Q_1 \cap Q_2) \subseteq \mathrm{Ass}(M/Q_1) \cup \mathrm{Ass}(M/Q_2) = \{p\}$.

(8.D) Let N be a submodule of M. A primary decomposition of N is an equation $N = Q_1 \cap \cdots \cap Q_r$ with Q_i primary in M. Such a decomposition is said to be irredundant if no Q_i can be omitted and if the associated primes of M/Q_i $(1 \leqslant i \leqslant r)$ are all distinct. Clearly any primary decomposition can be simplified to an irredundant one.

(8.E) LEMMA. If $N = Q_1 \cap \cdots \cap Q_r$ is an irredundant primary decomposition and if Q_i belongs to p_i, then we have

$$\mathrm{Ass}(M/N) = \{p_1, \ldots, p_r\}.$$

Proof. There is a natural monomorphism $M/N \to M/Q_1 \oplus \cdots \oplus M/Q_r$, whence $\mathrm{Ass}(M/N) \subseteq \bigcup_i \mathrm{Ass}(M/Q_i) = \{p_1, \ldots, p_r\}$. Conversely, $(Q_2 \cap \cdots \cap Q_r)/N$ is isomorphic to a non-zero submodule of M/Q_1 so that $\mathrm{Ass}(Q_2 \cap \cdots \cap Q_r/N) = \{p_1\}$, and since $Q_2 \cap \cdots \cap Q_r/N \simeq$ M/N we have $p_1 \in \mathrm{Ass}(M/N)$. Similarly for other p_i's.

(8.F) PROPOSITION. Let N be a p-primary submodule of an A-module M, and let p' be a prime ideal. Put $M' = M_{p'}$, and $N' = N_{p'}$, and let $\nu: M \to M'$ be the canonical map. Then

(i) $N' = M'$ if $p \not\subseteq p'$,

(ii) $N = \nu^{-1}(N')$ if $p \subseteq p'$ (symbolically one may write $N = M \cap N'$).

Proof. (i) We have $M'/N' = (M/N)_{p'}$ and $\mathrm{Ass}_A(M'/N') = \mathrm{Ass}_A(M/N) \cap \{\text{primes contained in } p'\} = \emptyset$. Hence $M'/N' = 0$.

(ii) Since $\mathrm{Ass}(M/N) = \{p\}$ and since $p \subseteq p'$, the multiplicative set $A - p'$ does not contain zero-divisors for M/N. Therefore the natural map $M/N \to (M/N)_{p'} = M'/N'$ is injective.

COROLLARY. Let $N = Q_1 \cap \cdots \cap Q_r$ be an irredundant primary decomposition of a submodule N of M, let Q_1 be p_1-primary and suppose p_1 is minimal in Ass(M/N). Then $Q_1 = M \cap N_{p_1}$, hence the primary component Q_1 is uniquely determined by N and by p_1.

Remark. If p_i is an embedded prime of M/N then the corresponding primary component Q_i is not necessarily unique.

(8.G) THEOREM 11. Let A be a noetherian ring and M an A-module. Then one can choose a p-primary submodule $Q(p)$ for each $p \in \mathrm{Ass}(M)$ in such a way that $(0) = \bigcap_{p \in \mathrm{Ass}(M)} Q(p)$.

Proof. Fix an associated prime p of M, and consider the set of submodules $N = \{N \subseteq M \mid p \notin \mathrm{Ass}(N)\}$. This set is not empty since (0) is in it, and if $N' = \{N_\lambda\}_\lambda$ is a linearly ordered subset of N then $\bigcup N_\lambda$ is an element of N (because $\mathrm{Ass}(\bigcup N_\lambda) = \bigcup \mathrm{Ass}(N_\lambda)$ by the definition of Ass). Therefore N has maximal elements by Zorn; choose one of them and call it $Q = Q(p)$. Since p is associated to M and not to Q we have $M \neq Q$. On the other hand, if M/Q had an associated prime p' other than p, then M/Q would contain a submodule $Q'/Q \simeq A/p'$ and then Q' would belong to N contradicting the maximality of Q. Thus $Q = Q(p)$ is a p-primary submodule of M. As $\mathrm{Ass}(\bigcap_p Q(p)) = \bigcap \mathrm{Ass}(Q(p)) = \emptyset$ we have $\bigcap Q(p) = (0)$.

COROLLARY. If M is finitely generated then any submodule N of M has a primary decomposition.

Proof. Apply the theorem to M/N and notice that Ass(M/N) is finite.

(8.H) Let p be a prime ideal of a noetherian ring A, and let $n > 0$ be an integer. Then p is the unique minimal prime over-ideal of p^n, therefore the p-primary component of p^n is uniquely determined; this is called the n-th symbolic power of p and is denoted by $p^{(n)}$. Thus $p^{(n)} = p^n A_p \cap A$. It can happen that $p^n \neq p^{(n)}$. Example: let k be a field and B = k[x, y] the polynomial ring in the indeterminates x and y. Put $A = k[x, xy, y^2, y^3]$ and $p = yB \cap A = (xy, y^2, y^3)$. Then $p^2 = (x^2y^2, xy^3, y^4, y^5)$. Since $y = xy/x \in A_p$, we have $B = k[x, y] \subseteq A_p$ and hence $A_p = B_{yB}$. Thus $p^{(2)} = y^2 B_{yB} \cap A = y^2 B \cap A = (y^2, y^3) \neq p^2$. An irredundant primary decomposition of p^2 is given by $p^2 = (y^2, y^3) \cap (x^2, xy^3, y^4, y^5)$.

9. Homomorphisms and Ass

(9.A) PROPOSITION. Let $\phi: A \to B$ be a homomorphism of noetherian rings and M a B-module. We can view M as an A-module by means of ϕ. Then

$$\mathrm{Ass}_A(M) = {}^a\phi(\mathrm{Ass}_B(M)).$$

Proof. Let $P \in \mathrm{Ass}_B(M)$. Then there exists an element x of M such that $\mathrm{Ann}_B(x) = P$. Since $\mathrm{Ann}_A(x) = \mathrm{Ann}_B(x) \cap A = P \cap A$ we have $P \cap A \in \mathrm{Ass}_A(M)$. Conversely, let $p \in \mathrm{Ass}_A(M)$ and take an element $x \in M$ such that $\mathrm{Ann}_A(x) = p$. Put $\mathrm{Ann}_B(x) = I$, let $I = Q_1 \cap \dots \cap Q_r$ be an irredundant primary decomposition of the ideal I and let Q_i be P_i-primary. Since $M \supseteq Bx \simeq B/I$ the set Ass(M) contains $\mathrm{Ass}(B/I) = \{P_1, \dots, P_r\}$. We will prove $P_i \cap A = p$ for some i. Since $I \cap A = p$ we have $P_i \cap A \supseteq p$ for all i. Suppose $P_i \cap A \neq p$ for all i. Then there exists $a_i \in P_i \cap A$ such that $a_i \notin p$, for each i. Then $a_i^m \in Q_i$ for all i if m is sufficiently large, hence $a = \Pi_i a_i^m \in I \cap A = p$, contradiction. Thus $P_i \cap A = p$ for some i and $p \in {}^a\phi(\mathrm{Ass}_B(M))$.

(9.B) THEOREM 12. (Bourbaki). Let $\phi: A \to B$ be a homomorphism of noetherian rings, E an A-module and F a B-module. Suppose F is flat as an A-module. Then:

(i) for any prime ideal p of A,

$$ {}^a\phi(\mathrm{Ass}_B(F/pF)) = \mathrm{Ass}_A(F/pF)) = \begin{cases} \{p\} & \text{if } F/pF \neq 0 \\ \emptyset & \text{if } F/pF = 0. \end{cases} $$

(ii) $\mathrm{Ass}_B(E \otimes_A F) = \bigcup_{p \in \mathrm{Ass}(E)} \mathrm{Ass}_B(F/pF)$.

COROLLARY. Let A and B be as above and suppose B is A-flat. Then

$$ \mathrm{Ass}_B(B) = \bigcup_{p \in \mathrm{Ass}(A)} \mathrm{Ass}_B(B/pB), $$

and ${}^a\phi(\mathrm{Ass}_B(B)) = \{p \in \mathrm{Ass}(A) \mid pB \neq B\}$. We have ${}^a\phi(\mathrm{Ass}_B(B)) = \mathrm{Ass}(A)$ if B is faithfully flat over A.

Proof of Theorem 12. (i) The module F/pF is flat over A/p (base change), and A/p is a domain, therefore F/pF is torsion-free as an A/p-module by (3.F). The assertion follows from this. (ii) The inclusion $\supseteq$ is immediate: if $p \in \mathrm{Ass}(E)$ then E contains a submodule isomorphic to A/p, whence $E \otimes F$ contains a submodule isomorphic to $(A/p) \otimes_A F = F/pF$ by the flatness of F. Therefore $\mathrm{Ass}_B(F/pF) \subseteq \mathrm{Ass}_B(E \otimes F)$. To prove the other inclusion $\supseteq$ is more difficult.

Step 1. Suppose E is finitely generated and coprimary with $\mathrm{Ass}(E) = \{p\}$. Then any associated prime $P \in \mathrm{Ass}_B(E \otimes F)$ lies over p. In fact, the elements of p are locally nilpotent (on E, hence) on $E \otimes F$, therefore $p \subseteq P \cap A$. On the other hand the elements of $A - p$ are E-regular, hence $E \otimes F$-regular by the flatness of F. Therefore $A - p$ does not meet P, so that $P \cap A = p$. Now, take a chain of submodules

$$ E = E_0 \supset E_1 \supset \dots \supset E_r = (0) $$

such that $E_i/E_{i+1} \simeq A/p_i$ for some prime ideal p_i. Then $E \otimes F = E_0 \otimes F \supseteq E_1 \otimes F \supseteq \dots \supseteq E_r \otimes F = (0)$ and $E_i \otimes F/E_{i+1} \otimes F \simeq F/p_iF$, so that $\mathrm{Ass}_B(E \otimes F) \subseteq \bigcup_i \mathrm{Ass}_B(F/p_iF)$. But if $P \in \mathrm{Ass}_B(F/p_iF)$ and if $p_i \neq p$ then $P \cap A = p_i$ (by (i)) $\neq p$, hence $P \notin \mathrm{Ass}_B(E \otimes F)$ by what we have just proved. Therefore $\mathrm{Ass}_B(E \otimes F) \subseteq \mathrm{Ass}_B(F/pF)$ as wanted.

Step 2. Suppose E is finitely generated. Let $(0) = Q_1 \cap \dots \cap Q_r$ be an irredundant primary decomposition of (0) in E. Then E is isomorphic to a submodule of $E/Q_1 \oplus \dots \oplus E/Q_r$, and so $E \otimes F$ is isomorphic to a submodule of the direct sum of the $E/Q_i \otimes F$'s. Then $\mathrm{Ass}_B(E \otimes F) \subseteq \bigcup \mathrm{Ass}_B(E/Q_i \otimes F) = \bigcup \mathrm{Ass}_B(F/p_iF)$.

Step 3. General case. Write $E = \bigcup_\lambda E_\lambda$ with finitely generated submodules E_λ. Then it follows from the definition of the associated primes that $\mathrm{Ass}(E) = \bigcup \mathrm{Ass}(E_\lambda)$ and $\mathrm{Ass}(E \otimes F) = \mathrm{Ass}(\bigcup E_\lambda \otimes F) = \bigcup \mathrm{Ass}(E_\lambda \otimes F)$. Therefore the proof is reduced to the case of finitely generated E.

(9.C) THEOREM 13. Let $A \to B$ be a flat homomorphism of noetherian rings; let q be a p-primary ideal of A and assume that pB is prime. Then qB is pB-primary.

Proof. Replacing A by A/q and B by B/qB, one may assume $q = (0)$. Then $\mathrm{Ass}(A) = \{p\}$, whence $\mathrm{Ass}(B) = \mathrm{Ass}_B(B/pB) = \{pB\}$ by the preceding theorem.

(9.D) We say a homomorphism $\phi: A \to B$ of noetherian rings is non-degenerate if ${}^a\phi$ maps Ass(B) into Ass(A). A flat homomorphism is non-degenerate by the Cor. of Th.12.

PROPOSITION. Let $f: A \to B$ and $g: A \to C$ be homomorphisms of noetherian rings. Suppose 1) $B \otimes_A C$ is noetherian, 2) f is flat and 3) g is non-degenerate. Then $1_B \otimes g: B \to B \otimes C$ is also non-degenerate. (In short, the property of being non-degenerate is preserved by flat base change.)

Proof. Left to the reader as an exercise.

CHAPTER 4. GRADED RINGS

10. Graded Rings and Modules

(10.A) A graded ring is a ring A equipped with a direct decomposition of the underlying additive group, $A = \bigoplus_{n \geq 0} A_n$, such that $A_n A_m \subseteq A_{n+m}$. A graded A-module is an A-module M, together with a direct decomposition as a group $M = \bigoplus_{n \in Z} M_n$ such that $A_n M_m \subseteq M_{n+m}$. Elements of A_n (or M_n) are called homogeneous elements of degree n. A submodule N of M is said to be a graded (or homogeneous) submodule if $N = \bigoplus (N \cap M_n)$. It is easy to see that this condition is equivalent to

(*) N is generated over A by homogeneous elements,

and also to

(**) if $x = x_r + x_{r+1} + \cdots + x_s \in N$, $x_i \in M_i$ (all i), then each x_i is in N.

If N is a graded submodule of M, then M/N is also a graded

A-module, in fact $M/N = \bigoplus M_n / N \cap M_n$.

(10.B) PROPOSITION. Let A be a noetherian graded ring, and M a graded A-module. Then

i) any associated prime p of M is a graded ideal, and there exists a homogeneous element x of M such that $p = \mathrm{Ann}(x)$;

ii) one can choose a p-primary graded submodule $Q(p)$ for each $p \in \mathrm{Ass}(M)$ in such a way that $(0) = \bigcap_{p \in \mathrm{Ass}(M)} Q(p)$.

<u>Proof</u>. i) Let $p \in \mathrm{Ass}(M)$. Then $p = \mathrm{Ann}(x)$ for some $x \in M$. Write $x = x_e + x_{e-1} + \dots + x_0$, $x_i \in M_i$. Let $f = f_r + f_{r-1} + \dots + f_0 \in p$, $f_i \in A_i$. We shall prove that all f_i are in p. We have

$$0 = fx = f_r x_e + (f_{r-1}x_e + f_r x_{e-1}) + \dots + (\sum_{i+j=p} f_i x_j) + \dots + f_0 x_0 .$$

Hence $f_r x_e = 0$, $f_{r-1}x_e + f_r x_{e-1} = 0, \dots, f_{r-e}x_e + \dots + f_r x_0 = 0$ (we put $f_i = 0$ for $i < 0$). It follows that $f_r^e x_i = 0$ for $0 \leq i \leq e$. Hence $f_r^e x = 0$, $f_r^e \in p$, therefore $f_r \in p$. By descending induction we see that all f_i are in p, so that p is a graded ideal. Then $p \in \mathrm{Ann}(x_i)$ for all i, and clearly $p = \bigcap_{i=0}^{e} \mathrm{Ann}(x_i)$. Since p is prime this means $p = \mathrm{Ann}(x_i)$ for some i.

ii) A slight modification of the proof of (8.G) Th.11

proves the assertion. Alternatively, we can derive it from Th.11 and from the following Lemma: <u>Let p be a graded ideal and let $Q \subset M$ be a p-primary submodule. Then the largest graded submodule Q' contained in Q (i.e. the submodule generated by the homogeneous elements in Q) is again p-primary.</u> Proof: let p' be an associated prime of M/Q'. Since both p and p' are graded, $p' = p$ iff $p' \cap H = p \cap H$ where H is the set of homogeneous elements of A. If $a \in p \cap H$ then a is locally nilpotent on M/Q'. If $a \in H$, $a \notin p$, then for $x \in M$ satisfying $ax \in Q'$, $x = \Sigma x_i$, $x_i \in M_i$, we have $ax_i \in Q' \subseteq Q$ for each i, hence $x_i \in Q$ for each i, hence $x \in Q'$. Thus $a \notin p'$.

(10.C) In this book we define a filtration of a ring A to be a descending sequence of ideals

$$(*) \qquad A = J_0 \supseteq J_1 \supseteq J_2 \supseteq \dots$$

satisfying $J_n J_m \subseteq J_{n+m}$. Given a filtration (*), we construct a graded ring A' as follows. The underlying additive group is

$$A' = \bigoplus_{n=0}^{\infty} J_n/J_{n+1} ,$$

and if $\xi \in A'_n = J_n/J_{n+1}$ and $\eta \in A'_m = J_m/J_{m+1}$, then choose $x \in J_n$ and $y \in J_m$ such that $\xi = (x \bmod J_{n+1})$ and $\eta = (y \bmod J_{m+1})$ and put $\xi\eta = (xy \bmod J_{n+m+1})$. This multiplication is well defined and makes A' a graded ring.

When I is an ideal of A, its powers define a filtration $A = I^0 \supseteq I \supseteq I^2 \supseteq \dots$. This is called the I-adic filtration, and its associated graded ring is denoted by $gr^I(A)$.

(10.D) PROPOSITION. If A is a noetherian ring and I an ideal, then $gr^I(A)$ is noetherian.

<u>Proof</u>. Write $gr^I(A) = \bigoplus_{n=0}^{\infty} A'_n$, $A'_n = I^n/I^{n+1}$. Then $A'_0 = A/I$ is a noetherian ring. Let $I = a_1A + \dots + a_rA$ and let $\bar{a}_i$ denote the image of a_i in I/I^2. Then $gr^I(A)$ is generated by $\bar{a}_1, \dots, \bar{a}_r$ over A'_0, therefore is noetherian.

(10.E) Let A be an artinian ring, and $B = A[X_1,\dots,X_m]$ the polynomial ring with its natural grading. Let $M = \bigoplus_{n=0}^{\infty} M_n$ be a finitely generated, graded B-module. Put $F_M(n) = \ell(M_n)$ for $n \geqslant 0$, where $\ell(\ )$ denotes the length of A-module. The numerical function F_M measures the largeness of M. The number $F_M(n)$ is finite for any n, because there exists a degree-preserving epimorphism of B-modules

$$\bigoplus_{i=1}^{p} B(d_i) \xrightarrow{f} M$$

where $B(d) = B$ as a module but $B(d)_n = B_{n-d}$ (in fact, if M is generated over B by homogeneous elements $\xi_1, \dots, \xi_p$ with $\deg(\xi_i) = d_i$ then the map $f: \bigoplus B(d_i) \to M$ such that

$f(b_1,\dots,b_p) = \Sigma\, b_i\xi_i$ satisfies the requirement), so that $\ell(M_n) \leqslant \Sigma\, \ell(B_{n-d_i}) < \infty$. Note that, since the number of the monomials of degree n in $X_1, \dots, X_m$ is $\binom{n+m-1}{m-1}$, we have $F_B(n) = \ell(B_n) = \binom{n+m-1}{m-1}\ell(A)$.

(10.F) THEOREM 14. Let A, B and M be as above. Then there is a polynomial $f_M(x)$ in one variable with rational coefficients such that $F_M(n) = f_M(n)$ for $n \gg 0$ (i.e. for all sufficiently large n).

<u>Proof</u>. Let P(M) denote the assertion for M. We consider the graded submodules N of M and we will prove P(M/N) by induction on the largeness of N (note that M satisfies the maximum condition for submodules). For N = M the assertion is obvious. Supposing P(M/N') is true for any graded submodule N' of M properly containing N, we prove P(M/N).

Case 1. If $N = N_1 \cap N_2$ with $N_i \supset N$ $(i = 1,2)$, then using $N_1 + N_2 / N_1 \simeq N_2/N$ we get

$$F_{M/N} = F_{M/N_2} + F_{N_1+N_2/N_1}$$

$$= F_{M/N_2} + F_{M/N_1} - F_{M/N_1+N_2}$$

and the assertion P(M/N) follows from $P(M/N_1)$, $P(M/N_2)$ and $P(M/N_1+N_2)$.

Case 2. If N is <u>irreducible</u> (in the sense that it is not the intersection of two larger submodules) then N is a primary submodule of M; let $\mathrm{Ass}(M/N) = \{p\}$. Put $I = X_1B + \dots + X_mB$ and $M' = M/N$. If $I \subseteq p$ then we claim that $M'_n = 0$ for large n. In fact, if $\{\xi_1,\dots,\xi_p\}$ is a set of homogeneous generators of M' over B and if $d = \max(\deg \xi_i)$, then $M'_{d+n} = I^n M'_d$. On the other hand we have $p^p M' = (0)$ for some $p > 0$. Thus $M'_n = 0$ for $n > p + d$, and P(M') holds with $f_{M'} = 0$. It remains to show the case $I \not\subseteq p$. We may suppose that $X_1 \notin p$. Then the sequence

$$0 \to (M/N)_{n-1} \xrightarrow{X_1} (M/N)_n \to (M/N + X_1M)_n \to 0$$

is exact for $n > 0$. Since $N + X_1M \supset N$ there is a polynomial $f(x) = a_dx^d + \dots + a_0$ with rational coefficients satisfying $P(M/N + X_1M)$. Thus there is an integer $n_0 > 0$ such that

$$F_{M/N}(n) - F_{M/N}(n-1) = a_dn^d + \dots + a_0 \quad (n > n_0).$$

Then

$$F_{M/N}(n) = a_d\Big(\sum_{i=n_0+1}^{n} i^d\Big) + a_{d-1}\Big(\sum_{i=n_0+1}^{n} i^{d-1}\Big) + \dots + a_0(n - n_0) + F_{M/N}(n_0) \qquad (n > n_0),$$

which means (cf. the remark below) that $F_{M/N}(n)$ is a polynomial of degree d + 1 in n for $n > n_0$, as wanted.

Remark 1. Put $\binom{x}{r} = x(x-1)\cdots(x-r+1)/\,r!$, $\binom{x}{0} = 1$. Then any polynomial f(x) of degree d in $\mathbf{Q}[x]$ can be written

$$f(x) = c_d\binom{x+d}{d} + c_{d-1}\binom{x+d-1}{d-1} + \dots + c_0\binom{x}{0}, \quad c_i \in \mathbf{Q}.$$

Moreover, since $\binom{x+r}{r} - \binom{x+r-1}{r} = \binom{x+r-1}{r-1}$, we have $f(x) - f(x-1) = c_d\binom{x+d-1}{d-1} + \dots + c_1\binom{x}{0}$. It follows by induction on d that, if $f(n) \in Z$ for $n \gg 0$, we have $c_i \in Z$ for all i (and so $f(n) \in Z$ for all $n \in Z$). It also follows that, if F(n) is a numerical function such that

$$F(n) - F(n-1) = f(n) \quad \text{for } n > n_0,$$

then $F(n) = c_d\binom{n+d+1}{d+1} + \dots + c_0\binom{n+1}{1} + \text{const}$ for $n > n_0$.

Remark 2. The polynomial $f_M(x)$ of the theorem is called the Hilbert polynomial or the Hilbert characteristic function of M.

11. Artin-Rees Theorem

(11.A) Let A be a ring, I an ideal of A and M an A-module. We define a filtration of M to be a descending sequence of submodules

$$(*) \qquad M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$$

The filtration is said to be I-admissible if $IM_i \subseteq M_{i+1}$ for all i, I-adic if $M_i = I^iM$, and essentially I-adic if it is I-admissible and if there is an integer i_0 such that $IM_i = M_{i+1}$ for $i > i_0$.

Given a filtration (*), we can define a topology on M by taking $\{x + M_n \mid n = 1,2,\dots\}$ as a fundamental system of neighborhoods of x for each $x \in M$. This topology is separated iff $\bigcap^{\infty} M_n = (0)$. The topology defined by the I-adic filtration is called the I-adic topology of M. An essentially I-adic filtration defines the I-adic topology on M, since $I^i M \subseteq M_i \subseteq I^{i-i_0} M_{i_0} \subseteq I^{i-i_0} M$.

(11.B) LEMMA. Let A, I and M be as above. Let $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \ldots$ be an I-admissible filtration such that all M_i are finite A-modules, let X be an indeterminate and put $A' = \Sigma I^n X^n$ and $M' = \Sigma M_n X^n$. Then the filtration is essentially I-adic iff M' is finitely gnerated over A'.

Proof. A' is a graded subring of A[X] and M' is a subgroup of $M \otimes_A A[X]$ such that $A'M' \subseteq M'$, hence M' is a graded A'-module. If $M' = A'\xi_1 + \ldots + A'\xi_r$, $\xi_i \in M'_{d_i}$, then $M'_n = (IX)M'_{n-1}$ (hence $M_n = IM_{n-1}$) for $n > \max d_i$. Conversely, if $M_n = IM_{n-1}$ for $n > d$, then M' is generated over A' by $M_{d-1}X^{d-1} + \ldots + M_1 X + M_0$, which is, in turn, generated by a finite number of elements over A.

(11.C) THEOREM 15. (Artin-Rees) Let A be a noetherian ring, I an ideal, M a finite A-module and N a submodule. Then there exists an integer $r > 0$ such that

$$I^n M \cap N = I^{n-r}(I^r M \cap N) \quad \text{for } n > r.$$

Proof. In other words, the theorem asserts that the filtration $(I^n M \cap N)_{n=0,1,2,\ldots}$ of N (induced on N by the I-adic filtration of M) is essentially I-adic. The filtration is I-admissible, and $N' = \sum (I^n M \cap N) X^n$ is a submodule of the finite A'-module $M' = \sum I^n M X^n$, where $A' = \sum I^n X^n$. If $I = a_1 A + \ldots + a_r A$ then $A' = A[a_1 X, \ldots, a_r X]$, so that A' is noetherian. Therefore N' is finite over A'. Thus the assertion follows from the preceding lemma.

Remark. It follows that the I-adic topology on M induces the I-adic topology on N. This is not always true if M is infinite over A.

(11.D) THEOREM 16. (Intersection theorem). Let A, I and M be as in the preceding theorem, and put $N = \bigcap^{\infty} I^n M$. Then we have $IN = N$.

Proof. For sufficiently large n we get $N = I^n M \cap N = I^{n-r}(I^r M \cap N) \subseteq IN \subseteq N$.

COROLLARY 1. If $I \subseteq \mathrm{rad}(A)$ then $\bigcap^{\infty} I^n M = (0)$. In other words M is I-adically separated in that case.

COROLLARY 2. (Krull) Let A be a noetherian ring and $I = \mathrm{rad}(A)$. Then $\bigcap^{\infty} I^n = (0)$.

COROLLARY 3. (Krull) Let A be a noetherian domain and let I be any proper ideal. Then $\bigcap^{\infty} I^n = (0)$.

Proof. Putting $N = \bigcap I^n$ we have $IN = N$, whence there exists $x \in I$ such that $(1 + x)N = (0)$ by (1.M). Since A is an integral domain and since $1 + x \neq 0$, we have $N = (0)$.

(11.E) PROPOSITION. Let A be a noetherian ring, M a finite A-module, I and ideal, and J an ideal generated by M-regular elements. Then there exists $r > 0$ such that

$$I^nM : J = I^{n-r}(I^rM : J) \quad \text{for } n > r.$$

Proof. Let $J = a_1A + \ldots + a_pA$ where the a_i are M-regular. Let S be the multiplicative subset of A generated by $a_1, \ldots, a_p$, and consider the A-submodules $a_j^{-1}M$ of $S^{-1}M$. Put $L = a_1^{-1}M \oplus \ldots \oplus a_p^{-1}M$ and let Δ_M be the image of the diagonal map $x \to (x, x, \ldots, x)$ from M to L. Then $M \simeq \Delta_M$, and

$$I^nM : J = \bigcap_j (I^nM : a_j) = \bigcap (I^n a_j^{-1}M \cap M) \simeq I^nL \cap \Delta_M ,$$

so that the assertion follows from the Artin-Rees theorem applied to L and Δ_M.

CHAPTER 5. DIMENSION

12. Dimension

(12.A) Let A be a ring, $A \neq 0$. A finite sequence of n+1 prime ideals $p_0 \supset p_1 \supset \cdots \supset p_n$ is called a prime chain of length n. If $p \in \mathrm{Spec}(A)$, the supremum of the lengths of the prime chains with $p = p_0$ is called the height of p and denoted by $ht(p)$. Thus $ht(p) = 0$ means that p is a minimal prime ideal of A.

Let I be a proper ideal of A. We define the height of I to be the minimum of the heights of the prime ideals containing I: $ht(I) = \inf\{ht(p) \mid p \supseteq I\}$.

The dimension of A is defined to be the supremum of the heights of the prime ideals in A:

$$\dim(A) = \sup\{ht(p) \mid p \in \mathrm{Spec}(A)\}.$$

It is also called the Krull dimension of A. If dim(A) is finite then it is equal to the length of the longest prime chains in A. For example, a principal ideal domain has dimension one.

It follows from the definition that

$$ht(p) = \dim(A_p) \qquad (p \in \mathrm{Spec}(A)),$$

and that, for any ideal I of A,

$$\dim(A/I) + ht(I) \leqslant \dim(A).$$

(12.B) Let $M \neq 0$ be an A-module. We define the dimension of M by

$$\dim(M) = \dim(A/\mathrm{Ann}(M)).$$

(When M = 0 we put dim(M) = -1.) Under the assumption that A is noetherian and $M \neq 0$ is finite over A, the following conditions are equivalent:

(1) M is an A-module of finite length,

(2) the ring A/Ann(M) is artinian,

(3) dim(M) = 0.

In fact, (3) $\Leftrightarrow$ (2) $\Rightarrow$ (1) is obvious by (2.C). Let us prove (1) $\Rightarrow$ (3). We suppose $\ell(M)$ is finite, and replacing A by A/Ann(M) we assume that Ann(M) = (0). If dim(A) > 0, take a minimal prime p of A which is not maximal. Since M is finite over A and since Ann(M) = (0), we easily see that $M_p \neq 0$. Hence p is a minimal member of Supp(M), so that $p \in \mathrm{Ass}(M)$. Then M contains a submodule isomorphic to A/p,

and since $\dim(A/p) > 0$ we have $\ell(A/p) = \infty$, contradiction. Therefore dim(A) (= dim(M)) = 0.

(12.C) Let A be a noetherian semi-local ring, and $\mathfrak{m} =$ rad(A). An ideal I is called an ideal of definition of A if $\mathfrak{m}^\nu \subseteq I \subseteq \mathfrak{m}$ for some $\nu > 0$. This is equivalent to saying that

$I \subseteq \mathfrak{m}$, and A/I is artinian.

Let I be an ideal of definition and M a finite A-modlle. Put

$$A^* = gr^I(A) = \oplus I^n/I^{n+1},$$

and

$$M^* = gr^I(M) = \oplus I^nM/I^{n+1}M.$$

Let $I = Ax_1 + \ldots + Ax_r$. Then the graded ring A* is a homomorphic image of $B = (A/I)[X_1, \ldots, X_r]$, and M* is a finite, graded A*-module. Therefore $F_{M^*}(n) = \ell(I^nM/I^{n+1}M)$ is a polynomial in n, of degree $\leqslant r-1$, for $n >> 0$. It follows that the function

$$\chi(M, I; n) \underset{\mathrm{def}}{=} \ell(M/I^nM) = \sum_{j=0}^{n-1} F_{M^*}(j)$$

is also a polynomial in n, of degree $\leqslant r$, for $n >> 0$. The polynomial which represents $\chi(M, I; n)$ for $n >>0$ is called the Hilbert polynomial of M with respect to I. If J is another ideal of definition of A, then $J^s \subseteq I$ for some $s > 0$, so that we have $\chi(M, I; n) \leqslant \chi(M, J; sn)$. Thus, if $\chi(M, I; n) = a_d n^d + \ldots + a_0$ and $\chi(M, J; n) = b_{d'} n^{d'} + \ldots + b_0$, then $d \leqslant d'$. By symmetry we get $d = d'$. Thus the degree d of the Hilbert polynomial is independent of the choice of I. We denote it by d(M). Remember that, if there exists an ideal of definition of A generated by r elements, then $d(M) \leqslant r$.

(12.D) PROPOSITION. Let A be a noetherian semi-local ring, I an ideal of definition of A and

$$0 \to M' \to M \to M'' \to 0$$

an exact sequence of finite A-modules. Then $d(M) = \max(d(M'), d(M''))$. Moreover, $\chi(M,I;\, n) - \chi(M',I;\, n) - \chi(M'',I;\, n)$ is a polynomial of degree $< d(M')$ for $n >> 0$.

Proof. Since $\ell(M''/I^nM'') = \ell(M/M'+I^nM) \leqslant \ell(M/I^nM)$, we get $d(M'') \leqslant d(M)$. Furthermore, $\chi(M,I;\, n) - \chi(M'',I;\, n) = \ell(M/I^nM) - \ell(M/M'+I^nM) = \ell(M'+I^nM/I^nM) = \ell(M'/M'\cap I^nM)$, and there exists $r > 0$ such that $M'\cap I^nM \subseteq I^{n-r}M'$ for $n > r$ by Artin-Rees. Thus $\ell(M'/I^nM') \geqslant \ell(M'/M'\cap I^nM) \geqslant \ell(M'/I^{n-r}M')$. This means that $\chi(M,I;\, n) - \chi(M'',I;\, n)$ and $\chi(M',I;\, n)$ have the same degree and the same leading term.

(12.E) LEMMA 1. Let A be a noetherian semi-local ring. Then $d(A) \geqslant \dim(A)$.

Proof. Induction on d(A). If $d(A) = 0$ then $\mathfrak{m}^\nu = \mathfrak{m}^{\nu+1} = \ldots$ for some $\nu > 0$. By the intersection theorem ((11.D) Cor.1), this implies $\mathfrak{m}^\nu = (0)$. Hence $\ell(A)$ is finite and $\dim(A) = 0$.

Suppose $d(A) > 0$. As the case $\dim(A) = 0$ is trivial, we assume $\dim(A) > 0$. Let $p_0 \supset \cdots \supset p_{e-1} \supset p_e = p$ be a prime chain of length $e > 0$, and take an element $x \in p_{e-1}$ such that $x \notin p$. Then $\dim(A/xA + p) \geqslant e - 1$. Applying the preceding proposition to the exact sequence

$$0 \to A/p \xrightarrow{x} A/p \to A/xA + p \to 0$$

we have $d(A/xA + p) < d(A/p) \leqslant d(A)$. Thus, by induction hypothesis we get $e - 1 \leqslant \dim(A/xA + p) \leqslant d(A/xA + p) < d(A)$. Hence $e \leqslant d(A)$, therefore $\dim(A) \leqslant d(A)$.

Remark. The lemma shows that the dimension of A is finite. When A is an arbitrary noetherian ring and p is a prime ideal, we have $ht(p) = \dim(A_p)$ so that $ht(p)$ is finite. (This was first proved by Krull by a different method.) Thus the descending chain condition holds for prime ideals in a noetherian ring. On the other hand, there are noetherian rings with infinite dimension.

(12.F) LEMMA 2. Let A be a noetherian semi-local ring, $M \neq 0$ a finite A-module, and $x \in rad(A)$. Then

$$d(M) \geqslant d(M/xM) \geqslant d(M) - 1.$$

Proof. Let I be an ideal of definition containing x. Then $\chi(M/xM,I;\, n) = \ell(M/xM + I^nM) = \ell(M/I^nM) - \ell(xM + I^nM/I^nM)$ and $xM + I^nM/I^nM \simeq xM/xM \cap I^nM \simeq M/(I^nM:x)$ and $I^{n-1}M \subseteq$

$(I^nM:x)$, therefore

$$\chi(M/xM, I; n) \geqslant \ell(M/I^nM) - \ell(M/I^{n-1}M)$$
$$= \chi(M, I; n) - \chi(M, I; n-1).$$

It follows that $d(M/xM) \geqslant d(M) - 1$.

(12.G) LEMMA 3. Let A and M be as above, and let $\dim(M) = r$. Then there exist r elements $x_1, \ldots, x_r$ of rad(A) such that $\ell(M/x_1M + \ldots + x_rM) < \infty$.

Proof. Let I be an ideal of definition of A. When $r = 0$ we have $\ell(M) < \infty$ and the assertion holds. Suppose $r > 0$, and let $p_1, \ldots, p_t$ be those minimal prime over-ideals of Ann(M) which satisfy $\dim(A/p_i) = r$. Then no maximal ideals are contained in any p_i, hence $\mathrm{rad}(A) \not\subseteq p_i$ $(1 \leqslant i \leqslant t)$. Thus by (1.B) there exists $x_1 \in \mathrm{rad}(A)$ which is not contained in any p_i. Then $\dim(M/x_1M) \leqslant r - 1$, and the assertion follows by induction on dim(M).

(12.H) THEOREM 17. Let A be a noetherian semi-local ring, $\mathfrak{m} = \mathrm{rad}(A)$ and $M \neq 0$ a finite A-module. Then $d(M) = \dim(M)$ = the smallest integer r such that there exist elements $x_1, \ldots, x_r$ of $\mathfrak{m}$ satisfying $\ell(M/x_1M + \ldots + x_rM) < \infty$.

Proof. If $\ell(M/x_1M + \ldots + x_rM) < \infty$ we have $d(M) \leqslant r$ by Lemma 2. When r is the smallest possible we have $r \leqslant \dim(M)$ by Lemma 3. It remains to prove $\dim(M) \leqslant d(M)$. Take a sequence of submodules $M = M_1 \supset M_2 \supset \ldots \supset M_{k+1} = (0)$ such that $M_i/M_{i+1} \simeq A/p_i$, $p_i \in \mathrm{Spec}(A)$. Then $p_i \supseteq \mathrm{Ann}(M)$ and $\mathrm{Ass}(M) \subseteq \{p_1, \ldots, p_k\}$. Since $\mathrm{Supp}(M) = V(\mathrm{Ann}(M))$ all the minimal over-ideals of Ann(M) are in Ass(M) (hence also in $\{p_1, \ldots, p_k\}$) by (7.D). Therefore

$$d(M) = \max d(A/p_i) \quad \text{by (12.D)}$$
$$\geqslant \max \dim(A/p_i) \quad \text{by Lemma 1}$$
$$= \dim(A/\mathrm{Ann}(M)) = \dim(M),$$

which completes the proof.

(12.I) THEOREM 18. Let A be a noetherian ring and $I = (a_1, \ldots, a_r)$ be an ideal generated by r elements. Then any minimal prime over-ideal p of I has height $\leqslant r$. In particular, $\mathrm{ht}(I) \leqslant r$.

Proof. Since pA_p is the only prime ideal of A_p containing IA_p, the ring $A_p/IA_p = A_p/(a_1A_p + \ldots + a_rA_p)$ is artinian. Therefore $\mathrm{ht}(p) = \dim(A_p) \leqslant r$ by Th. 17.

(12.J) Let $(A, \mathfrak{m}, k)$ be a noetherian local ring of dimension d. In this case, an ideal of definition of A and a primary ideal belonging to $\mathfrak{m}$ are the same thing. We know (Th.17) that no ideals of definition are generated by less than d elements, and that there are ideals of definition generated by exactly d elements. If $(x_1,\dots,x_d)$ is an ideal of definition then we say that $\{x_1,\dots,x_d\}$ is a <u>system of parameters</u> of A. If there exists a system of parameters generating the maximal ideal $\mathfrak{m}$, then we say that A is a <u>regular local ring</u> and we call such a system of parameters a <u>regular system of parameters</u>. Since the number of elements of a minimal basis of $\mathfrak{m}$ is equal to $\mathrm{rank}_k\, \mathfrak{m}/\mathfrak{m}^2$, we have in general

$$\dim(A) \leqslant \mathrm{rank}_k\, \mathfrak{m}/\mathfrak{m}^2,$$

and the equality holds iff A is regular.

(12.K) PROPOSITION. Let $(A,\mathfrak{m})$ be a noetherian local ring and $x_1,\dots,x_d$ a system of parameters of A. Then

$$\dim(A/(x_1,\dots,x_i)) = d - i = \dim(A) - i$$

for each $1 \leqslant i \leqslant d$.

Proof. Put $\bar{A} = A/(x_1,\dots,x_i)$. Then $\dim(\bar{A}) \leqslant d - i$ since $\bar{x}_{i+1},\dots,\bar{x}_d$ generate an ideal of definition of $\bar{A}$. On the other hand, if $\dim(\bar{A}) = p$ and if $\bar{y}_1,\dots,\bar{y}_p$ is a system of parameters of $\bar{A}$, then $x_1,\dots,x_i,y_1,\dots,y_p$ generate an ideal of definition of A so that $p + i \geqslant d$, that is, $p \geqslant d - i$.

13. Homomorphism and Dimension

(13.A) Let $\phi\colon A \to B$ be a homomorphism of rings. Let $\mathfrak{p} \in$

Spec(A), and put $\kappa(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. Then $\mathrm{Spec}(B \otimes_A \kappa(\mathfrak{p}))$ is called the <u>fibre</u> over $\mathfrak{p}$ (of the canonical map ${}^a\phi\colon \mathrm{Spec}(B) \to \mathrm{Spec}(A)$). There is a canonical homeomorphism between ${}^a\phi^{-1}(\mathfrak{p})$ and $\mathrm{Spec}(B \otimes \kappa(\mathfrak{p}))$. If P is a prime ideal of B lying over $\mathfrak{p}$, the corresponding prime of $B \otimes \kappa(\mathfrak{p}) = B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$ is $PB_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$; denote it by P^*. Then the local ring $(B \otimes_A \kappa(\mathfrak{p}))_{P^*}$ can be identified with $B_P/\mathfrak{p}B_P = B_P \otimes_A \kappa(\mathfrak{p})$; in fact, we have $(B_\mathfrak{p})_{PB_\mathfrak{p}} = B_P$ and so $(B \otimes \kappa(\mathfrak{p}))_{P^*} = (B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p})_{PB_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}} = B_P/\mathfrak{p}B_P$ by (1.I.2). Now we have the following theorem.

(13.B) THEOREM 19. Let $\phi\colon A \to B$ be a homomorphism of noetherian rings; let $P \in \mathrm{Spec}(B)$ and $\mathfrak{p} = P \cap A$. Then

(1) $\mathrm{ht}(P) \leqslant \mathrm{ht}(\mathfrak{p}) + \mathrm{ht}(P/\mathfrak{p}B)$, in other words

$$\dim(B_P) \leqslant \dim(A_\mathfrak{p}) + \dim(B_P \otimes \kappa(\mathfrak{p}));$$

(2) the equality holds in (1) if the going-down theorem holds for ϕ (e.g. if ϕ is flat);

(3) if ${}^a\phi\colon \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective and if the going-down theorem holds, then we have i) $\dim(B) \geqslant \dim(A)$, and ii) $\mathrm{ht}(I) = \mathrm{ht}(IB)$ for any ideal I of A.

<u>Proof</u>. (1) Replacing A and B by $A_\mathfrak{p}$ and B_P, we may suppose that $(A,\mathfrak{p})$ and (B,P) are local rings such that $P \cap A = \mathfrak{p}$. We have to prove $\dim(B) \leqslant \dim(A) + \dim(B/\mathfrak{p}B)$. Let $a_1,\dots,a_r$ be a system of parameters of A and put $I = \Sigma a_i A$. Then

$p^n \subseteq I$ for some $n > 0$, so that $p^n B \subseteq IB \subseteq pB$. Thus the ideals pB and IB have the same radical. Therefore it follows from the definition that $\dim(B/pB) = \dim(B/IB)$. If $\dim(B/IB) = s$ and if $\{\bar{b}_1, \ldots, \bar{b}_s\}$ is a system of parameters of B/IB, then $b_1, \ldots, b_s$, $a_1, \ldots, a_r$ generate an ideal of definition of B. Hence $\dim(B) \leqslant r + s$.

(2) We use the same notation as above. If $ht(P/pB) = s$ there exists a prime chain of length s, $P = P_0 \supset P_1 \supset \ldots \supset P_s$, such that $P_s \supseteq pB$. As $p = P \cap A \supseteq P_i \cap A \supseteq p$, all the P_i lie over p. If $ht(p) = r$ then there exists a prime chain $p \supset p_1 \supset \ldots \supset p_r$ in A, and by going-down there exists a prime chain $P_s = Q_0 \supset Q_1 \supset \ldots \supset Q_r$ of B such that $Q_i \cap A = p_i$. Thus $P = P_0 \supset P_1 \supset \ldots \supset P_s \supset Q_1 \supset \ldots \supset Q_r$ is a prime chain of length $r + s$, therefore $ht(P) \geqslant r + s$.

(3) i) follows from (2). ii) Take a minimal prime over-ideal P of IB such that $ht(P) = ht(IB)$, and put $p = P \cap A$. Then $ht(P/pB) = 0$, hence by (2) we get $ht(IB) = ht(P) = ht(p) \geqslant ht(I)$. Conversely, let p be a minimal prime over-ideal of I such that $ht(p) = ht(I)$, and take a prime P of B lying over p. Replacing P if necessary we may suppose that P is a minimal prime over-ideal of pB. Then $ht(I) = ht(p) = ht(P) \geqslant ht(IB)$.

(13.C) THEOREM 20. Let B be a noetherian ring, and let A be a noetherian subring over which B is integral. Then

(1) $\dim(A) = \dim(B)$,

(2) for any $P \in Spec(B)$ we have $ht(P) \leqslant ht(P \cap A)$,

(3) if, moreover, the going-down theorem holds between A and B, then for any ideal J of B we have $ht(J) = ht(J \cap A)$.

Proof. Since $P_1 \subset P_2$ implies $P_1 \cap A \subset P_2 \cap A$ by (5.E) ii), we have $\dim(B) \leqslant \dim(A)$. On the other hand the going-up theorem proves $\dim(B) \geqslant \dim(A)$. Thus $\dim(B) = \dim(A)$. The inequality $ht(P) \leqslant ht(P \cap A)$ follows from Th.19 (1), since $ht(P/(P \cap A)B) = 0$ by (5.E) ii). To prove (3), first take a prime ideal P of B containing J such that $ht(P) = ht(J)$. Then $ht(P) = ht(P \cap A)$ by Th.19 (3), so that $ht(J) = ht(P) = ht(P \cap A) \geqslant ht(J \cap A)$. Next let p be a prime ideal of A containing $J \cap A$ such that $ht(p) = ht(J \cap A)$. Since B/J is integral over the subring $A/J \cap A$, there exists a prime P of B containing J and lying over p. Then $ht(J \cap A) = ht(p) = ht(P) \geqslant ht(J)$.

(13.D) THEOREM 21. Let $\phi: A \to B$ be a homomorphism of noetherian rings and suppose that the going-up theorem holds for ϕ. Let p and q be prime ideals of A such that $p \supset q$. Then $\dim(B \otimes_A \kappa(p)) \geqslant \dim(B \otimes_A \kappa(q))$.

Proof. Put $r = \dim(B \otimes_A \kappa(q))$ and $s = \mathrm{ht}(p/q)$. Take a prime chain $Q_0 \subset \dots \subset Q_r$ in B such that $Q_i \cap A = q$ for all i, and a prime chain $q = p_0 \subset p_1 \subset \cdots \subset p_s = p$ in A. By going-up we can find a prime chain $Q_r \subset Q_{r+1} \subset \cdots \subset Q_{r+s}$ in B such that $Q_{r+j} \cap A = p_j$. Then Q_{r+s} lies over p and $\mathrm{ht}(Q_{r+s}/Q_0) \geqslant r+s$. Applying Th.19 (1) to $A/q \to B/Q_0$ we get $\mathrm{ht}(Q_{r+s}/Q_0) \leqslant s + \mathrm{ht}(Q_{r+s}/Q_0 + pB) \leqslant s + \mathrm{ht}(Q_{r+s}/pB) \leqslant s + \dim(B \otimes \kappa(p))$. Thus $r \leqslant \dim(B \otimes \kappa(p))$, Q.E.D.

$$\begin{array}{lll} B & Q_{r+s} \supset \dots \supset Q_r & \\ & \qquad\qquad\quad \cup & \\ & \qquad\qquad\quad \vdots & \\ & \qquad\qquad\quad \cup & \\ & \qquad\qquad\quad Q_0 & \\ A & p = p_s \supset \dots \supset q & \end{array}$$

(13.E) Remark. The local form of theorem 21 is inconvenient for applications in algebraic geometry. The global counterpart of the going-up theorem is the closedness of a morphism. Thus, we have the following geometric theorem: Let $f: X \to Y$ be a closed morphism (e.g. a proper morphism) between noetherian schemes, and let y and y' be points of Y such that y' is a specialization of y. Then $\dim f^{-1}(y') \geqslant \dim f^{-1}(y)$. The proof is essentially the same as above.

14. Finitely Generated Extensions

(14.A) THEOREM 22. Let A be a noetherian ring and let $A[X_1,\dots,X_n]$ be a polynomial ring in n variables. Then

$$\dim A[X_1,\dots,X_n] = \dim A + n.$$

Proof. Enough to prove the case $n = 1$. Put $B = A[X]$. Let p be a prime ideal of A and let P be a prime ideal of B which is maximal among the prime ideals lying over p. We claim that $\mathrm{ht}(P/pB) = 1$. In fact, localizing A and B by the multiplicative set $A - p$ we can assume that p is a maximal ideal, and then $B/pB = (A/p)[X]$ is a polynomial ring in one variable over a field. Therefore B/pB is a principal ideal domain and every maximal ideal has height one. Thus $\mathrm{ht}(P/pB) = 1$. Since B is free over A we have $\mathrm{ht}(P) = \mathrm{ht}(p) + 1$ by Th.19 (2). As the map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective, we obtain $\dim B = \dim A + 1$.

COROLLARY. Let k be a field. Then $\dim k[X_1,\dots,X_n] = n$, and the ideal $(X_1,\dots,X_i)$ is a prime ideal of height i, for $1 \leqslant i \leqslant n$.

Proof. Since $(0) \subset (X_1) \subset (X_1,X_2) \subset \dots \subset (X_1,\dots,X_i) \subset \dots \subset (X_1,\dots,X_n)$ is a prime chain of length n and since $\dim k[X_1,\dots,X_n] = n$, the assertion is obvious.

(14.B) A ring A is said to be <u>catenary</u> if, for each pair of prime ideals p, q with $p \supset q$, $ht(p/q)$ is finite and is equal to the length of any maximal prime chain between p and q. (When A is noetherian, the condition $ht(p/q) < \infty$ is automatically satisfied.) Thus if A is a noetherian domain the following conditions are equivalent:

(1) A is catenary,

(2) for any pair of prime ideals p, q such that $p \supset q$, we have $ht(p) = ht(q) + ht(p/q)$,

(3) for any pair of prime ideals p, q such that $p \supset q$ with $ht(p/q) = 1$, we have $ht(p) = ht(q) + 1$.

If A is catenary, then clearly any localization $S^{-1}A$ and any homomorphic image A/I of A are also catenary.

A ring A is said to be <u>universally catenary</u> (u.c. for short) if A is noetherian and if every A-algebra of finite type is catenary. Since any A-algebra of finite type is a homomorphic image of $A[X_1,\dots,X_n]$ for some n, a noetherian ring A is universally catenary iff $A[X_1,\dots,X_n]$ is catenary for every $n \geq 0$.

If A is u.c., so are the localizations of A, the homomorphic images of A and any A-algebras of finite type.

(14.C) THEOREM 23. Let A be a noetherian domain, and let B be a finitely generated overdomain of A. Let $P \in Spec(B)$

and $p = P \cap A$. Then we have

$$(*) \qquad ht(P) \leq ht(p) + tr.deg._A B - tr.deg._{\kappa(p)} \kappa(P).$$

And the equality holds if A is universally catenary, or if B is a polynomial ring $A[X_1,\dots,X_n]$. (Here, $tr.deg._A B$ means the transcendence degree of the quotient field of B over that of A, and $\kappa(P)$ is the quotient field of B/P.)

<u>Proof</u>. Let $B = A[x_1,\dots,x_n]$. By induction on n it is enough to consider the case n = 1. So let $B = A[x]$. Replacing A by A_p, and B by $B_p = A_p[x]$, we assume that (A,p) is a local ring. Put $k = \kappa(p) = A/p$ and $I = \{f(X) \in A[X] \mid f(x) = 0\}$. Thus $B = A[X]/I$.

Case 1. $I = (0)$. Then $B = A[X]$, $tr.deg._A B = 1$ and $B/pB = k[X]$. Therefore $ht(P/pB) = 1$ or 0 according as $P \supset pB$ (then $tr.deg._k \kappa(P) = 0$) or $P = pB$ (then $tr.deg._k \kappa(P) = 1$). In other words $ht(P/pB) = 1 - tr.deg._k \kappa(P)$. On the other hand, $ht(P) = ht(p) + ht(P/pB)$ by Th.19. Thus the equality holds in (*).

Case 2. $I \neq (0)$. Then $tr.deg._A B = 0$. Let P^* be the inverse image of P in A[X], so that $P = P^*/I$ and $\kappa(P) = \kappa(P^*)$. Since A is a subring of $B = A[X]/I$ we have $A \cap I = (0)$. Therefore, if K denotes the quotient field of A then $ht(I) = ht(IK[X]) \leq \dim K[X] = 1$. Since $I \neq (0)$ we have $ht(I) = 1$. Hence $ht(P) \leq ht(P^*) - ht(I) = ht(P^*) - 1$, where the equality holds if A is u.c.. On the other hand we have $ht(P^*) = ht(p) + 1 - \text{tr.deg.}_k \kappa(P^*)$ by case 1, and $\kappa(P^*) = \kappa(P)$. Our assertions follow immediately from these.

<u>Definition</u>. We shall call the inequality (*) the dimension inequality. If B is a finitely generated overdomain of A and if the equality in (*) holds for any prime ideal of B, then we say that the <u>dimension formula holds</u> between A and B.

(14.D) COROLLARY. A noetherian ring A is universally catenary iff the following is true: A is catenary, and for any prime p of A and for any finitely generated overdomain B of A/p, the dimension formula holds between A/p and B.

<u>Proof</u>. If A (hence A/p) is u.c., then the condition holds by the theorem. Conversely, suppose the condition holds. Let B be any A-algebra of finite type and let $Q' \supset Q$ be prime ideals of B. We have to show that all maximal prime chains between Q' and Q have the same length. Replacing B by B/Q and A by $A/A \cap Q$ we can assume that B is a finitely generated overdomain of A. We are going to prove that for any prime ideals P and P' of B such that $P \supset P'$ we have $ht(P) = ht(P') + ht(P/P')$. Put $p = P \cap A$, $p' = P' \cap A$ and $n = \text{tr.deg.}_A B$. Then $ht(P) = ht(p) + n - \text{tr.deg.}_{\kappa(p)} \kappa(P)$, $ht(P') = ht(p') + n - \text{tr.deg.}_{\kappa(p')} \kappa(P')$, and by the assumption applied to B/P' and A/p', we also have $ht(P/P') = ht(p/p') + \text{tr.deg.}_{\kappa(p')} \kappa(P') - \text{tr.deg.}_{\kappa(p)} \kappa(P)$. Since A is catenary we have $ht(p) = ht(p') + ht(p/p')$. It follows that $ht(P) = ht(P') + ht(P/P')$.

(14.E) EXAMPLE. All noetherian rings that appear in algebraic geometry are catenary. And many algebraists had in vain tried to know if all noetherian rings are catenary, until Nagata constructed counterexamples in 1956 (cf. Local Rings, p.203, Example 2). In particular, he produced a noetherian local domain which is catenary but not universally catenary. We will sketch here his construction in its simplest form.

Let k be a field and let $S = k[[x]]$ be the formal power series ring over k in one variable x. Take an element $z = \sum_{i=1}^{\infty} a_i x^i$ of S which is algebraically independent over $k(x)$. (It is well known that the quotient field of S has an infinite transcendence degree over $k(x)$. Cf. e.g. Zariski-Samuel, Commutative Algebra, Vol.II, p.220.) Put $z_j = (z - \sum_{i<j} a_i x^i)/x^{j-1}$ for $j = 1,2,\dots$, (note that $z_1 = z$), and let R be the subring of S which is generated over k by x and by all the z_j's: $R = k[x, z_1, z_2, \dots]$. Consider the ideals $\mathfrak{m} = (x)$ and $\mathfrak{n} = (x-1, z_1, z_2, \dots)$ of R. Since $x(z_{j+1} + a_j) = z_j$ we have $z_j \in \mathfrak{m}$ for all j, and $\mathfrak{m}$ is a maximal ideal of R with $R/\mathfrak{m} = k$. The local ring $R_{\mathfrak{m}}$ is a subring of S and

and $\mathfrak{m}R_{\mathfrak{m}} = xR_{\mathfrak{m}} \subset xS$. Hence $\bigcap_n x^nR \subseteq \bigcap_n x^nS = (0)$. Then it is easy to see that any ideal ($\neq (0)$) of $R_{\mathfrak{m}}$ is of the form $x^iR_{\mathfrak{m}}$. Thus $R_{\mathfrak{m}}$ is noetherian, and is a regular local ring of dimension 1. On the other hand, R is a subring of the rational function field in two variables $k(x,z)$, and so we have $R/(x-1) = k[x,z_1,z_2,\dots]/(x-1) \simeq k[z]$, hence $\mathfrak{n} = (x-1,\ z)$ and $R/\mathfrak{n} \simeq k$. The local ring $R_{\mathfrak{n}}$ contains x^{-1} and hence it is a localization of the ring $R[x^{-1}] = k[x,\ x^{-1},\ z]$. This shows that $R_{\mathfrak{n}}$ is noetherian. Clearly $R_{\mathfrak{n}}$ is a regular local ring of dimension 2. Let B be the localization of R with respect to the multiplicatively closed subset $(R - \mathfrak{m}) \cap (R - \mathfrak{n})$. Then $\mathfrak{m}B$ and $\mathfrak{n}B$ are the only maximal ideals of B by (1.B), and the local rings $B_{\mathfrak{m}B} = R_{\mathfrak{m}}$ and $B_{\mathfrak{n}B} = R_{\mathfrak{n}}$ are noetherian. It follows easily (using (1.H)) that any ideal of B is finitely generated. Thus B is a semi-local noetherian domain. Put $I = \mathrm{rad}(B)$ and $A = k + I$. Then A is a subring of B, and it is easy to see that (A,I) is a local ring. As $B/I \simeq B/\mathfrak{m}B \oplus B/\mathfrak{n}B \simeq k \oplus k$ the ring B is a finite A-module. It follows (e.g. by Eakin's theorem cited in (2.D)) that A is also noetherian. We have $\mathrm{ht}(\mathfrak{m}B) = 1$ and $\mathrm{ht}(\mathfrak{n}B) = 2$, hence $\dim A = \dim B = 2$ by (13.C) Th.20 (1). If A were u.c. then we would have $\mathrm{ht}(\mathfrak{m}B) = \mathrm{ht}(\mathfrak{m}B \cap A) = \mathrm{ht}_A(I) = \dim A = 2$ by the dimension formula. Therefore A is not u.c.. But A is catenary because it is a local domain of dimension 2.

(14.F) THEOREM 24. Let $A = k[X_1,\dots,X_n]$ be a polynomial ring over a field k, and let I be an ideal of A with $\mathrm{ht}(I) = r$. Then we can choose $Y_1,\dots,Y_n \in A$ in such a way that

1) A is integral over $k[Y] = k[Y_1,\dots,Y_n]$, and
2) $I \cap k[Y] = (Y_1,\dots,Y_r)$.

Proof. Induction on r. If $r = 0$ then $I = (0)$ and we can take $Y_i = X_i$. When $r = 1$, let $Y_1 = f(X)$ be any non-zero element of I. Write $f(X) = \sum_{i=1}^{s} a_iM_i(X)$, where $0 \neq a_i \in k$ and $M_i(X)$ are distinct monomials in $X_1,\dots,X_n$, and take n positive integers $d_1 = 1,\ d_2,\ \dots,d_n$. If $M(X) = \prod X_i^{a_i}$ then let us call the integer $\sum a_id_i$ the weight of the monomial $M(X)$. By a suitable choice of $d_2,\dots,d_n$ we can see to it that no two of the monomials $M_1,\dots,M_s$ that appear in $f(X)$ have the same weight. (If p is a given prime number, we can take $d_2 = p^{\nu_2},\dots,d_s = p^{\nu_s}$ where $\nu_i - \nu_{i-1}$ $(i = 2,\dots,s;\ \nu_1 = 0)$ are large integers. This remark will be useful for some applications.) Put $Y_i = X_i - X_1^{d_i}$ $(i = 2,\dots,n)$. Then $Y_1 = f(X) = f(X_1,\ Y_2 + X_1^{d_2},\ \dots,\ Y_n + X_1^{d_n}) = a_iX_1^e + g(X_1,\ Y_2,\ \dots,\ Y_n)$ where g is a polynomial whose degree in X_1 is less than e and a_i is the coefficient of the term with highest weight in $f(X)$. Then X_1 is integral over $k[Y]$, and hence $X_i = Y_i + X_1^{d_i}$ $(i = 2,\dots,n)$ are also integral over $k[Y]$. The ideal (Y_1) of $k[Y]$ is prime of height 1, $(Y_1) \subseteq I \cap k[Y]$, and $\mathrm{ht}(I \cap k[Y]) = \mathrm{ht}(I) = 1$ by Th.20 (3). (Note that $k[Y]$ is integrally closed and so the going-down theorem holds between $k[X]$ and $k[Y]$.) Therefore $(Y_1) = I \cap k[Y]$, as wanted. When $r > 1$, let J be an ideal of $k[X]$ such that $J \subset I$, $ht(J) = r - 1$. (The existence of such J is easy to prove for any noetherian ring and for any ideal I of height r. Take $f_1 \in I$ from outside of the minimal prime ideals, and $f_2 \in I$ from outside of the minimal prime over-ideals of (f_1), and $f_3 \in I$ from outside of the minimal prime over-ideals of (f_1, f_2), and so on, and put $J = (f_1, \ldots, f_{r-1})$. Th.18 is the basis of this construction.) By induction hypothesis there exist $Z_1, \ldots, Z_n \in k[X]$ such that $k[X]$ is integral over $k[Z]$ and that $k[Z] \cap J = (Z_1, \ldots, Z_{r-1})$. Put $I' = I \cap k[Z]$. Then $ht(I') = ht(I) = r$, and so $I' \supset (Z_1, \ldots, Z_{r-1})$. Thus we can choose an element $0 \neq f(Z_r, \ldots, Z_n)$ of I'. Following the method we used for the case $r = 1$, we put $Y_i = Z_i$ $(i < r)$, $Y_r = f(Z_r, \ldots, Z_n)$, $Y_{r+j} = Z_{r+j} - Z_r^{e_j}$ $(1 \leq j \leq n-r)$. Then, for a suitable choice of $e_1, \ldots, e_{n-r}$, $k[Z]$ is integral over $k[Y]$. Moreover, $I \cap k[Y]$ contains the prime ideal $(Y_1, \ldots, Y_r)$ of height r and so coincides with it. The proof is completed.

Remark. The above proof shows that we can choose the Y_i's in such a way that $Y_{r+1}, \ldots, Y_n$ have the form $Y_{r+j} = X_{r+j} + F_j(X_1, \ldots, X_r)$, where F_j is a polynomial with coefficients in the prime subring k_0 of k (i.e. the canonical image of Z in k). If $ch(k) = p > 0$ then we can see to it that $F_j(X_1, \ldots, X_r) \in k_0[X_1^p, \ldots, X_r^p]$ for all j.

(14.G) COROLLARY.1. (Normalization theorem of E.Noether) Let $A = k[x_1, \ldots, x_n]$ be a finitely generated algebra over a field k. Then there exist $y_1, \ldots, y_r \in A$ which are algebraically independent over k such that A is integral over $k[y_1, \ldots, y_r]$. We have $r = \dim A$. If A is a domain we also have $r = \text{tr.deg.}_k A$.

Proof. Write $A = k[X_1, \ldots, X_n]/I$, and put $ht(I) = n - r$. According to the theorem there exist elements $Y_1, \ldots, Y_n$ of $k[X_1, \ldots, X_n]$ such that $k[X]$ is integral over $k[Y]$ and that $I \cap k[Y] = (Y_{r+1}, \ldots, Y_n)$. Putting $y_i = Y_i \bmod I$ $(1 \leq i \leq r)$ we get the required result. The equality $r = \dim A$ follows from Th.20. The last assertion is obvious, as A is algebraic over $k(y_1, \ldots, y_r)$.

COROLLARY 2. Let k be an algebraically closed field. Then any maximal ideal $\mathfrak{m}$ of $k[X_1, \ldots, X_n]$ is of the form $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$, $a_i \in k$.

Proof. Since $0 = \dim(A/\mathfrak{m}) = \text{tr.deg.}_k A/\mathfrak{m}$, we get $A/\mathfrak{m} \simeq k$. Hence $X_i \equiv a_i$ $(\mathfrak{m})$ for some $a_i \in k$ for each i. Since $(X_1 - a_1, \ldots, X_n - a_n)$ is obviously a maximal ideal, it is $\mathfrak{m}$.

(14.H) COROLLARY 3. Let A be a finitely generated algebra over a field k. Then (1) if A is an integral domain, we have $\dim(A/p) + \mathrm{ht}(p) = \dim A$ for any prime ideal p of A, and (2) A is universally catenary.

Proof. (1) Take $y_1, \ldots, y_r \in A$ as in Cor.1, and put $p' = p \cap k[y]$. Then $\dim A = r$, $\dim(A/p) = \dim(k[y]/p')$ and $\mathrm{ht}(p) = \mathrm{ht}(p')$. As $k[y]$ is isomorphic to the polynomial ring in r variables, we have $\mathrm{ht}(p') + \dim(k[y]/p') = r$ by the theorem.

(2) It suffices to prove that k is universally catenary. This is a consequence of (1) and (14.D), but we will give a direct proof. We are going to prove $k[X_1, \ldots, X_n]$ is catenary. Let $P \supset Q$ be prime ideals of $k[X] = k[X_1, \ldots, X_n]$. Then we have

$$\mathrm{ht}(P) = n - \dim(k[X]/P)$$

$$\mathrm{ht}(Q) = n - \dim(k[X]/Q),$$

and by (1)

$$\mathrm{ht}(P/Q) = \dim(k[X]/Q) - \dim(k[X]/P).$$

Therefore $\mathrm{ht}(P/Q) = \mathrm{ht}(P) - \mathrm{ht}(Q)$, Q.E.D.

(14.K) COROLLARY 4. (Dimension of intersection in an affine space). Let p_1 and p_2 be prime ideals in a polynomial ring $R = k[X_1, \ldots, X_n]$ over a field k, with $\dim(R/p_1) = r$, $\dim(R/p_2) = s$. Let q be any minimal prime over-ideal of $p_1 + p_2$. Then $\dim(R/q) \geqslant r + s - n$.
(In geometric terms this means that, if V_1 and V_2 are irreducible slosed sets of dimension r and s respectively, in an affine n-space $\mathrm{Spec}(k[X_1, \ldots, X_n])$. Then any irreducible component of $V_1 \cap V_2$ has dimension not less than $r + s - n$.)

Proof. Let $Y_1, \ldots, Y_n$ be another set of n indeterminates and let p_2' be the image of p_2 in $k[Y_1, \ldots, Y_n]$ by the isomorphism $k[X] \simeq k[Y]$ over k which maps X_i to Y_i $(1 \leqslant i \leqslant n)$. Let I be the ideal of $k[X,Y] = k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ generated by p_1 and p_2', and D the ideal $(X_1 - Y_1, \ldots, X_n - Y_n)$ of $k[X,Y]$. Then $k[X,Y]/I \simeq (R/p_1) \otimes_k (R/p_2)$, $k[X,Y]/D \simeq k[X]$. Take $\xi_1, \ldots, \xi_r \in R/p_1$ and $\eta_1, \ldots, \eta_s \in R/p_2$ such that R/p_1 (resp. R/p_2) is integral over $k[\xi]$ (resp. over $k[\eta]$). Then $k[X,Y]/I$ is integral over $k[\xi,\eta]$ which is a polynomial ring in r+s variables. Thus $\dim(k[X,Y]/I) = \dim k[\xi,\eta] = r + s$. Writing $k[X,Y]/I = k[x,y]$ we have $k[X,Y]/D + I = k[x,y]/(x_1 - y_1, \ldots, x_n - y_n)$. Since $k[X,Y]/I + D \simeq k[X]/p_1 + p_2$, the prime q of $k[X]$ corresponds to a minimal prime over-ideal Q of I + D in $k[X,Y]$ such that $k[X]/q \simeq k[X,Y]/Q$. Then Q/I is a minimal prime over-ideal of $(x_1 - y_1, \ldots, x_n - y_n)$ of $k[x,y]$, hence $\mathrm{ht}(Q/I) \leqslant n$ by Th.18. Therefore $\dim k[X]/q = \dim k[x,y]/(Q/I) = \dim k[x,y] - \mathrm{ht}(Q/I) \geqslant r + s - n$ by the preceding corollary.

(14.L) THEOREM 25. (Zero-point theorem of Hilbert).

Let k be a field, A be a finitely generated k-algebra and I be a proper ideal of A. Then the radical of I is the intersection of all maximal ideals containing I.

Proof. Let N denote the intersection of all maximal ideals containing I, and suppose that there is an element $a \in N$ which is not in the radical of I. Put $S = \{1, a, a^2, \ldots\}$ and $A' = S^{-1}A$. Then $IA' \neq (1)$, so there is a maximal ideal P' of A' containing IA'. Since A' is also finitely generated over k, we have $0 = \dim A'/P' = \text{tr.deg.}_k A'/P'$. Putting $A \cap P' = P$ we have $k \subseteq A/P \subseteq A'/P'$, hence $0 = \text{tr.deg.}_k A/P = \dim A/P$. Thus P is a maximal ideal of A containing I, and $a \notin P$, contradiction.

Remark. The theorem can be stated as follows: if A is a k-algebra of finite type, then the correspondence which maps each closed set V(I) of Spec(A) to $V(I) \cap \Omega(A)$ is a bijection between the closed sets of Spec(A) and the closed sets of $\Omega(A)$. When k is algebraically closed and $A \simeq k[X_1, \ldots, X_n]/I$ one can identify $\Omega(A)$ with the algebraic variety in k^n defined by the ideal I (i.e. the set of zero-points of I in k^n).

CHAPTER 6. DEPTH

15. M-regular Sequences

(15.A) Let A be a ring, M be an A-module and $a_1, \ldots, a_r$ be a sequence of elements of A. We write $(\underline{a})$ for the ideal $(a_1, \ldots, a_r)$, and $\underline{a}M$ for the submodule $\Sigma a_i M = (\underline{a})M$.

We say $a_1, \ldots, a_r$ is an M-regular sequence (or simply M-sequence) if the following conditions are satisfied:

(1) for each $1 \leq i \leq r$, a_i is not a zero-divisor on $M/(a_1, \ldots, a_{i-1})M$, and

(2) $M \neq \underline{a}M$.

When all a_i belong to an ideal I we say $a_1, \ldots, a_r$ is an M-regular sequence in I. If, moreover, there is no $b \in I$ such that $a_1, \ldots, a_r, b$ is M-regular, then $a_1, \ldots, a_r$ is said to be a maximal M-regular sequence in I. Notice that the notion of M-regular sequence depends on the order of the elements in the sequence.

LEMMA 1. Suppose that $a_1,\dots,a_r$ is M-regular and

$$a_1\xi_1 + \dots + a_r\xi_r = 0, \qquad \xi_i \in M.$$

Then $\xi_i \in \underline{a}M$ for all i.

Proof. Induction on r. For r = 1, $a_1\xi_1 = 0$ implies $\xi_1 = 0$. Let r > 1. Since a_r is $M/(a_1,\dots,a_{r-1})M$ - regular we have $\xi_r = \Sigma_{i=1}^{r-1} a_i\eta_i$, hence $\Sigma_{i=1}^{r-1} a_i(\xi_i + a_r\eta_i) = 0$. By induction hypothesis, for i < r we get $\xi_i + a_r\eta_i \in (a_1,\dots,a_{r-1})M$, so that $\xi_i \in (a_1,\dots,a_r)M$.

THEOREM 26. Let A, M be as above and $a_1,\dots,a_r \in A$ be an M-regular sequence. Then for every sequence $\nu_1,\dots,\nu_r$ of integers > 0, the sequence $a_1^{\nu_1},\dots,a_r^{\nu_r}$ is M-regular.

Proof. It suffices to prove that $a_1^{\nu},a_2,\dots,a_r$ is M-regular, because then $a_2,\dots,a_r$ will be $M/a_1^{\nu}M$ -regular and we can repeat the argument. We use induction on ν, the case $\nu = 1$ being true by assumption. Let $\nu > 1$ and assume that $a_1^{\nu-1},a_2,\dots,a_r$ is M-regular. a_1^{ν} is certainly M-regular. Let i > 1 and assume that $a_1^{\nu},a_2,\dots,a_{i-1}$ is an M-regular sequence. Let $a_i\omega = a_1^{\nu}\xi_1 + a_2\xi_2 + \dots + a_{i-1}\xi_{i-1}$. Then $\omega = a_1^{\nu-1}\eta_1 + a_2\eta_2 + \dots + a_{i-1}\eta_{i-1}$ by the induction hypothesis. So $a_1^{\nu-1}(a_1\xi_1 - a_i\eta_1) + a_2(\xi_2 - a_i\eta_2) + \dots + a_{i-1}(\xi_{i-1} - a_i\eta_{i-1}) = 0$, hence

$a_1\xi_1 - a_i\eta_1 \in (a_1^{\nu-1},a_2,\dots,a_{i-1})M$ by Lemma 1. It follows that $a_i\eta_1 \in (a_1,a_2,\dots,a_{i-1})M$, hence $\eta_1 \in (a_1,\dots,a_{i-1})M$ and so $\omega \in (a_1^{\nu},a_2,\dots,a_{i-1})M$.

(15.B) Let A be a ring, $X_1,\dots,X_n$ be indeterminates over A and M be an A-module. An element of $M\otimes_A A[X_1,\dots,X_n]$ can be viewed as a polynomial $F(X) = F(X_1,\dots,X_n)$ with coefficients in M. Therefore we write $M[X_1,\dots,X_n]$ for $M\otimes_A A[X_1,\dots,X_n]$. If $a_1,\dots,a_n \in A$ then $F(a) \in M$.

Let $a_1,\dots,a_n \in A$, $I = (\underline{a})$. We say that $a_1,\dots,a_n$ is an M-quasiregular sequence if the following condition is satisfied.

(*) For every $\nu > 0$ and for every homogeneous polynomial $F(X) \in M[X_1,\dots,X_n]$ of degree ν such that $F(a) \in I^{\nu+1}M$, we have $F \in IM[X]$.

Obviously this concept does not depend on the order of the elements. But $a_1,\dots,a_i$ (i < n) need not be M-quasiregular. The condition (*) can be stated in the following form.

(**) If $F(X) \in M[X_1,\dots,X_n]$ is homogeneous and $F(a) = 0$, then the coefficients of F are in IM.

Define a map $\phi : (M/IM)[X_1,\dots,X_n] \to gr^I M = \bigoplus_{\nu \geq 0} I^{\nu}M/I^{\nu+1}M$ as follows. If $F(X) \in M[X]$ is homogeneous of degree ν, let $\psi(F)$ = the image of F(a) in $I^{\nu}M/I^{\nu+1}M$. Then ψ is a degree-preserving additive map from M[X] to $gr^I(M)$, and since it maps $IM[X]$ to 0 it induces $\phi : (M/IM)[X] \to gr^I(M)$. This is clearly surjective, and (*) is equivalent to

(***) ϕ is an isomorphism: $(M/IM)[X_1,\ldots,X_n] \simeq gr^I(M)$.

THEOREM 27. Let A be a ring, M an A-module, $a_1,\ldots,a_n \in A$ and $I = \underline{a}M$. Then:

i) if $a_1,\ldots,a_n$ is M-quasiregular and $x \in A$, $IM:x = IM$, then $I^\nu M : x = I^\nu M$ for all $\nu > 0$,

ii) if $a_1,\ldots,a_n$ is M-regular then it is M-quasiregular;

iii) if M, M/a_1M, $M/(a_1,a_2)M,\ldots,M/(a_1,\ldots,a_{n-1})M$ are separated in the I-adic topology, then the converse of ii) is also true.

Remark. The separation condition of iii) is satisfied in either of the following cases:

(α) A is noetherian, M is finitely generated and $I \subseteq \mathrm{rad}(A)$,

(β) A is a graded ring $A = \bigoplus_{\nu \geq 0} A_\nu$, M is a graded A-module $M = \bigoplus_{\nu \geq 0} M_\nu$ and each a_i is homogeneous of degree > 0.

<u>Proof</u>. i) Induction on ν. Let $\nu > 1$, $\xi \in M$ and suppose $x\xi \in I^\nu M$. Then $\xi \in I^{\nu-1}M$, hence there exists a homogeneous polynomial $F(X) \in M[X_1,\ldots,X_n]$ of degree $\nu-1$ such that $\xi = F(a)$. Since $x\xi = xF(a) \in I^\nu M$, the coefficients of F are in $IM : x = IM$. Therefore $\xi = F(a) \in I^\nu M$.

ii) Induction on n. For $n = 1$ it is easy to check. Let

$n > 1$. By induction hypothesis $a_1,\ldots,a_{n-1}$ is M-quasiregular. Let $F(X) \in M[X_1,\ldots,X_n]$ be homogeneous of degree ν such that $F(a) = 0$. We will prove $F \in IM[X]$ by induction on ν. Write $F(X) = G(X_1,\ldots,X_{n-1}) + X_nH(X_1,\ldots,X_n)$. Then G and H are homogeneous of degree ν and $\nu-1$, respectively. By i) we have $H(a) \in (a_1,\ldots,a_{n-1})^\nu M : a_n = (a_1,\ldots,a_{n-1})^\nu M \subseteq I^\nu M$, therefore by the induction hypothesis on ν we have $H \in IM[X]$. Since $H(a) \in (a_1,\ldots,a_{n-1})^\nu M$ there exists $h(X) \in M[X_1,\ldots,X_{n-1}]$ which is homogeneous of degree ν such that $H(a) = h(a)$. Putting $G(X_1,\ldots,X_{n-1}) + a_nh(X_1,\ldots,X_{n-1}) = g(X)$ we have $g(a_1,\ldots,a_{n-1}) = 0$, hence by the induction hypothesis on n we have $g \in IM[X]$, hence $G \in IM[X]$ and so $F \in IM[X]$.

iii) If $a_1\xi = 0$ then $\xi \in IM$, hence $\xi = \Sigma a_i\eta_i$ and $\Sigma a_1a_i\eta_i = 0$, hence $\eta_i \in IM$ and $\xi \in I^2M$. In this way we see $\xi \in \bigcap_\nu I^\nu M = 0$. Thus a_1 is M-regular. Put $M_1 = M/a_1M$. If $a_2,\ldots,a_n$ is M_1-quasiregular then our assertion will be proved by induction on n. ($M \neq IM$ follows from the separation condition.) Let $F(X_2,\ldots,X_n) \in M[X_2,\ldots,X_n]$ be homogeneous of degree ν such that $F(a_2,\ldots,a_n) \in a_1M$. Put $F(a_2,\ldots,a_n) = a_1\omega$, and assume $\omega \in I^iM$. Then $\omega = G(a_1,\ldots,a_n)$ for some homogeneous polynomial of degree i, and

(†) $\qquad F(a_2,\ldots,a_n) = a_1G(a_1,\ldots,a_n)$.

If $i < \nu-1$ then $G \in IM[X]$ and so $\omega \in I^{i+1}M$. We thus conclude that $\omega \in I^{\nu-1}M$. If $i = \nu-1$ in (†), then $F(X_2,\ldots,X_n) - X_1G(X)$

$\in IM[X]$, and since F does not contain X_1 we have $F \in IM[X]$. Therefore F mod $a_1M[X] \in (a_2,\dots,a_n)M_1[X]$.

The theorem shows that, under the assumptions of iii), any permutation of an M-regular sequence is M-regular.

Examples. 1. Let k be a field and $A = k[X,Y,Z]$. Put $a_1 = X(Y-1)$, $a_2 = Y$ and $a_3 = Z(Y-1)$. Then a_1,a_2,a_3 is an A-regular sequence, while a_1,a_3,a_2 is not.

2. There exists a non-noetherian local ring $(A,\mathfrak{m})$ such that $\mathfrak{m} = (x_1, x_2)$ where x_1,x_2 is an A-regular sequence but x_2 is a zero-divisor in A. (J. Dieudonne, Nagoya Math. J. 27-1 (1966), 355-356.)

(15.C) If $a_1,a_2,\dots \in A$ is an M-regular sequence then the sequence of submodules a_1M, $(a_1,a_2)M,\dots$ is strictly increasing, hence the sequence of ideals $(a_1),(a_1,a_2),\dots$ is also strictly increasing. If A is noetherian such a sequence must stop. Therefore each M-regular sequence in I can be extended to a maximal M-regular sequence in I. The next theorem shows that any two maximal M-regular sequences in I have the same length if M is finitely generated.

THEOREM 28. Let A be a noetherian ring, M a finite A-module and I an ideal of A with $IM \neq M$. Let $n > 0$ be an integer.

Then the following are equivalent:

(1) $\mathrm{Ext}^i_A(N, M) = 0$ $(i < n)$ for every finite A-module N with $\mathrm{Supp}(N) \subseteq V(I)$;

(2) $\mathrm{Ext}^i_A(A/I, M) = 0$ $(i < n)$;

(3) there exists a finite A-module N with $\mathrm{Supp}(N) = V(I)$ such that $\mathrm{Ext}^i_A(N, M) = 0$ $(i < n)$;

(4) there exists an M-regular sequence $a_1,\dots,a_n$ of length n in I.

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) is trivial. (3) $\Rightarrow$ (4): We have $\mathrm{Ext}^0_A(N, M) = \mathrm{Hom}_A(N, M) = 0$. If no elements of I are M-regular, then I is contained in the join of the associated primes of M, hence in one of them by (1.B): $I \subseteq P$ for some $P \in \mathrm{Ass}(M)$. Then there exists an injection $A/P \to M$. Localizing at P we get $\mathrm{Hom}_{A_P}(k, M_P) \neq 0$, where $k = A_P/PA_P$. Since $P \in V(I) = \mathrm{Supp}(N)$, we have $N_P \neq 0$ and so $N_P/PN_P = N \otimes_A k \neq 0$ by NAK. Then $\mathrm{Hom}_k(N\otimes k, k) \neq 0$. Therefore $\mathrm{Hom}_{A_P}(N_P, M_P) \neq 0$. But the left hand side is a localization of $\mathrm{Hom}_A(N, M)$, which is 0. This is a contradiction, therefore there exists an M-regular element $a_1 \in I$. If $n > 1$, put $M_1 = M/a_1M$. From the exact sequence

$$(*) \qquad 0 \to M \xrightarrow{a_1} M \to M_1 \to 0$$

we get the long exact sequence

$$\dots\to \mathrm{Ext}^i_A(N,M) \to \mathrm{Ext}^i_A(N,M_1) \to \mathrm{Ext}^{i+1}_A(N,M) \to\dots$$

which shows that $\mathrm{Ext}_A^i(N, M_1) = 0$ $(i < n-1)$. So by induction on n there exists an M_1-regular sequence $a_2, \ldots, a_n$ in I.

(4) $\Rightarrow$ (1): Put $M_1 = M/a_1M$. Then $\mathrm{Ext}_A^i(N, M_1) = 0$ $(i<n-1)$ by induction on n. From (*) we get exact sequences

$$0 \to \mathrm{Ext}_A^i(N, M) \xrightarrow{a_1} \mathrm{Ext}_A^i(N, M) \quad (i < n).$$

But $\mathrm{Supp}(N) = V(\mathrm{Ann}(N)) \subseteq V(I)$, hence $I \subseteq$ radical of $\mathrm{Ann}(N)$, and so $a_1^r N = 0$ for some $r > 0$. Therefore a_1^r annihilates $\mathrm{Ext}_A^i(N, M)$ as well. Thus we have $\mathrm{Ext}_A^i(N, M) = 0$ $(i < n)$.

Under the assumptions of the theorem, we call the length of the maximal M-regular sequences in I the <u>I-depth</u> of M and denote it by $\mathrm{depth}_I(M)$. The theorem shows that

$$\mathrm{depth}_I(M) = \min\{i \mid \mathrm{Ext}_A^i(A/I, M) \neq 0\}.$$

When $(A, \mathfrak{m})$ is a local ring we write depth M or $\mathrm{depth}_A M$ for $\mathrm{depth}_{\mathfrak{m}}(M)$ and call it simply the <u>depth</u> of M. Thus depth M = 0 iff $\mathfrak{m} \in \mathrm{Ass}(M)$. If A is an arbitrary noetherian ring and $P \in \mathrm{Spec}(A)$, we have depth $M_P = 0 \Leftrightarrow PA_P \in \mathrm{Ass}_{A_P}(M_P) \Leftrightarrow P \in \mathrm{Ass}_A(M) \Rightarrow \mathrm{depth}_P(M) = 0$. In general we have $\mathrm{depth}_{A_P}(M_P) \geqslant \mathrm{depth}_P(M)$, because localization preserves exactness. When IM = M we define $\mathrm{depth}_I(M) = \infty$. For instance $\mathrm{depth}_I(M) = 0$ if M = 0.

(15.D) D. Rees introduced the notion of <u>grade</u>, which is closely related to depth, in 1957. (The grade of an ideal or module, Proc. Camb. Phil. Soc. 53, 28-42.) Let A be a noetherian ring, $M \neq 0$ be a finite A-module and $I = \mathrm{Ann}(M)$. Then he puts

$$\mathrm{grade}\ M = \inf\{i \mid \mathrm{Ext}_A^i(M,A) \neq 0\}.$$

According to the above theorem, we have

$$\mathrm{grade}\ M = \mathrm{depth}_I(A), \quad I = \mathrm{Ann}(M).$$

Also, it follows from the definition that

$$\mathrm{grade}\ M \leqslant \mathrm{proj.dim}\ M.$$

When I is an ideal of A, grade(A/I) is called the <u>grade</u> of I. [Thus grade I can have two meanings according to whether I is viewed as an ideal or as a module. When confusion can arise, the depth notation should be used.] The grade of an ideal I is $\mathrm{depth}_I(A)$, the length of maximal A-sequence in I. If $a_1, \ldots, a_r$ is an A-regular sequence it is easy to see that $\mathrm{ht}(a_1, \ldots, a_r) = r$. Therefore

$$\mathrm{grade}\ I \leqslant \mathrm{ht}\ I.$$

PROPOSITION. Let A be a noetherian ring, M ($\neq 0$) and N be finite A-modules, grade M = k and proj.dim $N = \ell < k$. Then

$$\mathrm{Ext}_A^i(M, N) = 0 \quad (i < k - \ell).$$

<u>Proof</u>. Induction on ℓ. If $\ell = 0$ then N is a direct summand of a free module. Since our assertion holds for A by definition, it holds for N also. If $\ell > 0$ take an exact sequence

$0 \to N' \to L \to N \to 0$ with L free. Then proj.dim $N' = \ell - 1$ and our assertion is proved by induction.

(15.E) LEMMA 2. (Ischebeck) Let $(A, \mathfrak{m})$ be a noetherian local ring and $M \neq 0$ and $N \neq 0$ be finite A-modules. Put depth $M = k$, $\dim N = r$. Then

$$\mathrm{Ext}^i_A(N, M) = 0 \quad (i < k - r).$$

Proof. Induction on r. If $r = 0$ then $\mathrm{Supp}(N) = \{\mathfrak{m}\}$ and the assertion follows from Th.28. Let $r > 0$. By p.51 Th.10 we can easily reduce to the case $N = A/P$, $P \in \mathrm{Spec}(A)$. Since $r = \dim A/P > 0$ we can pick $x \in \mathfrak{m} - P$, and then $0 \to N \xrightarrow{x} N \to N' \to 0$ is exact, where $N' = A/(P + Ax)$ has dimension $< r$. Then using induction hypothesis we get exact sequences

$$0 \to \mathrm{Ext}^i_A(N, M) \xrightarrow{x} \mathrm{Ext}^i_A(N, M) \to \mathrm{Ext}^{i+1}_A(N', M) = 0$$

for $i < k-r$, and these Ext must vanish by NAK. Q.E.D.

THEOREM 29. Let $(A, \mathfrak{m})$ be a noetherian local ring and let $M \neq 0$ be a finite A-module. Then we have

$$\text{depth } M \leq \dim(A/P) \quad \text{for every } P \in \mathrm{Ass}(M).$$

Proof. If $P \in \mathrm{Ass}(M)$ then $\mathrm{Hom}_A(A/P, M) \neq 0$, hence depth $M \leq \dim(A/P)$ by Lemma 2.

(15.F) LEMMA 3. Let A be a ring, and let E and F be

finite A-modules. Then $\mathrm{Supp}(E \otimes F) = \mathrm{Supp}(E) \cap \mathrm{Supp}(F)$.

Proof. For $P \in \mathrm{Spec}(A)$ we have $(E \otimes F)_P = (E \otimes_A F) \otimes_A A_P = E_P \otimes_{A_P} F_P$. Therefore the assertion is equivalent to the following: Let $(A, \mathfrak{m}, k)$ be a local ring and E and F be finite A-modules. Then $E \otimes F \neq 0 \Leftrightarrow E \neq 0$ and $F \neq 0$. Now $\Rightarrow$ is trivial. Conversely, if $E \neq 0$ and $F \neq 0$ then $E \otimes k = E/\mathfrak{m}E \neq 0$ by NAK. Similarly $F \otimes k \neq 0$. Since k is a field we get $(E \otimes F) \otimes k = (E \otimes k) \otimes_k (F \otimes k) \neq 0$, so $E \otimes F \neq 0$.

LEMMA 4. Let A be a noetherian local ring and M be a finite A-module. Let $a_1, \ldots, a_r$ be an M-regular sequence. Then

$$\dim M/(a_1, \ldots, a_r)M = \dim M - r.$$

Proof. We have $\dim M/\underline{a}M \geq \dim M - r$ by Th.17. On the other hand, suppose f is an M-regular element. We have $\mathrm{Supp}(M/fM) = \mathrm{Supp}(M) \cap \mathrm{Supp}(A/fA) = \mathrm{Supp}(M) \cap V(f)$ by Lemma 3, and f is not in any minimal element of Supp(M), in other words V(f) does not contain any irreducible component of Supp(M). Hence $\dim(M/fM) < \dim M$. This proves $\dim M/\underline{a}M \leq \dim M - r$.

PROPOSITION. Let A be a noetherian ring, M a finite A-module and I an ideal. Then

$$\mathrm{depth}_I(M) = \inf\{\text{depth } M_P \mid P \in V(I)\}.$$

Proof. Let n denote the value of the right hand side. If $n = 0$ then depth $M_P = 0$ for some $P \supseteq I$, and then $I \subseteq P \in \mathrm{Ass}(M)$. Thus $\mathrm{depth}_I(M) = 0$. If $0 < n < \infty$, then I is not contained in any associated prime of M, and so there exists by (1.B) an M-regular element $a \in I$. Put $M' = M/aM$. Then $\mathrm{depth}\ (M')_P = \mathrm{depth}\ M_P/aM_P = \mathrm{depth}\ M_P - 1$ for $P \supseteq I$, and $\mathrm{depth}_I(M') = \mathrm{depth}_I(M) - 1$. Therefore our assertion is proved by induction on n. If $n = \infty$ then $PM_P = M_P$ for all $P \in V(I)$. If $IM \neq M$ we would have $(M/IM)_P \neq 0$ for every $P \in \mathrm{Supp}(M/IM) = V(I) \cap \mathrm{Supp}(M)$. If P is a minimal element of $\mathrm{Supp}(M/IM)$ then $\mathrm{Supp}_{A_P}(M/IM)_P = \{PA_P\}$, hence the A_P-module $(M/IM)_P = M_P/IM_P$ is coprimary in M_P and $P^sM_P \subseteq IM_P$ for some $s > 0$ by (8.B). Hence $PM_P \neq M_P$, contradiction. Therefore $IM = M$ and $\mathrm{depth}_I(M) = \infty$.

16. Cohen-Macaulay Rings

(16.A) Let $(A, \mathfrak{m})$ be a noetherian local ring and M a finite A-module. We know that depth $M \leqslant \dim M$ provided that $M \neq 0$. We say that M is Cohen-Macaulay (briefly, C.M.) if $M = 0$ or if depth $M = \dim M$. If the local ring A is C.M. as A-module then we call A a Cohen-Macaulay ring.

THEOREM 30. Let $(A, \mathfrak{m})$ be a noetherian local ring and M a finite A-module. Then:

i) if M is a C.M. module and $P \in \mathrm{Ass}(M)$, then we have depth $M = \dim A/P$. Consequently M has no embedded primes;

ii) if $a_1, \ldots, a_r$ is an M-regular sequence in $\mathfrak{m}$ and $M' = M/\underline{a}M$, then

M is C.M. $\Leftrightarrow$ M' is C.M. ;

iii) if M is C.M., then for every $P \in \mathrm{Spec}(A)$ the A_P-module M_P is C.M., and if $M_P \neq 0$ we have

$$\mathrm{depth}_P(M) = \mathrm{depth}_{A_P} M_P.$$

Proof. i) Since $\mathrm{Ass}(M) \neq \emptyset$, M is not 0 and so depth M = dim M. Since $P \in \mathrm{Supp}(M)$ we have $\dim M \geqslant \dim A/P$, and $\dim A/P \geqslant$ depth M by Th.29.

ii) By NAK we have $M = 0$ iff $M' = 0$. Suppose $M \neq 0$. Then $\dim M' = \dim M - r$ by Lemma 4, and depth M' = depth $M - r$.

iii) We may assume that $M_P \neq 0$. Hence $P \supseteq \mathrm{Ann}(M)$. We know that $\dim M_P \geqslant \mathrm{depth}_{A_P} M_P \geqslant \mathrm{depth}_P(M)$. So we will prove $\mathrm{depth}_P(M) = \dim M_P$ by induction on $\mathrm{depth}_P(M)$. If $\mathrm{depth}_P(M) = 0$ then P is contained in some $P' \in \mathrm{Ass}(M)$, but $\mathrm{Ann}(M) \subseteq P \subseteq P'$ and the associated primes of M are the minimal prime over-ideals of Ann(M) by i). Hence $P = P'$, and $\dim M_P = 0$. Next suppose $\mathrm{depth}_P(M) > 0$; take an M-regular element $a \in P$ and put $M_1 = M/aM$. Since localization preserves exactness, the element a is M_P-regular. Therefore we have

$\dim (M_1)_P = \dim M_P/aM_P = \dim M_P - 1$ and $\mathrm{depth}_P(M_1) = \mathrm{depth}_P(M) - 1$. Since M_1 is C.M. by ii), by induction hypothesis we have $\dim (M_1)_P = \mathrm{depth}_P(M_1)$. We are done.

(16.B) THEOREM 31. Let $(A, \mathfrak{m})$ be a C.M. local ring. Then: i) for every proper ideal I of A, we have

$$\mathrm{ht}\, I = \mathrm{depth}_I(A) = \mathrm{grade}\, I, \quad \mathrm{ht}\, I + \dim A/I = \dim A;$$

ii) A is catenary;

iii) for every sequence $a_1, \ldots, a_r$ in $\mathfrak{m}$, the following conditions are equivalent:

(1) the sequence $a_1, \ldots, a_r$ is A-regular,

(2) $\mathrm{ht}\,(a_1, \ldots, a_i) = i \quad (1 \leq i \leq r)$,

(3) $\mathrm{ht}\,(a_1, \ldots, a_r) = r$,

(4) there exist $a_{r+1}, \ldots, a_n$ ($n = \dim A$) in $\mathfrak{m}$ such that $\{a_1, \ldots, a_n\}$ is a system of parameters of A.

Proof. iii) (1) ⇒ (2) is easy by p.77 Th.18. (2) ⇒ (3) is trivial. (3) ⇒ (4): trivial if $\dim A = r$. If $\dim A > r$ then $\mathfrak{m}$ is not a minimal prime over-ideal of $(a_1, \ldots, a_r)$, so we can take $a_{r+1} \in \mathfrak{m}$ which is not in any minimal prime over-ideal of $(a_1, \ldots, a_r)$. Then $\mathrm{ht}\,(a_1, \ldots, a_{r+1}) = r + 1$, and we can continue. [Thus these implications are true for any noetherian local ring.] (4) ⇒ (1): It suffices to show that every system of parameters $x_1, \ldots, x_n$ of A is an A-regular sequence. If $P \in \mathrm{Ass}(A)$ then $\dim A/P = n$, hence $x_1 \notin P$. Therefore x_1 is A-regular. Put $A' = A/(x_1)$. Then A' is a C.M. local ring of dimension n-1 by Th.30, and the images of $x_2, \ldots, x_n$ in A' form a system of parameters of A'. Thus $x_2, \ldots, x_n$ is A'-regular.

i) Let $\mathrm{ht}(I) = r$. Then one can choose $a_1, \ldots, a_r \in I$ in such a way that $\mathrm{ht}\,(a_1, \ldots, a_i) = i$ holds for $1 \leq i \leq r$. Then the sequence $a_1, \ldots, a_r$ is A-regular by iii). Hence $r \leq \mathrm{grade}\, I$. Conversely if $b_1, \ldots, b_s$ is an A-regular sequence in I then $\mathrm{ht}\,(b_1, \ldots, b_s) = s \leq \mathrm{ht}\, I$. Hence $\mathrm{grade}\, I = \mathrm{ht}\, I$. Since $\mathrm{ht}\, I = \inf \{ \mathrm{ht}\, P \mid P \in V(I)\}$ and $\dim A/I = \sup \{ \dim A/P \mid P \in V(I)\}$, if $\mathrm{ht}\, P = \dim A - \dim A/P$ holds for all prime ideals P then we will have $\mathrm{ht}\, I = \dim A - \dim A/I$ in general. So let P be a prime ideal. Put $\dim A = \mathrm{depth}\, A = n$, $\mathrm{ht}\, P = r$. By Th.30 iii) A_P is a C.M. ring and $\mathrm{ht}\, P = \dim A_P = \mathrm{depth}_P(A)$. So we can find an A-regular sequence $a_1, \ldots, a_r$ in P. Then $A/(a_1, \ldots, a_r)$ is C.M. of dimension n-r, and P is a minimal prime over-ideal of $(\underline{a})$. Therefore $\dim A/P = n-r$ by Th.30 i).

ii) If $P \supset Q$ are two prime ideals of A, since A_P is C.M. we have $\dim A_P = \mathrm{ht}\, QA_P + \dim A_P/QA_P$, i.e. $\mathrm{ht}\, P - \mathrm{ht}\, Q = \mathrm{ht}(P/Q)$. Therefore A is catenary.

(16.C) We say a noetherian ring A is Cohen-Macaulay if A_P is a C.M. local ring for every prime ideal of A. By Th.30 this is equivalent to saying that A_m is a C.M. local ring for every maximal ideal m.

Let A be a noetherian ring and I an ideal; let $\mathrm{Ass}_A(A/I) = \{P_1,\dots,P_s\}$. We say that I is unmixed if $\mathrm{ht}(P_i) = \mathrm{ht}(I)$ for all i. We say that the unmixedness theorem holds in A if the following is true: if $I = (a_1,\dots,a_r)$ is an ideal of height r generated by r elements, where r is any non-negative integer, then I is unmixed. (Note that such an ideal is unmixed iff A/I has no embedded primes.) The condition implies in particular (for r = 0) that A has no embedded primes. If I is as above and if it possesses an embedded prime P, let m be a maximal ideal containing P. Then in A_m the ideal IA_m has PA_m as embedded prime. Therefore, the unmixedness theorem holds in A if it holds in A_m for all maximal ideals m.

THEOREM 32. Let A be a noetherian ring. Then A is C.M. iff the unmixedness theorem holds in A.

Proof. Suppose the unmixedness theorem holds in A. Let P be a prime ideal of height r. Then we can find $a_1,\dots,a_r \in P$ such that $\mathrm{ht}\,(a_1,\dots,a_i) = i$ for $1 \le i \le r$. The ideal $(a_1,\dots,a_i)$ is unmixed by assumption, so a_{i+1} lies in no associated primes of $A/(a_1,\dots,a_i)$. Thus $a_1,\dots,a_r$ is an A-regular sequence in P, hence $r \le \mathrm{depth}_P(A) \le \mathrm{depth}\,A_P \le \dim A_P = r$, so that A_P is a C.M. local ring.

Conversely, suppose A is C.M.. To prove the unmixedness theorem we may localize, so we assume that A is a C.M. local ring. We know that the ideal (0) is unmixed. Let $(a_1,\dots,a_r)$ be an ideal of height $r > 0$. Then $a_1,\dots,a_r$ is an A-regular sequence by Th.31, hence $A/(a_1,\dots,a_r)$ is C.M. by Th.30 and so $(a_1,\dots,a_r)$ is unmixed. Q.E.D.

(16.D) THEOREM 33. Let A be a Cohen-Macaulay ring. Then the polynomial ring $A[X_1,\dots,X_n]$ is also Cohen-Macaulay. As a consequence, any homomorphic image of a C.M. ring is universally catenary.

Proof. Enough to consider the case of n = 1. Let P be a prime ideal of B = A[X], and put $p = P \cap A$. We want to prove that the local ring B_P is C.M.. Since B_P is a localization of $A_p[X]$ and since A_p is C.M., we may assume that A is a C.M. local ring and p is the maximal ideal. Then $B/pB = k[X]$, where k is a field. Therefore we have either $P = pB$, or $P = pB + fB$ where $f = f(X) \in B$ is a monic polynomial of positive degree. As B is flat over A, so is B_P. It follows that any

A-regular sequence $a_1,\dots,a_r$ ($r = \dim A$) in p is also B_P-regular. If $P = pB$ we have $\dim B_P = \dim A$ by (13.B) Th.19, and as depth $B_P \geqslant \dim A$ we see that B_P is C.M.. If $P = pB+fB$ then $\dim B_P = \dim A + 1$ by Th.19, and since any monic polynomial is a non-zero-divisor in $A/(a_1,\dots,a_r)[X]$ we have depth $B_P \geqslant r + 1 = \dim B_P$. Thus B_P is C.M. in this case also. The last assertion is obvious.

(16.E) Example 1. A polynomial ring $k[X_1,\dots,X_n]$ over a field k is C.M. by Th.33. (Macaulay proved the unmixedness theorem for polynomial rings before 1916. Kaplansky says "In many aspects Macaulay was far ahead of his time, and some aspects of his work won full appreciation only recently".)

Example 2. Let $A = k[x,y]$ be a polynomial ring in two variables x, y over a field k, and put $B = k[x^2,xy,y^2,x^3,x^2y,xy^2,y^3]$. Then A and B have the same quotient field and A is integral over B. Put $m = (xA + yA)\cap B$. Then we have $x^4 \notin x^3B$ and $x^4 m \subseteq x^3B$, so that $m \in \mathrm{Ass}_B(B/x^3B)$. It follows that the local ring B_m is not Cohen-Macaulay.

(16.F) PROPOSITION. Let A be a C.M. ring, and $J = (a_1,\dots,a_r)$ be an ideal of height r. Then A/J^ν is C.M., and hence J^ν is unmixed, for every $\nu > 0$.

Proof. We may assume that A is local. Let k be its residue field and put $d = \dim A/J$. Since $a_1,\dots,a_r$ is an A-regular sequence, $J^\nu/J^{\nu+1}$ is isomorphic to a free A/J-module by Th. 27. Since A/J is C.M. with depth $A/J = d$, and since $\mathrm{depth}_A A/J = \mathrm{depth}_{A/J} A/J$, we have $\mathrm{Ext}^i_A(k, A/J) = 0$ $(i < d)$. Then $\mathrm{Ext}^i_A(k, J^\nu/J^{\nu+1}) = 0$ $(i < d)$ and by induction on ν we get $\mathrm{Ext}^i_A(k, A/J^\nu) = 0$ $(i < d)$. Therefore depth $A/J^\nu \geqslant d = \dim A/J^\nu$, so that A/J^ν is C.M.

EXERCISES. 1. Find an example of a noetherian local ring A and a finite A-module M such that depth M > depth A. Also find A, M and $P \in \mathrm{Spec}(A)$ such that depth $M_P > \mathrm{depth}_P(M)$.

2. Show that, if A is a noetherian local ring (or noetherian graded ring) which is a catenary domain, and if $a_1,\dots,a_r$ are elements of the maximal ideal (resp. homogeneous elements of positive degree) such that ht $(a_1,\dots,a_r) = r$, then ht $(a_1,\dots,a_i) = i$ for each $1 \leqslant i \leqslant r$. [The condition that A is a domain is necessary. In fact, if $A = k[X,Y,Z]/(X,Y)\cap(Z) = k[x,y,z]$, then ht$(x, y+z) = 2$ and ht$(x) = 0$.]

3. Let $(A,\mathfrak{m},k)$ be a local ring and $u: M \to N$ a homomorphism of finite A-modules. We say that u is minimal if $u\otimes 1_k: M\otimes k \to N\otimes k$ is an isomorphism. Show that

(i) u is minimal $\Leftrightarrow$ u is surjective and $\mathrm{Ker}(u) \subseteq \mathfrak{m}M$;

(ii) for any finite A-module M there exists a minimal homomorphism $u: F \to M$ with F free;

(iii) if $0 \to K \xrightarrow{v} F \xrightarrow{u} M \to 0$ is exact with u minimal and with K and F free, then the homomorphisms

$$v_*: \mathrm{Ext}^i_A(k, K) \to \mathrm{Ext}^i_A(k, F), \quad i = 0,1,2,\dots$$

induced by v are zero. [Hint: If $K = A^n$, $F = A^m$ and v is represented by a $n \times m$ matrix (c_{ij}), then $c_{ij} \in \mathfrak{m}$, and v_* is represented by the same matrix on $\mathrm{Ext}_A^i(k,K) \simeq \mathrm{Ext}_A^i(k,A)^n$.]

4. Let A be a noetherian local ring and M be a finite A-module having finite projective dimension. Then one has the following formula due to Auslander-Buchsbaum:

$$\text{proj.dim } M + \text{depth } M = \text{depth } A.$$

[Hint: Use induction on proj.dim M. For the case proj.dim M = 1, use the exercise 3 above.]

5. Let A be as above and let $P \in \mathrm{Spec}\, A$. Show that

i) depth $A \leqslant \mathrm{depth}_P(A) + \dim A/P$,

ii) Put codepth A = dim A − depth A. Then

$$\text{codepth } A \geqslant \text{codepth } A_P.$$

Further References.

The concept of depth has striking applications in unexpected areas:

1. R. Hartshorne: Complete intersections and connectedness. Amer. J. Math. 84 (1962), 497-508.

For instance he proves that, if A is a noeth. local ring and if $\mathrm{Spec}(A) - \{\mathfrak{m}\}$ is disconnected, then depth $A \leqslant 1$.

2. D.Buchsbaum- D.Eisenbud: What makes a complex exact ? J. of Alg. 25(1973),259-268.

They show that if $C. : 0 \to F_n \to F_{n-1} \to \ldots \to F_o$ is a complex of finite free modules over a noetherian ring, and if E_i denote the matrix of the map $F_i \to F_{i-1}$, then the exactness of C. can be fully expressed in terms of the ranks of the modules and maps and depth I_i, where I_i is the ideal generated by certain minors of the matrix E_i $(1 \leqslant i \leqslant n)$. For applications of their theorem, cf. D.Eisenbud: Some directions on recent progress in comm. algebra, in Proc.Symp.Pure Math.29 (1975).

CHAPTER 7. NORMAL RINGS and REGULAR RINGS

17. Classical Theory

(17.A) Let A be an integral domain, and K be its quotient field. We say that A is normal if it is integrally closed in K. If A is normal, so is the localization $S^{-1}A$ for every multiplicatively closed subset S of A not containing 0. Since $A = \bigcap_{\text{all max.}\mathfrak{p}} A_{\mathfrak{p}}$ by (1.H), the domain A is normal iff $A_{\mathfrak{p}}$ is normal for every maximal ideal $\mathfrak{p}$.

An element u of K is said to be almost integral over A if there exists an element a of A $(a \neq 0)$ such that $au^n \in A$ for all $n > 0$. If u and v are almost integral over A, so are $u + v$ and uv. If $u \in K$ is integral over A then it is almost integral over A. The converse is also true when A is noetherian. In fact, if $a \neq 0$ and $au^n \in A$ $(n = 1,2,\ldots)$, then A[u] is a submodule of the finite A-module $a^{-1}A$, whence A[u] itself is finite over A and u is integral over A. We say that A is completely normal if every element u of K which is almost integral over A belongs to A. For a noetherian domain normality and complete normality coincide. Valuation rings of rank (= Krull dimension) greater than one (cf. Nagata: LOCAL RINGS or Zariski-Samuel: COMM. ALG. vol.II) are normal but not completely normal.

We say (in accordance with the usage of EGA) that a ring B is <u>normal</u> if B_p is a normal domain for every prime ideal p of B. A noetherian normal ring is a direct product of a finite number of normal domains.

(17.B) PROPOSITION. (1) Let A be a completely normal domain. Then a polynomial ring $A[X_1,\dots,X_n]$ over A is also completely normal. Similarly for a formal power series ring $A[[X_1,\dots,X_n]]$. (2). Let A be a normal ring. Then $A[X_1,\dots,X_n]$ is normal.

<u>Proof</u>. (1) Enough to treat the case of $n = 1$. Let K denote the quotient field of A. Then the quotient field of A[X] is K(X). Let $u \in K(X)$ be almost integral over A[X]. Since $A[X] \subseteq K[X]$ and since K[X] is completely normal (because of unique factorization), the element u must belong to K[X]. Write $u = \alpha_r X^r + \alpha_{r+1}X^{r+1} + \dots + \alpha_d X^d$, $\alpha_r \neq 0$. Let $f(X) = b_s X^s + b_{s+1}X^{s+1} + \dots + b_t X^t \in A[X]$ be such that $fu^m \in A[X]$ for all n. Then $b_s \alpha_r^n \in A$ for all n so that $\alpha_r \in A$. Then $u - \alpha_r X^r = \alpha_{r+1}X^{r+1} + \dots$ is almost integral over A[X], so we get $\alpha_{r+1} \in A$ as before, and so on. Therefore $u \in A[X]$. The case of A[[X]] is proved similarly.

(2) Let P be a prime ideal and let $p = P \cap A$. Then $A[X]_P$ is a localization of $A_p[X]$ and A_p is a normal domain. So we may assume that A is a normal domain with quotient field K. Let $u = P(X)/Q(X)$ $(P,Q \in A[X])$ be such that $u^d + f_1(X)u^{d-1} + \dots + f_d(X) = 0$ with $f_i \in A[X]$. In order to prove that $u \in A[X]$, we consider the subring A_0 of A generated by 1 and by the coefficients of P,Q and all the $f_i(X)$'s. Then u is in the quotient field of $A_0[X]$ and is integral over $A_0[X]$. The proof of (1) shows that u is a polynomial in X: $u = \alpha_r X^r + \dots + \alpha_d X^d$, and that each coefficient α_i is almost integral over A_0. As A_0 is noetherian, α_i is integral over A_0 and a fortiori over A. Therefore $\alpha_i \in A$, as wanted.

<u>Remark</u>. There exists a normal ring A such that A[[X]] is not normal (A.Seidenberg).

(17.C) Let A be a ring and I an ideal with $\bigcap_{n=1}^{\infty} I^n = (0)$. Then for each non-zero element a of A there is an integer $n \geqslant 0$ such that $a \in I^n$ and $a \notin I^{n+1}$. We then write $n = \mathrm{ord}(a)$

(or $\mathrm{ord}_I(a)$) and call it the order of a (with respect to I). We have $\mathrm{ord}(a + b) \geq \min(\mathrm{ord}(a), \mathrm{ord}(b))$ and $\mathrm{ord}(ab) \geq \mathrm{ord}(a) + \mathrm{ord}(b)$.

Put $A' = \mathrm{gr}^I(A) = \bigoplus_{n \geq 0} I^n/I^{n+1}$. For an element a of A with $\mathrm{ord}(a) = n$, we call the image of a in $I^n/I^{n+1} = A'_n$ the leading form of a and denote it by a^*. We define $0^* = 0$ ($\varepsilon A'$). The map $a \mapsto a^*$ is in general neither additive nor multiplicative, but if $a^*b^* \neq 0$ (i.e. if $\mathrm{ord}(ab) = \mathrm{ord}(a) + \mathrm{ord}(b)$) then we have $(ab)^* = a^*b^*$, and if $\mathrm{ord}(a) = \mathrm{ord}(b)$ and $a^* + b^* \neq 0$ then we have $(a + b)^* = a^* + b^*$. It follows that, for any ideal Q of A, the set Q^* of the leading forms of the elements of Q is a graded ideal of A'. Warning: if $Q = \Sigma a_i A$ it does not necessarily follow that $Q^* = \Sigma a_i^* A'$. But if Q is a principal ideal aA and if A' is a domain, then we have $Q^* = a^*A'$.

Put $\bar{A} = A/Q$ and $\bar{I} = (I + Q)/Q$. Then it holds that $\mathrm{gr}^{\bar{I}}(\bar{A}) \simeq \mathrm{gr}^I(A)/Q^*$. In fact, we have $\bar{I}^n/\bar{I}^{n+1} = (I^n + Q)/(I^{n+1} + Q) \simeq I^n/I^n \cap (I^{n+1} + Q) = I^n/(I^n \cap Q) + I^{n+1} = A'_n/Q^*_n$.

(17.D) THEOREM 34 (Krull). Let A, I and A' be as above. Then 1) if A' is a domain, so is A;

2) suppose that A is noetherian and that $I \subseteq \mathrm{rad}(A)$, then, if A' is a normal domain, so is A.

Proof. 1) Let a and b be non-zero-elements of A. Then $a^* \neq 0$ and $b^* \neq 0$, hence $(ab)^* = a^*b^* \neq 0$ and so $ab \neq 0$.

2) The ring A is a domain by 1). Let $a, b \in A$, $b \neq 0$, and suppose that a/b is integral over A. We have to prove $a \in bA$. The A-module A/bA is separated in the I-adic topology by (11.D) Cor.1, in other words $bA = \bigcap_{n=1}^{\infty} (bA + I^n)$. Therefore it suffices to prove that $a \in bA + I^n$ for all n. Suppose that $a \in bA + I^{n-1}$ is already proved. Then $a = br + a'$ with $r \in A$ and $a' \in I^{n-1}$, and $a'/b = a/b - r$ is integral over A. So we can replace a by a' and assume that $a \in I^{n-1}$. We are to prove $a \in bA + I^n$. Since a/b is almost integral over A there exists $0 \neq c \in A$ such that $ca^m \in b^mA$ for all m. As A' is a domain the map $a \mapsto a^*$ is multiplicative, hence we have $c^*a^{*m} \in b^{*m}A'$ for all m, and since A' is noetherian (by (10.D)) and normal we have $a^* \in b^*A'$. Let $c \in A$ be such that $a^* = b^*c^*$. Then $n - 1 < \mathrm{ord}(a) < \mathrm{ord}(a - bc)$, whence $a - bc \in I^n$ so that $a \in bA + I^n$. Q.E.D.

Remark. Even when A is a normal domain it can happen that A' is not a domain. Example: $A = k[x,y,z] = k[X,Y,Z]/(Z^2 - X^2 - Y^3)$, where k is a field of characteristic $\neq 2$, and $I = (x,y,z)$. We have $A' = \mathrm{gr}^I(A) \simeq k[X,Y,Z]/(Z^2 - X^2)$, so $(x^* - z^*)(x^* + z^*) = 0$. On the other hand A is normal. In general, a ring of the form $k[X_1,\ldots,X_n,Z]/(Z^2 - f(X))$ is normal provided that f(X) is square-free.

(17.E) Let $(A, \mathfrak{m}, k)$ be a noetherian local ring of dimension d. Recall that the ring A is said to be regular if $\mathfrak{m}$ is generated by d elements, or what amounts to the same, if $d = \mathrm{rank}_k \mathfrak{m}/\mathfrak{m}^2$ (cf. (12.J)). A regular local ring of dimension 0 is nothing but a field. The formal power series ring $k[[X_1,\dots,X_d]]$ over a field k is a typical example of regular local ring.

THEOREM 35. Let $(A, \mathfrak{m}, k)$ be a noetherian local ring. Then A is regular iff the graded ring $gr(A) = \bigoplus \mathfrak{m}^n/\mathfrak{m}^{n+1}$ associated to the $\mathfrak{m}$-adic filtration is isomorphic (as a graded k-algebra) to a polynomial ring $k[X_1,\dots,X_d]$.

Proof. Suppose A is regular, and let $\{x_1,\dots,x_d\}$ be a regular system of parameters. Then $gr(A) = k[x_1^*,\dots,x_d^*]$, hence gr(A) is of the form $k[X_1,\dots,X_d]/I$ where I is a graded ideal. If I contains a homogeneous polynomial $F(X) \neq 0$ of degree n_0 then we would have, for $n > n_0$,

$$\ell(A/\mathfrak{m}^{n+1}) \leq \binom{n+d}{d} - \binom{n-n_0+d}{d} = \text{a polynomial of degree } d-1 \text{ in } n.$$

But the Hilbert function $\ell(A/\mathfrak{m}^n)$ of A is a polynomial in n (for large n) of degree d by (12.H). Therefore the ideal I must be (0).

Conversely, suppose $gr(A) \simeq k[X_1,\dots,X_d]$. Then we get $\dim A = d$ from the consideration of the Hilbert polynomial, while $\mathrm{rank}_k \mathfrak{m}/\mathfrak{m}^2 = \mathrm{rank}_k(kX_1 + \dots + kX_d) = d$. Thus A is regular.

(17.F) THEOREM 36. Let A be a regular local ring and $\{x_1,\dots,x_d\}$ a regular system of parameters. Then:

1) A is a normal domain;

2) $x_1,\dots,x_d$ is an A-regular sequence, and hence A is a Cohen-Macaulay local ring;

3) $(x_1,\dots,x_i) = \mathfrak{p}_i$ is a prime ideal of height i for each $1 \leq i \leq d$, and $A/\mathfrak{p}_i$ is a regular local ring of diemnsion $d - i$;

4) conversely, if $\mathfrak{p}$ is an ideal of A and if $A/\mathfrak{p}$ is regular and has dimension $d - i$, then there exists a regular system of parameters $\{y_1,\dots,y_d\}$ such that $\mathfrak{p} = (y_1,\dots,y_i)$.

Proof. 1) follows from Th.34 and Th.35.

2) follows from Th.27 as well as from 3) below.

3) We have $\dim(A/\mathfrak{p}_i) = d - i$ by (12.K), while the maximal ideal $\mathfrak{m}/\mathfrak{p}_i$ of $A/\mathfrak{p}_i$ is generated by $d - i$ elements $\bar{x}_{i+1},\dots,\bar{x}_d$. Therefore $A/\mathfrak{p}_i$ is regular, and hence $\mathfrak{p}_i$ is a prime by 1).

4) Put $\bar{\mathfrak{m}} = \mathfrak{m}/\mathfrak{p}$. Then $d - i = \mathrm{rank}_k \bar{\mathfrak{m}}/\bar{\mathfrak{m}}^2 =$

$\operatorname{rank}_k \mathfrak{m}/(\mathfrak{m}^2 + \mathfrak{p}) = \operatorname{rank}_k \mathfrak{m}/\mathfrak{m}^2 - \operatorname{rank}_k(\mathfrak{m}^2 + \mathfrak{p})/\mathfrak{m}^2$, hence $i = \operatorname{rank}_k(\mathfrak{m}^2 + \mathfrak{p})/\mathfrak{m}^2$. Thus we can choose i elements $y_1, \ldots, y_i$ of $\mathfrak{p}$ which span $\mathfrak{p} + \mathfrak{m}^2$ mod $\mathfrak{m}^2$ over k, and d - i elements $y_{i+1}, \ldots, y_d$ of $\mathfrak{m}$ which, together with $y_1, \ldots, y_i$, span $\mathfrak{m}$ mod $\mathfrak{m}^2$ over k. Then $\{y_1, \ldots, y_d\}$ is a regular system of parameters of A, so that $(y_1, \ldots, y_i) = \mathfrak{p}'$ is a prime ideal of height i by 3). As $\mathfrak{p} \supseteq \mathfrak{p}'$ and $\dim(A/\mathfrak{p}) = d - i$, we must have $\mathfrak{p} = \mathfrak{p}'$. Q.E.D.

(17.G) Let A be a regular local ring of dimension 1, and let P = aA be the maximal ideal of A. Then the non-zero ideals of A are the powers $P^n = a^nA$ $(n \geqslant 0)$ of P. (Proof: if I is an ideal and $I \neq 0$, then there exists $n \geqslant 0$ such that $I \subseteq P^n = a^nA$ and $I \not\subseteq P^{n+1}$. Then $a^{-n}I$ is an ideal of A not contained in the maximal ideal P, therefore $a^{-n}I = A$, i.e. $I = a^nA$, as claimed.) Thus A is a principal ideal domain. Furthermore, any fractional ideal (that is, finitely generated non-zero A-submodule of the quotient field K of A) is equal to some a^nA $(n \gtreqless 0)$. If $0 \neq x \in K$ and $xA = a^nA$, then we write $n = \operatorname{ord}(x)$. Then $x \longmapsto \operatorname{ord}(x)$ is a valuation of K with $\mathbb{Z}$ as the value group, and A is the ring of the valuation. Conversely, let v be a valuation of K whose value group is discrete and of rank 1 (i.e. isomorphic to $\mathbb{Z}$); then the valuation ring R_v of v is called a principal valuation ring or a discrete valuation ring of rank 1, and is a regular local ring of dimension 1. Thus a principal valuation ring and a one-dimensional regular local ring are the same theing. On the contrary, no other kinds of valuation rings are noetherian.

In the next paragraph we shall learn another characterization (Th. 37) of the one-dimensional regular local rings.

(17.H) Let A be a noetherian domain with quotient field K. For any non-zero ideal I of A we put $I^{-1} = \{x \in K \mid xI \subseteq A\}$. We have $A \subseteq I^{-1}$ and $I \cdot I^{-1} \subseteq A$.

LEMMA 1. Let $0 \neq a \in A$ and $P \in \operatorname{Ass}_A(A/aA)$. Then $P^{-1} \neq A$.

<u>Proof</u>. By the definition of the associated primes there exists $b \in A$ such that $(aA : b) = P$. Then $(b/a)P \subseteq A$ and $b/a \notin A$.

LEMMA 2. Let (A, P) be a noetherian local domain such that $P \neq 0$ and $PP^{-1} = A$. Then P is a principal ideal, and so A is regular of dimension 1.

<u>Proof</u>. Since $\bigcap_{n=1}^{\infty} P^n = (0)$ by (11.D) Cor.3, we have $P \neq P^2$. Take $a \in P - P^2$. Then $aP^{-1} \subseteq A$, and if $aP^{-1} \subseteq P$ then $aA = aP^{-1}P \subseteq P^2$, contradicting the choice of a. Therefore we must have $aP^{-1} = A$, that is, $aA = aP^{-1}P = P$.

THEOREM 37. Let (A, P) be a noetherian local ring of dimension 1. Then A is regular iff it is normal.

Proof. Suppose A is normal (hence a domain). By Lemma 2 it suffices to show $PP^{-1} = A$. Assume the contrary. Then $PP^{-1} = P$, and hence $P(P^{-1})^n = P \subseteq A$ for any $n > 0$. Therefore all the elements of P^{-1} are integral over A, whence $P^{-1} = A$ by the normality. But, as dim A = 1, we have $P \in \mathrm{Ass}(A/aA)$ for any non-zero element a of P so that $P^{-1} \neq A$ by Lemma 1. Thus $PP^{-1} = P$ cannot occur. Q.E.D.

THEOREM 38. Let A be a noetherian normal domain. Then any non-zero principal ideal is unmixed, and it holds that $A = \bigcap_{ht(p)=1} A_p$. If $\dim A \leq 2$ then A is Cohen-Macaulay.

Proof. Let $a \neq 0$ be a non-unit of A and let $P \in \mathrm{Ass}(A/aA)$. Replacing A by A_P we may suppose that (A,P) is local. Then we have $P^{-1} \neq A$ by Lemma 1, and if ht(P) > 1 we would have a contradiction as in the preceding proof. Thus ht(P) = 1. This implies that aA is unmixed. The other assertions of the theorem follow immediately from that.

(17.I) Let A be a noetherian ring. Consider the following conditions about A for k = 0,1,2,... :

(S_k) it holds $\mathrm{depth}(A_p) \geq \inf(k, \mathrm{ht}(p))$ for all $p \in \mathrm{Spec}(A)$, and

(R_k) if $p \in \mathrm{Spec}(A)$ and $\mathrm{ht}(p) \leq k$, then A_p is regular.

The condition (S_0) is trivial. The condition (S_1) holds iff Ass(A) has no embedded primes. The condition (S_2), which is probably the most important, is equivalent to that not only Ass(A) but also Ass(A/fA) for every non-zero-divisor f of A have no embedded primes. The ring A is C.M. iff it satisfies all (S_k).

If (R_0) and (S_1) are satisfied then A is reduced, and conversely. The following theorem is due to Krull(1931) in the case A is a domain, and to Serre in the general case.

THEOREM 39. (Criterion of normality) A noetherian ring is normal iff it satisfies (S_2) and (R_1).

Proof. (After EGA IV_2 p.108). Let A be a noetherian ring. Suppose first that A is normal, and let p be a prime ideal. Then A_p is a field for $ht(p) = 0$, and regular for $ht(p) = 1$ by Th.37, hence the condition (R_1). Since a normal local ring is a domain, Th.38 implies that A satisfies (S_2).

Next suppose that A satisfies (S_2) and (R_1). Then A is reduced. Let $p_1,\ldots,p_r$ be the minimal prime ideals of A. Thus we have $(0) = p_1 \cap \ldots \cap p_r$. The total quotient ring ΦA

(cf. p.12) of A is isomorphic to the direct product $K_1 \times \dots \times K_r$, where K_i is the quotient field of A/p_i; this follows from (1.C) applied to ΦA.

We shall prove that A is integrally closed in ΦA. Suppose this is done; then the unit element e_i of K_i belongs to A since $e_i^2 - e_i = 0$, and we have $1 = e_1 + \dots + e_r$ and $e_i e_j = 0$ $(i \neq j)$. Therefore $A = Ae_1 \times \dots \times Ae_r$, and Ae_i is a normal domain as it is integrally closed in K_i; thus A is a normal ring. So suppose

$$(a/b)^n + c_1(a/b)^{n-1} + \dots + c_n = 0 \quad \text{in } \Phi A,$$

where a, b and the c_i's are elements of A and b is A-regular. This is equivalent to $a^n + \Sigma c_i a^{n-i} b^i = 0$. We want to prove $a \in bA$. Since bA is unmixed of height 1 by (S_2), we have only to show that $a_p \in b_p A_p$ for all prime ideals p of height 1 (where a_p and b_p are the canonical images of a and b in A_p). But A_p is normal by (R_1) for such p, and we have $a_p^n + \Sigma(c_i)_p a_p^{n-i} b_p^i = 0$, therefore $a_p \in b_p A_p$. Q.E.D.

(17.J) THEOREM 40. Let A be a ring such that for every prime ideal p the localization A_p is regular. Then the polynomial ring $A[X_1, \dots, X_n]$ over A has the same property.

<u>Proof</u>. As in the proof of (16.D) Th.33, we are led to the following situation: (A, p) is a regular local ring, n = 1 and P is a prime ideal of B = A[X] lying over p. And we have to prove B_P is regular. In this circumstance we have $P \supseteq pB$ and $B/pB = k[X]$, where $k = A/p$ is a field. Therefore either $P = pB$, or $P = pB + f(X)B$ with a monic polynomial f(X) in B. Put d = dim A. Then p is generated by d elements, so P is generated by d elements over B if $P = pB$, and by d+1 elements if $P = pB + fB$. On the other hand it is clear that $ht(pB) \geqslant d$, so we have ht(P) = d in the former case and ht(P) = d + 1 in the latter case by (12.I) Th.18. Therefore B_P is regular. Q.E.D.

In particular, all local rings of a polynomial ring $k[X_1, \dots, X_n]$ over a field are regular.

18. Homological Theory

(18.A) Let A be a ring. The projective (resp. injective) dimension of an A-module M is the length of a shortest projective (resp. injective) resolution of M.

LEMMA 1. (i) An A-module M is projective iff $\mathrm{Ext}^1_A(M, N) = 0$ for all A-modules N.

(ii) M is injective iff $\mathrm{Ext}^1_A(A/I, M) = 0$ for all ideals I of A.

<u>Proof</u>. Immediate from the definitions. In (ii) we use the

fact (which is proved by Zorn's lemma) that if any homomorphism $f: N \to M$ can be extended to any A-module N' containing N such that $N' = N + A\xi$ for some $\xi \in N'$, then M is injective.

LEMMA 2. Let A be a ring and n be a non-negative integer. Then the following conditions are equivalent:

(1) proj.dim $M \leq n$ for all A-modules M,

(2) proj.dim $M \leq n$ for all finite A-modules M,

(3) inj. dim $M \leq n$ for all A-modules M,

(4) $\mathrm{Ext}_A^{n+1}(M, N) = 0$ for all A-modules M and N.

Proof. (1) $\Rightarrow$ (2): trivial. (2) $\Rightarrow$ (3): take an exact sequence $0 \to M \to U_0 \to U_1 \to \dots \to U_{n-1} \to C \to 0$ with U_j injective for all j. Let I be any ideal. Then we have $\mathrm{Ext}_A^1(A/I, C) \simeq \mathrm{Ext}_A^{n+1}(A/I, M)$, which is zero by (2) since A/I is a finite A-module. (4) $\Rightarrow$ (1) is proved similarly, with "projective" instead of "injective" and with the arrows reversed. (3) $\Rightarrow$ (4) is trivial, as one can calculate $\mathrm{Ext}_A^*(M, N)$ using an injective resolution of N.

By virtue of Lemma 2 we have

$$\sup_M \,(\text{proj. dim } M) = \sup_M \,(\text{inj. dim } M).$$

We call this common value (which may be ∞) the global dimension of A and denote it by gl. dim A. (In EGA it is denoted by dim. coh(A).)

(18.B) LEMMA 3. Let A be a noetherian ring and M a finite A-module. Then M is projective iff $\mathrm{Ext}_A^1(M,N) = 0$ for all finite A-modules N.

Proof. Take a resolution $0 \to R \overset{i}{\to} F \to M \to 0$ with F finite and free. Then R is also finite, hence we have $\mathrm{Ext}^1(M,R) = 0$. Thus $\mathrm{Hom}(F,R) \to \mathrm{Hom}(R,R) \to 0$ is exact, and so there exists $s: F \to R$ with $s \circ i = id_R$, i.e. the sequence $0 \to R \to F \to M \to 0$ splits. Then M is a direct summand of a free module.

LEMMA 4. Let $(A, \mathfrak{m}, k)$ be a noetherian local ring, and M be a finite A-module. Then

$$\text{proj. dim } M \leq n \iff \mathrm{Tor}_{n+1}^A(M, k) = 0.$$

Proof. ($\Rightarrow$) Trivial. ($\Leftarrow$) The general case is easily reduced to the case n = 0. If $\mathrm{Tor}_1(M, K) = 0$, let $0 \to R \to F \overset{u}{\to} M \to 0$ be exact with u minimal (cf. p.113 Ex.3). Then $0 \to R\otimes k \to F\otimes k \overset{\bar{u}}{\to} M\otimes k \to 0$ is exact and $\bar{u}$ is an isomorphism, hence $R\otimes k = 0$ and so $R = 0$ by NAK. Therefore M is free, as wanted.

LEMMA 5. (I) Let A be a noetherian ring and M a finite A-module. Then (i) proj. dim M is equal to the supremum of proj. dim M_p (as A_p-module) for the maximal ideals p of A, and (ii) we have proj. dim $M \leqq n$ iff $\mathrm{Tor}^A_{n+1}(M, A/p) = 0$ for all maximal ideals p of A.

(II) The following conditions about a noetherian ring A are equivalent:

(1) gl. dim $A \leqslant n$,

(2) proj. dim $M \leqslant n$ for all finite A-modules M,

(3) inj. dim $M \leqslant n$ for all finite A-modules M,

(4) $\mathrm{Ext}^{n+1}_A(M, N) = 0$ for all finite A-modules M and N,

(5) $\mathrm{Tor}^A_{n+1}(M, N) = 0$ for all finite A-modules M and N.

(III) For any noetherian ring A, we have

$$\mathrm{gl.dim}\, A = \sup_{\max. p} \mathrm{gl.dim}(A_p).$$

Proof. (I) The assertion (i) follows from (3.E) and Lemma 2, while (ii) follows from (i) and Lemma 4.

(II) We already saw (2)$\Leftrightarrow$(1)$\Rightarrow$(3) in Lemma 2, and (3)$\Rightarrow$(4) and (2)$\Rightarrow$(5) are trivial. Moreover, (5) implies (2) by (I) above, and (4)$\Rightarrow$(2) is easy to see by Lemma 3.

(III) follows from (I) and (II).

THEOREM 41. Let $(A, \mathfrak{m}, k)$ be a noetherian local ring. Then gl.dim $A \leqslant n \Leftrightarrow \mathrm{Tor}^A_{n+1}(k,k) = 0$. Consequently, we have gl.dim A = proj.dim k (as A-module).

Proof. $\mathrm{Tor}_{n+1}(k,k) = 0 \Rightarrow$ proj.dim $k \leqslant n \Rightarrow \mathrm{Tor}_{n+1}(M,k) = 0$ for all M $\Rightarrow$ proj.dim $M \leqslant n$ for all finite M $\Rightarrow$ gl.dim $A \leqslant n$.

(18.C) LEMMA 6. Let $(A, \mathfrak{m}, k)$ be a noetherian local ring and M a finite A-module. If proj.dim $M = r < \infty$ and if x is an M-regular element in $\mathfrak{m}$, then proj.dim$(M/xM) = r + 1$.

Proof. The sequence $0 \to M \xrightarrow{x} M \to M/xM \to 0$ is exact by assumption, therefore the sequences

$$0 \to \mathrm{Tor}_i(M/xM, k) \to 0 \qquad (i > r + 1)$$

and $\mathrm{Tor}_{r+1}(M,k) = 0 \to \mathrm{Tor}_{r+1}(M/xM,k) \to \mathrm{Tor}_r(M,k) \xrightarrow{x} \mathrm{Tor}_r(M,k)$ are also exact. Since $k = A/\mathfrak{m}$ is annihilated by x, the A-module $\mathrm{Tor}_r(M,k)$ is also annihilated by x. Therefore $\mathrm{Tor}_{r+1}(M/xM, k) \simeq \mathrm{Tor}_r(M,k) \neq 0$ and $\mathrm{Tor}_i(M/xM, k) = 0$ for $i > r+1$. In view of Lemma 5 we then have proj.dim $M/xM = r+1$.

THEOREM 42. Let $(A, \mathfrak{m}, k)$ be a regular local ring of dimension n. Then gl.dim A = n.

Proof. Let $\{x_1,\ldots,x_n\}$ be a regular system of parameters. Then the sequence $x_1,\ldots,x_n$ is A-regular and $k = A/\Sigma x_i A$, hence we have proj.dim k = n by Lemma 6. So the theorem follows from Th.41.

COROLLARY. (Hilbert's Syzygy Theorem) Let $A = k[X_1,\dots,X_n]$ be a polynomial ring over a field k. Then gl.dim A = n.

Proof. This follows from Th.22, Th.40, Th.42 and Lemma 5.

We are going to prove a converse (due to Serre) of Th.42, namely that a noetherian local ring of finite global dimension is regular (Th.45). This is more important than Th.42, and its proof is also more difficult. Roughly speaking there are two different proofs: one is due to Nagata (simplified by Grothendieck) and uses induction on dim A. This proof is shorter and does not require big tools (cf. EGA IV_1 pp.46-48). The other is due to Serre and uses Koszul complex and minimal resolution; it has the merit of giving more information about the homology groups $Tor_i(k,k)$. Here we shall follow Serre's proof. We begin with explaining the necessary homological techniques, which are useful in other situations also.

(18.D) Koszul Complex. Let A be a ring. A complex (or more precisely, a chain complex) M. is a sequence

$$M. : \quad \dots \to M_n \xrightarrow{d} M_{n-1} \xrightarrow{d} \dots \xrightarrow{d} M_0 \xrightarrow{d} 0$$

of A-modules and A-linear maps such that $d^2 = 0$. The module M_i is called the i-dimensional part of the complex and the map d is called the differentiation. If L. and M. are two complexes, their tensor product $L.\otimes M.$ is, by definition, the

complex such that $(L.\otimes M.)_n = \bigoplus_{p+q=n} L_p \otimes_A M_q$ and such that $d: (L.\otimes M.)_n \to (L.\otimes M.)_{n-1}$ is defined on $L_p \otimes M_q$ by the formula $d(x\otimes y) = d_L(x)\otimes y + (-1)^p x\otimes d_M(y)$.

Let $x_1, \dots, x_n \in A$, and let Ae_i be a free A-module of rank one with a specified basis e_i for $i = 1,\dots,n$. Let $K.(x_i)\colon\ 0 \to Ae_i \xrightarrow{x_i} A \to 0$ denote the complex defined by $K_p(x_i) = 0$ $(p \neq 1,0)$, $= Ae_i$ $(p = 1)$ and $= A$ $(p = 0)$, and by $d(e_i) = x_i$. Then $H_0(K.(x_i)) = A/x_iA$ and $H_1(K.(x_i)) \simeq \mathrm{Ann}(x_i)$. For any complex C., we put $C.(x_1,\dots,x_n) = C.\otimes K.(x_1)\otimes\dots\otimes K.(x_n)$. If M is an A-module we view it as a complex M. with $M_n = 0$ $(n \neq 0)$ and $M_0 = M$, and we put $K.(x_1,\dots,x_n, M) = M.\otimes K.(x_1)\otimes\dots\otimes K.(x_n)$. If there is no danger of confusion we denote them by $C.(\underline{x})$ and by $K.(\underline{x}, M)$ respectively. These complexes are called Koszul complexes. We have $K_p(x_1,\dots,x_n, M) = 0$ for $n < p$, while

$$K_p(x_1,\dots,x_n, M) = \bigoplus_{\substack{p \text{ of the } \alpha_i\text{'s are } = 1 \\ \text{and the rest are } = 0}} M\otimes [K_{\alpha_1}(x_1)\otimes\dots\otimes K_{\alpha_n}(x_n)]$$

for $0 \leqslant p \leqslant n$. Put $e_{i_1\dots i_p} = u_1\otimes\dots\otimes u_n$, where $u_i = e_i$ for $i \in \{i_1,\dots,i_p\}$ and $u_i = 1$ for other i. Then

$$K_0(x_1,\dots,x_n, M) = M,$$

$$K_p(x_1,\dots,x_n, M) = \bigoplus_{1\leqslant i_1<\dots<i_p\leqslant n} M e_{i_1\dots i_p} \simeq M^{\binom{n}{p}} \quad (1 \leqslant p \leqslant n),$$

and

(1) $$d(me_{i_1 \ldots i_p}) = \sum_{r=1}^{p} (-1)^{r-1} x_{i_r} m\, e_{i_1 \ldots \hat{i}_r \ldots i_p}$$

(where $m \in M$, and $\hat{i}_r$ indicates that i_r is omitted there). The formula (1) for the operator d can be put into another form: let $\sum_{i_1 < \ldots < i_p} m_{i_1 \ldots i_p} e_{i_1 \ldots i_p}$ be an arbitrary element of $K_p(\underline{x}, M)$, and extend the $m_{i_1 \ldots i_p}$'s to an alternating function of the indices (i.e. such that $m_{\ldots i \ldots i \ldots} = 0$ and $m_{\ldots i \ldots j \ldots} = - m_{\ldots j \ldots i \ldots}$). Then we have

(2) $$d\Big(\sum_{i_1 < \ldots < i_p} m_{i_1 \ldots i_p} e_{i_1 \ldots i_p}\Big) = \sum_{j=1}^{n} x_j \Big(\sum_{i_1 < \ldots < i_{p-1}} m_{j i_1 \ldots i_{p-1}} e_{i_1 \ldots i_{p-1}}\Big).$$

There is another interpretation of the Koszul complex. Let $F = AX_1 + \ldots + AX_n$ be a free A-module of rank n with a basis $\{X_1, \ldots, X_n\}$. Then the exterior product $\bigwedge^p F$ is a free module of rank $\binom{n}{p}$ with $\{X_{i_1} \wedge \ldots \wedge X_{i_p} \mid 1 \leq i_1 < \ldots < i_p \leq n\}$ as a basis, so that there is an isomorphism of A-modules $M \otimes_A \bigwedge^p F \to K_p(\underline{x}, M)$ which maps $X_{i_1} \wedge \ldots \wedge X_{i_p}$ to $e_{i_1 \ldots i_p}$. Thus we can define $K.(\underline{x}, M)$ to be the complex $M \otimes L.$ with $L_p = \bigwedge^p F$ and with $d(X_{i_1} \wedge \ldots \wedge X_{i_p}) = \sum_{r=1}^{p} (-1)^{r-1} x_{i_r} X_{i_1} \wedge \ldots \wedge \hat{X}_{i_r} \wedge \ldots \wedge X_{i_p}$. If we adopt this definition then we have to check $d^2 = 0$ on $L.$, which is straightforward anyway.

For any $x \in A$, we have an exact sequence of complexes

(3) $$0 \to A \to K.(x) \to A' \to 0$$

where A' is the factor complex $K.(x)/A$, therefore $(A')_1 \simeq A$ and $(A')_n = 0$ for $n \neq 1$. Let $C.$ be any complex. Then tensoring the exact sequence (3) with $C.$ we get

(4) $$0 \to C. \to C.(x) \to C'. \to 0 \qquad (C'. = C. \otimes A'),$$

which is again exact. The complex C' is obtained from C by increasing the dimension by one: $C'_p = C_{p-1}$ and $d'_p = d_{p-1}$. Thus $H_p(C') \to H_{p-1}(C)$, and we get a long exact sequence

$$\ldots \to H_{p+1}(C.) \to H_{p+1}(C.(x)) \to H_p(C.) \xrightarrow{\delta_p} H_p(C.) \to$$
$$\ldots \xrightarrow{\delta_1} H_1(C.) \to H_1(C.(x)) \to H_0(C.) \xrightarrow{\delta_0} H_0(C.) \to H_0(C.(x)) \to 0.$$

One immediately checks that the connecting homomorphism δ_p is the multiplication by $(-1)^p x$. Therefore we get

LEMMA 7. If $C.$ is a complex with $H_p(C.) = 0$ for all $p > 0$, then $H_p(C.(x)) = 0$ for all $p > 1$ and

$$0 \to H_1(C.(x)) \to H_0(C.) \xrightarrow{x} H_0(C.) \to H_0(C.(x)) \to 0$$

is exact. If, in particular, x is $H_0(C.)$-regular, then we have $H_p(C.(x)) = 0$ for all $p > 0$ and $H_0(C.(x)) = H_0(C)/xH_0(C)$.

THEOREM 43. Let A be a ring, M an A-module and $x_1, \ldots, x_n$ an M-regular sequence in A. Then we have

$$H_p(K.(\underline{x}, M)) = 0 \quad (p > 0), \quad H_0(K.(\underline{x}, M)) = M/\sum_{1}^{n} x_i M.$$

COROLLARY. Let A be a ring and $x_1,\dots,x_n$ be an A-regular sequence in A. Then $K.(x_1,\dots,x_n, A)$ is a free resolution of the A-module $A/(x_1,\dots,x_n)$.

(18.E) Minimal Resolution. Let $(A,\mathfrak{m},k)$ be a noetherian local ring. We recall (p.113 Ex.3) that a homomorphism u: $L \to M$ is called minimal if $\bar{u} = u\otimes \mathrm{id}_k : \bar{L} = L\otimes k \to \bar{M} = M\otimes k$ is an isomorphism, or equivalently, if u is surjective with $\mathrm{Ker}(u) \subseteq \mathfrak{m}L$. Let M be a finite A-module. A free resolution of M, $\dots \to L_i \xrightarrow{d_i} L_{i-1} \to \dots \xrightarrow{d_1} L_0 \xrightarrow{d_0} M \to 0$, is called a minimal resolution if $d_i\colon L_i \to \mathrm{Ker}(d_{i-1})$ is minimal for each $i \geq 0$. In this case the complex

$$L.\otimes k: \quad \dots \to \bar{L}_i \xrightarrow{\bar{d}_i} \bar{L}_{i-1} \to \dots \xrightarrow{\bar{d}_1} \bar{L}_0 ,$$

where $\bar{L}_i = L_i\otimes k = L_i/\mathfrak{m}L_i$, has trivial differentiation (i.e. all $\bar{d}_i = 0$). Therefore we have $\mathrm{Tor}_i^A(M,k) \simeq \bar{L}_i$ for all i, and so $\mathrm{rank}\, L_i = \mathrm{rank}_k \mathrm{Tor}_i^A(M,k)$. In particular, all L_i are finite over A.

LEMMA 8. Let M be a finite module over a noetherian local ring A. Then a minimal resolution of M exists, and is unique up to (non-canonical) isomorphisms.

Proof. The existence is easy to see: one constructs a minimal resolution step by step, using minimal basis. To prove the uniqueness, let $L. \to M$ and $L'. \to M$ be two minimal resolutions of M. Since L. is a projective resolution there exists a homomorphism $f\colon L. \to L'.$ of complexes over M. Since

$$\begin{array}{ccccc} L_1 & \xrightarrow{d_1} & L_0 & \xrightarrow{\varepsilon} & M \\ \downarrow f_1 & & \downarrow f_0 & & \downarrow \mathrm{id} \\ L'_1 & \longrightarrow & L'_0 & \xrightarrow{\varepsilon'} & M \end{array}$$

is commutative and since ε and ε' are minimal, the map $\bar{f}_0$ is an isomorphism. Since both L_0 and L'_0 are free, the map f_0 is then defined by a square matrix T with $\det T \notin \mathfrak{m}$. Then f_0 itself is an isomorphism. Repeating the same reasoning we prove inductively that all f_i are isomorphisms.

Exercise. Let $L. \to M$ be a minimal resolution and $P. \to M$ be an arbitrary free resolution. Then we have $P. \simeq L. \oplus W.$ with some acyclic complex W..

LEMMA 9. Let $\to L_i \xrightarrow{d_i} L_{i-1} \to \dots \xrightarrow{d_1} L_0 \xrightarrow{\varepsilon} M \to 0$ be a minimal resolution of M, and

$$\to F_i \xrightarrow{d'_i} F_{i-1} \to \dots \xrightarrow{d'_1} F_0$$

be a complex with an augmentation $\varepsilon'\colon F_0 \to M$, such that

i) each F_i is finite and free over A,

ii) $\bar{\varepsilon}'\colon \bar{F}_0 \to \bar{M}$ is injective, and

iii) $d'_i(F_i) \subseteq \mathfrak{m}F_{i-1}$ for each $i > 0$, and d'_i induces an injection $\bar{F}_i \to (\mathfrak{m}/\mathfrak{m}^2)\otimes F_{i-1}$.

Then there exists a homomorphism of complexes over M

$$f: F. \to L.$$

such that each f_i maps F_i isomorphically onto a direct summand of L_i. Consequently, we have

$$\text{rank } F_i \leqq \text{rank } L_i = \text{rank}_k \text{ Tor}_i^A(M,k).$$

Proof. Since L. is a resolution and since each F_i is free, there exists a homomorphism f: F. → L. over M. We have to prove that, for each i, there exists an A-linear map $g_i: L_i \to F$ with $g_i f_i = id_{F_i}$. Since both F_i and L_i are free, we can easily see that such g_i exists iff $\overline{f}_i: \overline{F}_i \to \overline{L}_i$ is injective. Using the assumptions we prove inductively that $\overline{f}_i$ is injective, for i = 0,1,2,... .

(18.F) THEOREM 44. Let $(A,\mathfrak{m},k)$ be a noetherian local ring and let $s = \text{rank}_k\, \mathfrak{m}/\mathfrak{m}^2$. Then we have

$$\text{rank}_k \text{ Tor}_i^A(k,k) \geqq \binom{s}{i} \quad \text{for } 0 \leqq i \leqq s.$$

Proof. Take a minimal basis $\{x_1,\dots,x_s\}$ of $\mathfrak{m}$, and consider the Koszul complex $F. = K.(x_1,\dots,x_s,A)$. There is an obvious augmentation $F_0 = A \to k = A/\mathfrak{m}$, which satisfies the condition ii) of Lemma 9. By the definition of $d_p: F_p \to F_{p-1}$ it is clear that $d_p(F_p) \subseteq \mathfrak{m}F_{p-1}$. Moreover, we have $\overline{F}_p = k \otimes F_p = K_p(x_1,\dots,x_s;\, k)$ and $\mathfrak{m}/\mathfrak{m}^2 \otimes_A F_{p-1} = \mathfrak{m}/\mathfrak{m}^2 \otimes_k K_{p-1}(\underline{x};\, k)$. Since the residue classes of the x_i's modulo $\mathfrak{m}^2$ form a k-basis of $\mathfrak{m}/\mathfrak{m}^2$, the formula (2) of (18.D) implies that d_p induces an injection $\overline{F}_p \to \mathfrak{m}/\mathfrak{m}^2 \otimes F_{p-1}$. Thus the conditions of Lemma 9 are all satisfied. Therefore we have

$$\binom{s}{p} = \text{rank}_A F_p \leqq \text{rank}_k \text{ Tor}_p^A(k,k).$$

(18.G) THEOREM 45 (Serre). A noetherian local ring A is regular iff the global dimension of A is finite.

Proof. We have already proved the 'only-if' part in Th.42. So suppose that $(A,\mathfrak{m},k)$ is a noetherian local ring with gl.dim $A = n < \infty$. Put $\text{rank}_k\, \mathfrak{m}/\mathfrak{m}^2 = s$. Then $\text{Tor}_s^A(k,k) \neq 0$ by Th.44, hence gl.dim $A \geqq s$. On the other hand, it follows from the formula proj.dim M + depth M = depth A of Auslander-Buchsbaum (p.113 Ex.4) and from Th.41 that gl.dim A = proj.dim k = depth A. Therefore we get

$$\dim A \leqq \text{rank}_k\, \mathfrak{m}/\mathfrak{m}^2 \leqq \text{gl.dim } A = \text{depth } A \leqq \dim A.$$

Whence $\dim A = \text{rank}_k\, \mathfrak{m}/\mathfrak{m}^2$, which means A is regular.

COROLLARY. If A is a regular local ring then $A_{\mathfrak{p}}$ is regular for any $\mathfrak{p} \in \text{Spec}(A)$.

Proof. Let M be an $A_{\mathfrak{p}}$-module. As an A-module it has a projective resolution of finite length: $0 \to P_n \to \dots \to P_0 \to M \to 0$, $n \leqq$ gl.dim A. By flatness of $A_{\mathfrak{p}}$ the sequence $0 \to (P_n)_{\mathfrak{p}} \to \dots \to (P_0)_{\mathfrak{p}} \to M_{\mathfrak{p}} = M \to 0$ is exact, and gives a projective resolution of M as A_p-module. Hence $\text{gl.dim } A_p \leqq \text{gl.dim } A < \infty$.

DEFINITION. A ring A is called a regular ring if A_p is a regular local ring for every maximal ideal p of A. In view of the above Corollary, this is equivalent to saying that A_p is a regular local ring for every $p \in \text{Spec}(A)$.

(18.H) THEOREM 46. Let A be a regular local ring, and B a domain containing A which is a finite A-module. Then B is flat (hence free) over A iff B is Cohen-Macaulay. In particular, if B is regular then it is a free A-module.

Proof. Suppose B is flat over A. Then B is C.M. as A is so. (For, if P is a maximal ideal of B then $\dim B_P \leqslant \dim A$ by (13.C), while any A-regular sequence is also B_P-regular by the flatness and hence $\text{depth } B_P \geqslant \text{depth } A$.) Conversely, suppose B is Cohen-Macaulay. Since A is normal the going-down theorem holds between A and B by (5.E), so if $\mathfrak{m}$ is the maximal ideal of A we have $\text{ht}(\mathfrak{m}B) = \text{ht}(\mathfrak{m})$ by (13.B)Th.19(3). By the unmixedness theorem in B, any regular system of parameters of A is a B-regular sequence. Therefore the depth of B as A-module is equal to $\dim A = \text{depth } A$, and by the formula of Auslander-Buchsbaum (p.114 ex.4) we have $\text{proj.dim}_A B = 0$, i.e. B is A-free.

19. Unique Factorization

(19.A) Let A be an integral domain. An element $a \neq 0$ of A is said to be irreducible if it is a non-unit of A and if it is not a product of two non-units of A. The ring A is called a unique factorization domain (UFD) if every non-zero element is a product of a unit and of a finite number of irreducible elements and if such a representation is unique up to order and units. A noetherian domain in which every irreducible element generates a prime ideal is UFD.

THEOREM 47. A noetherian domain A is UFD iff every prime ideal of height 1 is principal.

Proof. Suppose that the condition holds. Let π be an irreducible element and let p be a minimal prime overideal of πA. Then $\text{ht}(p) = 1$ by Th.18, so that p is principal: $p = aA$. Then $\pi = au$ with some u, which must be a unit by the irreducibility of π. Thus $\pi A = p$. As we remarked above, this means that A is UFD. The converse is left to the reader.

(19.B) LEMMA. Let A be a noetherian domain and let $x \neq 0$ be an element such that xA is prime. Put $A_x = S^{-1}A$, where $S = \{1, x, x^2, \dots\}$. Then A is UFD iff A_x is so.

Proof is easy and is left to the reader.

THEOREM 48 (Auslander-Buchsbaum, 1959). A regular local ring $(A, \mathfrak{m})$ is UFD.

Proof. (Kaplansky) We use induction on dim A. If dim A = 0 then A is a field, and if dim A = 1 then A is a principal ideal domain. Suppose dim A > 1. Let $x \in \mathfrak{m} - \mathfrak{m}^2$. Then xA is prime, hence we have only to prove that A_x is UFD. Let $\mathfrak{p}'$ be a prime ideal of height 1 in A_x and put $\mathfrak{p} = \mathfrak{p}' \cap A$. Then $\mathfrak{p}' = \mathfrak{p}A_x$. Since A is a regular local ring, the A-module $\mathfrak{p}$ has a resolution of finite length

(1) $\quad 0 \to F_n \to F_{n-1} \to \cdots \to F_0 \to \mathfrak{p} \to 0$

with F_i finite and free. If P is a prime ideal of A_x, the local ring $(A_x)_P = A_{(A \cap P)}$ is a UFD by induction assumption. Therefore $\mathfrak{p}'(A_x)_P$ is principal. So we have $\text{proj.dim}\, \mathfrak{p}' = \sup_P (\text{proj.dim}\, \mathfrak{p}'(A_x)_P) = 0$ by (18.B)Lemma 5, i.e. $\mathfrak{p}'$ is projective. Localizing (1) with respect to $S = \{1, x, x^2, .\}$ we see

(2) $\quad 0 \to F'_n \to F'_{n-1} \to \cdots \to F'_0 \to \mathfrak{p}' \to 0$

is exact, where $F'_i = F_i \otimes A_x$ are finite and free over A_x. If we decompose (2) into short exact sequences

(3) $0 \to K'_0 \to F'_0 \to \mathfrak{p}' \to 0, \quad 0 \to K'_1 \to F'_1 \to K'_0 \to 0, \ \ldots,$

$0 \to F'_n \to F'_{n-1} \to K'_{n-1} \to 0,$

then each K'_i must be projective. Hence the short exact sequences of (3) split. It follows that

$$\bigoplus_{i \text{ even}} F'_i \simeq \bigoplus_{i \text{ odd}} F'_i \oplus \mathfrak{p}.$$

Thus, we have finite free A_x-modules F and G such that $F \simeq G \oplus \mathfrak{p}'$. Put rank G = r. Since $\mathfrak{p}'$ is a non-zero ideal of the integral domain A_x we have $\text{rank}\, \mathfrak{p}' = 1$ and rank F = r + 1. From this we can conclude that $\mathfrak{p}'$ is free (hence principal), in the following way. Take the (r + 1)-ple exterior products of F and $G + \mathfrak{p}'$, respectively. Then

$$A_x = \Lambda^{r+1} F \simeq \Lambda^{r+1}(G \oplus \mathfrak{p}') = \mathfrak{p}'$$

because $\Lambda^i \mathfrak{p}' = 0$ for all i > 1 (this last assertion can be seen by localization: if M is a projective module of rank 1 over a ring B, then $(\Lambda^i M)_P = \Lambda^i M_P \simeq \Lambda^i B_P = 0$ for i > 1 and for all $P \in \text{Spec}(B)$, so $\Lambda^i M = 0$.)

REMARKS TO CHAPTER 7.

1. As Th.35 suggests, regular local rings are similar to polynomial rings or power series rings in many aspects. In particular, the inequality on the dimension (14.K) can be extended to an arbitrary regular local ring. Namely, in the non-local form one has the following theorem (due to Serre): Let A be a regular ring, $P_i\, (i = 1,2)$ prime ideals of A and Q a minimal prime over-ideal of $P_1 + P_2$. Then

$$\text{ht}(Q) \leq \text{ht}(P_1) + \text{ht}(P_2).$$

For the proof see J.-P. Serre: Algèbre Locale· Multiplicité (2nd ed.) Ch.V, p.18.

2. A normal domain A is called a Krull ring if (1) for any non-zero element x of A, the number of the prime ideals of A of height one containing x is finite, and (2) $A = \bigcap_{ht(p)=1} A_p$. Noetherian normal rings are Krull, but not conversely. If A is a noetherian domain, then the integral closure of A in the quotient field of A is a Krull ring (Theorem of Y. Mori, cf. Nagata: Local Rings). On Krull rings, cf. Bourbaki: Alg. Comm. Ch.7.

3. P. Samuel has made an extensive study on the subject of unique factorization. Cf. his Tata lecture note.

4. We did not discuss valuation theory. On this topic the following paper contains important results in connection with algebraic geometry. Abhyankar: On the valuations centered in a local domain, Amer. J. Math. 78(1956), 321-348.

CHAPTER 8. FLATNESS II.

20. Local Criteria of Flatness

(20.A) In (18.B) Lemma 4 we proved the following.

> Let $(A, \mathfrak{m})$ be a noetherian local ring and M a finite A-module. Then M is flat iff $\mathrm{Tor}_1(M, A/\mathfrak{m}) = 0$.

The condition that M is finite over A is too strong; in geometric application it is often necessary to prove flatness of infinite modules. In this section we shall learn several criteria of flatness, due to Bourbaki, which are very useful.

Let A be a ring, I an ideal of A and M an A-module. We say that M is idealwise separated (i.s. for short) for I if, for each finitely generated ideal q of A, the A-module $q \otimes_A M$ is separated in the I-adic topology.

Example 1. Let B be a noetherian A-algebra such that $IB \subseteq \mathrm{rad}(B)$, and let M be a finite B-module. Then M is i.s. for I as an A-module: since $q \otimes_A M$ is a finite B-module and since the I-adic topology on $q\otimes M$ is nothing but the IB-adic topology, we can apply (11.D) Cor.1.

Example 2. When A is a principal ideal domain, any I-adically separated A-module M is i.s. for I.

Example 3. Let M be an I-adically separated flat A-module. Then M is i.s. for I. In fact we have $q\otimes M \simeq qM \subseteq M$.

(20.B) Put $gr(A) = gr^I(A) = \bigoplus_{n=0}^{\infty} I^n/I^{n+1}$, $gr(M) = gr^I(M) = \bigoplus_{n=0}^{\infty} I^nM/I^{n+1}M$, $A_0 = gr_0(A) = A/I$ and $M_0 = gr_0(M) = M/IM$. Then gr(M) is a graded gr(A)-module. There are canonical epimorphisms

$$\gamma_n: I^n/I^{n+1} \otimes_{A_0} M_0 \rightarrow I^nM/I^{n+1}M$$

for n = 0,1,2,... . In other words, there is a degree-preserving epimorphism $\gamma: gr(A) \otimes_{A_0} M_0 \rightarrow gr(M)$.

(20.C) THEOREM 49 (Local criteria of flatness). Let A be a ring, I an ideal of A and M an A-module. Assume that either

(α) I is nilpotent,

or (β) A is noetherian and M is idealwise separated for I.

Then the following are equivalent:

(1) M is A-flat;

(2) $Tor_1^A(N,M) = 0$ for all A_0-modules N;

(3) M_0 is A_0-flat, and $I \otimes_A M \simeq IM$ by the natural map, (note that, if I is a maximal ideal, the flatness over A_0 is trivial);

(3') M_0 is A_0-flat and $Tor_1^A(A_0,M) = 0$;

(4) M_0 is A_0-flat, and the canonical maps

$$\gamma_n: I^n/I^{n+1} \otimes_{A_0} M_0 \rightarrow I^nM/I^{n+1}M$$

are isomorphisms;

(5) $M_n = M/I^{n+1}M$ is flat over $A_n = A/I^{n+1}$, for each $n \geq 0$.

(The implications (1) $\Rightarrow$ (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (3') $\Rightarrow$ (4) $\Rightarrow$ (5) are true without any assumption on M.)

Proof. We first prove the equivalence of (1) and (5) under the assumption (α) or (β). The implication (1) $\Rightarrow$ (5) is just a change of base (cf.(3.C)).

(5) $\Rightarrow$ (1): The nilpotent case (α) is trivial ($A = A_n$ for some n). In the case (β), we prove the flatness of M by showing that, for every ideal q of A, the canonical map $j: q\otimes M \rightarrow M$ is injective. Since $q\otimes M$ is I-adically separated it suffices to prove that $Ker(j) \subseteq I^n(q\otimes M)$ for all $n > 0$. Fix an n. Then there exists, by Artin-Rees, an integer $k > n$ such that $q \cap I^k \subseteq I^n q$. Consider the natural maps

$$q\otimes M \xrightarrow{f} (q/I^k \cap q)\otimes M \xrightarrow{g} (q/I^nq)\otimes M = (q\otimes M)/I^n(q\otimes M).$$

Since M_{k-1} is A_{k-1}-flat, the natural map $q/(I^k \cap q) \otimes_A M = q/(I^k \cap q) \otimes_{A_{k-1}} M_{k-1} \rightarrow M_{k-1}$ is injective. Therefore

$\mathrm{Ker}(j) \subseteq \mathrm{Ker}(f)$, and a fortiori $\mathrm{Ker}(j) \subseteq \mathrm{Ker}(gf) = I^n(q \otimes M)$. Thus our assertion is proved.

Next we prove $(1) \Rightarrow (2) \Leftrightarrow (3) \Leftrightarrow (3') \Rightarrow (4) \Rightarrow (5)$ for arbitrary M. $(1) \Rightarrow (2)$ is trivial.

$(2) \Rightarrow (3)$: Let $0 \to N' \to N \to N'' \to 0$ be an exact sequence of A_0-modules. Then $0 = \mathrm{Tor}_1^A(N'', M) \to N' \otimes_A M = N' \otimes_{A_0} M_0 \to N \otimes_A M = N \otimes_{A_0} M_0$ is exact, so M_0 is A_0-flat. From the exact sequence $0 \to I \to A \to A_0 \to 0$ we get $0 = \mathrm{Tor}_1^A(A_0, M) \to I \otimes M \to M$ exact, which proves $I \otimes M \simeq IM$.

$(3) \Rightarrow (3')$: immediate.

$(3') \Rightarrow (2)$: let N be an A_0-module and take an exact sequence of A_0-modules $0 \to R \to F_0 \to N \to 0$ where F_0 is A_0-free. Then $\mathrm{Tor}_1^A(F_0, M) = 0 \to \mathrm{Tor}_1^A(N, M) \to R \otimes_{A_0} M_0 \to F_0 \otimes_{A_0} M_0$ is exact and M_0 is A_0-flat, hence $\mathrm{Tor}_1^A(N, M) = 0$.

$(2) \Rightarrow (4)$: consider the exact sequences

$$0 \to I^{n+1} \to I^n \to I^n/I^{n+1} \to 0$$

and the commutative diagrams

$$\begin{array}{ccccccccc}
0 & \to & I^{n+1} \otimes M & \to & I^n \otimes M & \to & (I^n/I^{n+1}) \otimes M & \to & 0 \\
 & & \downarrow \alpha_{n+1} & & \downarrow \alpha_n & & \downarrow \gamma_n & & \\
0 & \to & I^{n+1}M & \to & I^n M & \to & I^n M/I^{n+1}M & \to & 0,
\end{array}$$

where $\alpha_1, \alpha_2, \ldots$ are the natural epimorphisms, the first row is exact by (2) and the second row is of course exact. Since α_1 is injective by (3) we see inductively that all α_n are

injective. Thus they are isomorphisms, and consequently the γ_n are also isomorphisms.

Before proving $(4) \Rightarrow (5)$ we remark the following fact: if (2) holds then, for any $n \geqslant 0$ and for any A_n-module N, we have $\mathrm{Tor}_1^A(N, M) = 0$. In fact, if N is an A_n-module and $n > 0$, then IN and N/IN are A_{n-1}-modules, so that the assertion is proved by induction on n.

$(4) \Rightarrow (5)$: we fix an integer $n \geqslant 0$ and we are going to prove that M_n is A_n-flat. For $n = 0$ this is included in the assumptions, so we suppose $n > 0$. Put $I_n = I/I^{n+1}$.

Consider the commutative diagrams with exact rows:

$$\begin{array}{ccccccc}
(I^{i+1}/I^{n+1}) \otimes M & \longrightarrow & (I^i/I^{n+1}) \otimes M & \longrightarrow & (I^i/I^{i+1}) \otimes M & \longrightarrow & 0 \\
\downarrow \bar{\alpha}_{i+1} & & \downarrow \bar{\alpha}_i & & \downarrow \gamma_i & & \\
0 \longrightarrow I^{i+1}M_n = I^{i+1}M/I^{n+1}M & \longrightarrow & I^i M_n = I^i M/I^{n+1}M & \longrightarrow & I^i M/I^{i+1}M & \longrightarrow & 0
\end{array}$$

for $i = 1, 2, \ldots, n$. Since the γ_i are isomorphisms by assumption, and since $\bar{\alpha}_{n+1} = 0$, we see by descending induction on i that all $\bar{\alpha}_i$ are isomorphisms. In particular, $\bar{\alpha}_1 : I/I^{n+1} \otimes_A M = IA_n \otimes_{A_n} M_n \to IM_n$ is an isomorphism. Therefore the condition (3) (hence also (2)) holds for A_n, IA_n and M_n. From this and from what we have just remarked it follows that $\mathrm{Tor}_1^{A_n}(N, M_n) = 0$ for all A_n-modules N, hence M_n is A_n-flat.

Q.E.D.

(20.D) APPLICATION 1 (Hartshorne). Let $(B, \mathfrak{n})$ be a noetherian local ring containing a field k and let $x_1, \ldots, x_n$ be a B-regular sequence in $\mathfrak{n}$. Then the subring $k[x_1, \ldots, x_n]$ of B is isomorphic to the polynomial ring $A = k[X_1, \ldots, X_n]$, and B is flat over it.

Proof. Considering the k-algebra homomorphism $\phi: A \to B$ such that $\phi(X_i) = x_i$, we view B as an A-algebra. It suffices to prove B is flat over A. In fact, any non-zero element y of A is A-regular, so under the assumption of flatness it is also B-regular, hence $\phi(y) \neq 0$.

We apply the criterion (3') of Th.49 to A, $I = \sum_1^n X_i A$ and M = B. The A-module B is idealwise separated for I as $IB \subseteq \mathrm{rad}(B)$. Since $A/I = k$ is a field we have only to prove $\mathrm{Tor}_1^A(k, B) = 0$. Now the Koszul complex $K.(X_1, \ldots, X_n; A)$ is a free resolution of the A-module $k = A/I$ by Cor. to Th.43. So we have $\mathrm{Tor}_i^A(k, B) = H_i(K.(X_1, \ldots, X_n; A) \otimes_A B) = H_i(K.(x_1, \ldots, x_n; B))$, which is zero for $i > 0$ as $x_1, \ldots, x_n$ is a B-regular sequence.

(20.E) APPLICATION 2 (EGA 0_{III} (10.2.4)). Let $(A, \mathfrak{m}, k)$ and $(B, \mathfrak{n}, k')$ be noetherian local rings and $A \to B$ a local homomorphism. Let $u: M \to N$ be a homomorphism of finite B-modules, and assume that N is A-flat. Then the following are equivalent: (a) u is injective, and $N/u(M)$ is A-flat;

(b) $\bar{u}: M \otimes_A k \to N \otimes_A k$ is injective.

Proof. (a) $\Rightarrow$ (b). Immediate.

(b) $\Rightarrow$ (a). Let $x \in \mathrm{Ker}(u)$. Then $x \otimes 1 = 0$ in $M \otimes k = M/\mathfrak{m}M$, therefore $x \in \mathfrak{m}M$. We will show $x \in \bigcap_n \mathfrak{m}^n M = (0)$ by induction. Suppose $x \in \mathfrak{m}^n M$, let $\{a_1, \ldots, a_p\}$ be a minimal basis of the ideal $\mathfrak{m}^n$ and write $x = \sum a_i x_i$, $x_i \in M$. Then $u(x) = \sum a_i u(x_i) = 0$ in N. By flatness of N there exists $c_{ij} \in A$ and $x'_j \in N$ such that $\sum_i a_i c_{ij} = 0$ (for all j) and such that $u(x_i) = \sum_j c_{ij} x'_j$ (for all i). By the choice of $a_1, \ldots, a_p$ all the c_{ij} must belong to $\mathfrak{m}$. Thus $u(x_i) \in \mathfrak{m}N$, in other words $\bar{u}(x_i \otimes 1) = 0$. Since $\bar{u}$ is injective we get $x_i \in \mathfrak{m}M$, hence $x \in \mathfrak{m}^{n+1}M$. Thus u is injective and we get an exact sequence $0 \to M \xrightarrow{u} N \to N/u(M) \to 0$. From this and from the hypotheses it follows that $\mathrm{Tor}_1^A(k, N/u(M)) = 0$, which shows the flatness of $N/u(M)$ by Th.49.

(20.F) COROLLARY 1. Let A be a noetherian ring, B a noetherian A-algebra, M a finite B-module and $f \in B$. Suppose that (i) M is A-flat, and (ii) for each maximal ideal P of B, the element f is $M/(P \cap A)M$-regular. Then f is M-regular and M/fM is A-flat.

Proof. If K denotes the kernel of $M \xrightarrow{f} M$, then K = 0 iff

$K_P = 0$ for all maximal ideals P of B. Similarly, by an obvious extension of (3.J), M/fM is A-flat iff M_P/fM_P is flat over $A_{(P\cap A)}$ for all maximal P. The assumptions are also stable under localization. So we may assume that $(A, \mathfrak{m}, k)$ and $(B, \mathfrak{n}, k')$ are noetherian local rings and $A \to B$ is a local homomorphism. Then the assertion follows from (20.E).

COROLLARY 2. Let A be a noetherian ring and $B = A[X_1, \ldots, X_n]$ a polynomial ring over A. Let $f(X) \in B$ be such that its coefficients generate over A the unit ideal A. Then f is not a zero-divisor of B, and B/fB is A-flat.

(20.G) APPLICATION 3. Let $A \to B \to C$ be local homomorphisms of noetherian local rings and M be a finite C-module. Suppose B is A-flat. Let k denote the residue field of A. Then

$$M \text{ is B-flat} \Leftrightarrow M \text{ is A-flat and } M \otimes_A k \text{ is } B \otimes_A k\text{-flat}.$$

Proof. (⇒) Trivial. (⇐) Use the criterion (4) of Th.49.

For more applications of Th.49, cf. EGA 0_{III} (10.2).

21. Fibres of Flat Morphisms

(21.A) Let $\phi: A \to B$ be a homomorphism of noetherian rings; let $P \in \mathrm{Spec}(B)$, $p = P \cap A$ and $\kappa(p)$ = the residue field of A_p.

Then the 'fibre over p' is $\mathrm{Spec}(B \otimes_A \kappa(p))$, and 'the local ring of P on the fibre' is $B_P/pB_P = B_P \otimes_A \kappa(p)$ (cf. p.79). Suppose B is flat over A. Then we have

$$\dim(B_P) = \dim(A_p) + \dim(B_P \otimes \kappa(p))$$

by (13.B) Th.19.

(21.B) THEOREM 50. Let $(A, \mathfrak{m}, k)$ and $(B, \mathfrak{n}, k')$ be noetherian local rings, and let $A \to B$ a local homomorphism. Let M be a finite A-module and N be a finite B-module which is A-flat. Then we have

$$\mathrm{depth}_B(M \otimes_A N) = \mathrm{depth}_A M + \mathrm{depth}_{B\otimes k}(N \otimes k).$$

Proof. Induction on $n = \mathrm{depth}\, M + \mathrm{depth}\, N \otimes k$.

Case 1: $n = 0$. Then $\mathfrak{m} \in \mathrm{Ass}_A(M)$ and $\mathfrak{n} \in \mathrm{Ass}_B(N \otimes k)$, and we know (p.58) that

$$\mathrm{Ass}_B(M \otimes_A N) = \bigcup_{p \in \mathrm{Ass}_A(M)} \mathrm{Ass}_B(N \otimes A/p).$$

Hence $\mathfrak{n} \in \mathrm{Ass}_B(M \otimes N)$, i.e. $\mathrm{depth}_B(M \otimes N) = 0$.

Case 2: depth $M > 0$. Easy and left to the reader.

Case 3: depth $N \otimes k > 0$. Take $y \in \mathfrak{n}$ which is $N \otimes k$-regular. By (20.E) y is N-regular and N/yN is A-flat. From the exact sequence $0 \to N \xrightarrow{y} N \to N/yN \to 0$ it then follows that

$$0 \to M \otimes N \xrightarrow{y} M \otimes N \to M \otimes (N/yN) \to 0$$

is exact. Putting $\bar{N} = N/yN$ we get $\mathrm{depth}_B(M \otimes N) - 1 = \mathrm{depth}_B(M \otimes \bar{N})$, and $\mathrm{depth}_{B\otimes k}(N \otimes k) - 1 = \mathrm{depth}_{B\otimes k}(\bar{N} \otimes k)$.

From these and from the induction hypothesis on $\overline{N}$ we get the desired formula.

(21.C) COROLLARY 1. Let $A \to B$ be as above and suppose that B is A-flat. Then we have

$$\text{depth } B = \text{depth } A + \text{depth } B \otimes k,$$

and

$$B \text{ is C.M.} \iff A \text{ and } B\otimes k \text{ are C.M.}.$$

COROLLARY 2. Let A and B be noetherian rings and $A \to B$ be a faithfully flat homomorphism. Let i be a positive integer. Then (1) if B satisfies the condition (S_i) of (17.I), so does A;

(2) if A satisfies (S_i) and if all fibres satisfy (S_i) (i.e. $B\otimes\kappa(\mathfrak{p})$ satisfies (S_i) for every $\mathfrak{p} \in \operatorname{Spec}(A)$) then B satisfies (S_i).

Proof. (1) Given $\mathfrak{p} \in \operatorname{Spec}(A)$, take $P \in \operatorname{Spec}(B)$ which is minimal among prime ideals of B lying over $\mathfrak{p}$, and put $k = \kappa(\mathfrak{p})$. Then $\dim B_P \otimes k = \text{depth } B_P \otimes k = 0$, whence $\text{depth } B_P = \text{depth } A_{\mathfrak{p}}$ and $\dim B_P = \dim A_{\mathfrak{p}}$. Therefore

$$\text{depth } A_{\mathfrak{p}} = \text{depth } B_P \geqslant \inf(i, \dim B_P) = \inf(i, \dim A_{\mathfrak{p}}).$$

(2) Given $P \in \operatorname{Spec}(B)$, put $\mathfrak{p} = P \cap A$ and $k = \kappa(\mathfrak{p})$. Then

$$\begin{aligned}\text{depth } B_P &= \text{depth } A_{\mathfrak{p}} + \text{depth } (B_P \otimes k)\\ &\geqslant \inf(i, \dim A_{\mathfrak{p}}) + \inf(i, \dim B_P\otimes k)\\ &\geqslant \inf(i, \dim A_{\mathfrak{p}} + \dim B_P \otimes k)\\ &= \inf(i, \dim B_P).\end{aligned}$$

Q.E.D.

(21.D) THEOREM 51. Let $(A, \mathfrak{m}, k)$ and $(B, \mathfrak{n}, k')$ be noetherian local rings and $\phi: A \to B$ a local homomorphism. Then:

(i) if B is flat over A and regular, then A is regular.

(ii) if $\dim B = \dim A + \dim B\otimes k$ holds, and if A and $B\otimes k = B/\mathfrak{m}B$ are regular, then B is flat over A and regular.

Proof. (i) Since a flat base change commutes with homology, we have $\operatorname{Tor}_q^A(k, k) \otimes_A B = \operatorname{Tor}_q^B(k\otimes B, k\otimes B) = 0$ for $q > \dim B$. Since B is faithfully flat over A this implies $\operatorname{Tor}_q^A(k, k) = 0$, hence gl.dim A is finite, i.e. A is regular.

(ii) If $\{x_1, \ldots, x_r\}$ is a regular system of parameters of A and if $y_1, \ldots, y_s \in \mathfrak{n}$ are such that their images form a regular system of parameters of $B/\mathfrak{m}B$, then $\{\phi(x_1), \ldots, \phi(x_r), y_1, \ldots, y_s\}$ generates $\mathfrak{n}$, and $r + s = \dim B$ by hypothesis. Thus B is regular. To prove flatness it suffices, by the criterion (3') of Th.49, to prove $\operatorname{Tor}_1^A(k, B) = 0$. The Koszul complex $K.(x_1, \ldots x_r; A)$ is a free resolution of the A-module k, hence we have $\operatorname{Tor}_1^A(k, B) = H_1(K.(\underline{x}; A)\otimes_A B) = H_1(K.(\underline{x}; B))$. Since the sequence $\phi(x_1), \ldots, \phi(x_r)$ is a part of a regular system of parameters of B it is a B-regular sequence. Hence we have $H_i(K.(\underline{x}; B)) = 0$ for all $i > 0$, and we are done.

Remark. Even if B is regular and A-flat, the local ring $B\otimes k$ on the fibre is not necessarily regular. Example: put k = a field, $k[x,y] = k[X,Y]/((X-1)^2+Y^2-1)$, $B = k[x,y]_{(x,y)}$, $A = k[x]_{(x)}$ and $\mathfrak{m} = xA$. Then $B\otimes(A/\mathfrak{m}) \simeq k[Y]/(Y^2)$ has nilpotent elements.

(21.E) COROLLARY. Let A and B be noetherian rings and $A \to B$ a faithfully flat homomorphism. Then

i) if B satisfies (R_i), so does A;

ii) if A and all fibres $B\otimes\kappa(p)$ ($p \in \mathrm{Spec}(A)$) satisfy (R_i), then B satisfies (R_i);

iii) if B is normal (resp. C.M., resp. reduced), so is A. Conversely, if A and all fibres are normal (resp. ...) then B is normal (resp. ...).

Proof. i) and ii) are immediate from Th.51. As for iii), it is enough to recall (17.I) that normal $\Leftrightarrow (R_1) + (S_2)$, C.M. $\Leftrightarrow$ all (S_i), and reduced $\Leftrightarrow (R_0) + (S_1)$.

22. Theorem of Generic Flatness

(22.A) LEMMA 1. Let A be a noetherian domain, B an A-algebra of finite type and M a finite B-module. Then there exists $0 \neq f \in A$ such that $M_f = M\otimes_A A_f$ is A_f-free (where A_f is the localization of A with respect to $\{1,f,f^2,\ldots\}$).

Proof. We may suppose that $M \neq 0$. Then, by (7.E) Th.10 there exists a chain of submodules $0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$ with $M_i/M_{i-1} \simeq B/p_i$, $p_i \in \mathrm{Spec}(B)$. Since an extension of free modules is again free, it suffices to prove the lemma for the case that B is a domain and M = B. If the canonical map $A \to B$ has a non-trivial kernel then $B_f = 0$ for any non-zero element f of the kernel, and our assertion is trivial. So we may assume that A is a subring of the domain B. Let K be the quotient field of A. Then $B\otimes K = BK$ is a domain (contained in the quotient field of B) and is finitely generated as an algebra over K. Hence $\dim BK = \mathrm{tr.deg}_K BK < \infty$. Put $n = \dim BK$. We use induction on n. By the normalization theorem (14.G), the ring BK contains n algebraically independent elements $y_1,\ldots,y_n$ such that BK is integral over K[y]. We may assume that $y_i \in B$. Since B is finitely generated over A there exists $0 \neq g \in A$ such that $B_g = B\cdot A_g$ is integral over $A_g[y]$. Replacing A and B by A_g and B_g respectively, and putting C = A[y], we have that B is a finite module over the polynomial ring C. Let $b_1,\ldots,b_m$ be a maximal set of linearly independent elements over C in B. Then we have an exact sequence

$$0 \to C^m \to B \to B' \to 0$$

where B' is a finitely generated torsion C-module. Since $(C/p)\otimes K = CK/pK$ has a smaller dimension than $n = \dim CK$ for any non-zero prime ideal p of C, there exists by the induction assumption a non-zero element f of A such that B'_f is A_f-free. Since $C_f^m = (A_f[y_1,\dots,y_n])^m$ is also A_f-free, the localization B_f is A_f-free. Q.E.D.

An important special case of the Lemma is the following

THEOREM 52. Let A be a noetherian domain and B an A-algebra of finite type. Suppose that the canonical map $\phi: A \to B$ is injective. Then there exists $0 \neq f \in A$ such that B_f is A_f-free and $\neq 0$. Thus, the map ${}^a\phi$: Spec(B) $\to$ Spec(A) is faithfully flat over the non-empty open set D(f) = Spec(A) - V(f) of Spec(A), that is, ${}^a\phi^{-1}(D(f)) \to D(f)$ is faithfully flat.

(22.B) LEMMA 2. Let B be a noetherian ring and let U be a subset of Spec(B). Then U is open iff the following conditions are satisfied.

(1) U is stable under generalization,

(2) if $P \in U$ then U contains a non-empty open set of the irreducible closed set V(P).

Proof. Assume the conditions, and let F be the complement of U and $P_i (1 \leq i \leq s)$ be the generic points of the irreducible components of the closure $\overline{F}$ of F. Then (2) implies that P_i cannot lie in U. Hence $P_i \in F$, and so $F = \overline{F}$ by (1). Q.E.D.

THEOREM 53. Let A be a noetherian ring, B an A-algebra of finite type and M a finite B-module. Put $U = \{P \in \mathrm{Spec}(B) \mid M_P$ is flat over A$\}$. Then U is open in Spec(B).

Remark 1. The set U may be empty.

Remark 2. It follows from (6.I) Th.8 that a flat morphism of finite type between noetherian preschemes is an open map. Therefore the image of U in Spec(A) is open in Spec(A).

Proof. Let $P \supset Q$ be prime ideals of B with M_P flat over A. For any A-module N we have $N \otimes_A M_Q = (N \otimes_A M_P) \otimes_B B_Q$, therefore M_Q is flat over A and the condition (1) of Lemma 2 is verified for U. As for the condition (2), let $P \in U$ and put $p = P \cap A$ and $\overline{A} = A/p$. Let $Q \in V(P)$. Then $pB_Q \subseteq \mathrm{rad}(B_Q)$, so we can apply the local criterion of flatness that M_Q is flat over A iff M_Q/pM_Q is flat over $\overline{A}$ and $\mathrm{Tor}_1^A(M_Q, \overline{A}) = 0$. Applying Lemma 1 to $(\overline{A}, B/pB, M/pM)$ we see that there exists a neighborhood of P in V(pB) such that M_Q/pM_Q is flat over $\overline{A}$ for each point Q in it. On the other hand, since $0 = \mathrm{Tor}_1^A(M_P,\overline{A}) = \mathrm{Tor}_1^A(M,\overline{A}) \otimes_B B_P$ and since $\mathrm{Tor}_1^A(M,\overline{A})$ is a finite B-module, there exists a neighborhood of P in Spec(B) in which $\mathrm{Tor}_1^A(M_Q, \overline{A}) = 0$. Therefore there exists a non-empty open set of V(P) in which M_Q is A-flat for all points Q, in other words the set U in question contains a non-empty open set of V(P). Thus the theorem is proved.

(22.C) Let $\underline{P}$ be a property on noetherian local rings and let $\underline{P}(A)$ denote the set $\{p \in \mathrm{Spec}(A) \mid A_p$ has the property $\underline{P}\}$. Consider the following statement.

(NC) If A is a noetherian ring and if, for every $p \in \mathrm{Spec}(A)$, $\underline{P}(A/p)$ contains a non-empty open set of $\mathrm{Spec}(A/p)$, then $\underline{P}(A)$ is open in Spec(A).

While Lemma 2 of (22.B) was topological, (NC) is ring-theoretical and its validity of course depends on $\underline{P}$. Both are inventions of Nagata (NC means Nagata criterion), who proved (NC) for $\underline{P}$ = regular (cf. p.245). As an example we prove

PROPOSITION. (NC) is valid for $\underline{P}$ = CM.

Proof. CM(A) is stable under generalization. We will prove (2) of Lemma 2. If $P \in \mathrm{CM}(A)$ and ht $P = n$, we can take an A_P-regular sequence $y_1,\dots,y_n$ from P. Replacing A by A_a with suitable $a \in A - P$, we may assume that $y_1,\dots,y_n$ is an A-regular sequence and $I = \sum y_iA$ is a P-primary ideal. Then for $Q \in V(P)$, A_Q is CM iff A_Q/IA_Q is so. Hence we can replace A by A/I and assume that (0) is P-primary. So we have $P^r = 0$ for some $r > 0$. Since P^i/P^{i+1} is a finite A/P-module for each $0 \leq i < r$, we may assume (replacing A by some A_a) that the P^i/P^{i+1} are free A/P-modules. Then it is easy to see that a sequence $x_1,\dots,x_n \in A$ is A-regular if it is A/P-regular. By the hypothesis of (NC) we may assume further that A/P is CM. Then depth A_Q = depth A_Q/PA_Q = dim A_Q/PA_Q = dim A_Q, hence $Q \in \mathrm{CM}(A)$.

EXERCISE. If A is a homomorphic image of a CM ring, then CM(A) is open.

CHAPTER 9. Completion

23. Completion

(23.A) Let A be a ring, and let F be a set of ideals of A such that for any two ideals $I_1, I_2 \in F$ there exists $I_3 \in F$ contained in $I_1 \cap I_2$. Then one can define a topology on A by taking $\{x + I \mid I \in F\}$ as a fundamental system of neighborhoods of x for each $x \in A$. One sees immediately that in this topology the addition, the multiplication and the map $x \mapsto -x$ are continuous; in other words A is a topological ring. A topology on a ring obtained in this manner is called a linear topology. When M is an A-module one defined a linear topology on M in the same way, the only difference being that 'ideals' are replaced by 'submodules'. Let $M = \{M_\lambda\}$ be a set of submodules which defines the topology. Then M is separated (i.e. Hausdorff) iff $\bigcap_\lambda M_\lambda = (0)$. A submodule N of M is closed in M iff $\bigcap(M_\lambda + N) = N$, the left hand side being the closure of N.

(23.B) Let A be a ring, M an A-module linearly topologized by a set of submodules $\{M_\lambda\}$ and N a submodule of M. Let $\overline{M}_\lambda$ be the image of M_λ in M/N. Then the linear topology on M/N defined by $\{\overline{M}_\lambda\}$ is nothing but the quotient topology of the topology on M, as one can easily check. When we say "the quotient module M/N ", we shall always mean the module M/N with the quotient topology. It is separated iff N is closed.

(23.C) For simplicity, we shall consider in the following only such linear topologies that are defined by a countable set of submodules. This is equivalent to saying that the topology satisfies the first axiom of countability. If a linear topology on M is defined by $\{M_1, M_2, \dots\}$, then the set $\{M_1, M_1 \cap M_2, M_1 \cap M_2 \cap M_3, \dots\}$ defines the same topology. Therefore we can assume without loss of generality that $M_1 \supseteq M_2 \supseteq M_3 \supseteq \dots$ (in other words, the topology is defined by a filtration of M, cf. p.67). A sequence (x_n) of elements of M is a <u>Cauchy sequence</u> if, for every open submodule N of M, there exists an integer n_0 such that

(*) $$x_n - x_m \in N \quad \text{for all } n, m > n_0.$$

Since N is a submodule, the condition (*) can also be written as $x_{n+1} - x_n \in N$ for all $n > n_0$. Therefore a sequence (x_n) is Caucy iff $x_{n+1} - x_n$ converges to zero when n tends to infinity. A continuous homomorphism of linearly topologized modules maps Cauchy sequences into Cauchy sequences. A topological A-module M is said to be <u>complete</u> if every Cauchy sequence in M has a limit in M. Note that the limit of a Cauchy sequence is not uniquely determined if M is not separated.

(23.D) PROPOSITION. Let A be a ring and let M be an A-module with a linear topology defined by a filtration $M_1 \supseteq M_2 \supseteq \dots$; let N be a submodule of M. If M is complete, then the quotient module M/N is also complete.

<u>Proof</u>. Let $(\bar{x}_n)$ be a Cauchy sequence in M/N. For each $\bar{x}_n$ choose a pre-image x_n in M. We have $\bar{x}_{n+1} - \bar{x}_n \in \overline{M}_{i(n)}$ with $i(n) \to \infty$, therefore we can write

$$x_{n+1} - x_n = y_n + z_n, \quad y_n \in M_{i(n)}, \quad z_n \in N,$$

and the sequence (y_n) converges to zero in M. Let $s \in M$ be a limit of the Cauchy sequence $x_1, x_1 + y_1, x_1 + y_1 + y_2, \dots$; then its image $\bar{s}$ in M/N is a limit of the sequence $(\bar{x}_n)$. Thus M/N is complete.

(23.E) Let A be a ring, I an ideal and M an A-module. The set of submodules $\{I^n M \mid n = 1,2,..\}$ defines the I-adic topology of M. We also say that the topology is <u>adic</u> and that I is an ideal of definition for the topology. Clearly, any ideal J such that $I^n \subseteq J$ and $J^m \subseteq I$ for some $n,m > 0$ is an ideal of definition for the same topology. When both A and M are I-adically topologized, the map $(a,x) \mapsto ax$ $(a \in A,\ x \in M)$ is a continuous map from $A \times M$ to M. When A is a semi-local ring with $\mathrm{rad}(A) = \mathfrak{m}$ then it is viewed as an $\mathfrak{m}$-adic topological ring, unless the contrary is explicitly stated.

(23.F) Let k be a ring, and let A and B be k-algebras with linear topology defined by $\mathfrak{M} = \{I_n\}$ and $\mathfrak{N} = \{J_m\}$ respectively. Put $C = A \otimes_k B$. Then a linear topology can be defined on C by means of the set of ideals $\{I_nC + J_mC\}_{n,m}$. This is called the topology of tensor product. If A has the I-adic topology and B the J-adic topology, where I (resp. J) is an ideal of A (resp. B), then the topology of tensor product on C is the (IC + JC)-adic topology, for we have

$$(IC + JC)^{n+m-1} \subseteq I^nC + J^mC \quad \text{and} \quad I^nC + J^nC \subseteq (IC + JC)^n.$$

(23.G) PROPOSITION. Let A be a ring and I an ideal of A. Suppose that A is complete and separated for the I-adic topology. Then any element of the form u + x, where u is a unit in A and x is an element of I, is a unit in A. The ideal I is contained in the Jacobson radical of A.

Proof. We have $u + x = u(1 - y)$, where $y = -u^{-1}x \in I$. The infinite series $1 + y + y^2 + \ldots$ converges in A, and we have $(1 - y)(1 + y + y^2 + \ldots) = 1$ since A is separated. Thus $1 - y$ (hence also $u + x$) is a unit. The second assertion is easy.

(23.H) Let A be a ring and M a linearly topologized A-module. The completion of M is, by definition, an A-module M* with a complete separated linear topology, together with a continuous homomorphism $\varphi: M \to M^*$, having the following universal mapping property: for any A-module M' with a complete separated linear topology and for any continuous homomorphism $f: M \to M'$, there exists a unique continuous homomorphism $f^*: M^* \to M'$ satisfying $f^*\varphi = f$. The completion of M exists, and is unique up to isomorphisms. In fact the uniqueness is clear from the definition, while the existence can be proved by several methods. First of all, note that, if K is the intersection of all open submodules of M, the canonical map $\varphi: M \to M^*$ must factor through $M^h = M/K$ (which is called the Hausdorffization of M) and hence M and M^h have the same completion.

1. Take the completion of the uniform space M^h and call it M*. The topological space M* becomes a linearly topologized A-module by extending the A-module structure of M^h to M* by uniform continuity. The universal mapping property of M*

follows immediately, continuous homomorphisms $f: M \to M'$ being uniformly continuous.

2. Let W be the set of Cauchy sequences in M, and make it an A-module by defining the addition and the scalar multiplication termwise. Then the set W_0 of the null sequences (i.e. the sequences which have zero as a limit) is a submodule of W. Put $M^* = W/W_0$, and define the canonical map $\varphi: M \to M^*$ in the obvious way. For any open submodule N of M, let $\hat{N}$ denote the image in M^* of the set of Cauchy sequences in N. Then $\hat{N}$ is a submodule of M^*. The set of all such $\hat{N}$ defines a linear topology in M^*, and $\hat{N}$ is the closure of $\varphi(N)$ in this topology. It is easy to see that M^* is complete and separated and has the universal mapping property.

3. Denote by M^* the inverse limit of the discrete A-modules M/M_n, where (M_n) is a filtration of M defining the topology, and put the inverse limit topology (i.e. the topology as a subspace of the product space $\prod(M/M_n)$ on it. Let $\varphi: M \to M^*$ be defined in the obvious way, and let M_n^* denote the closure of $\varphi(M_n)$ in M^*. Then M_n^* consists of those vectors of M^* of which the first n coordinates are zero, and the set of submodules $\{M_n^* \mid n = 1,2,..\}$ defines a complete separated linear topology on M^*. Let M' be an A-module with a complete separated linear topology and $f: M \to M'$ a continuous homomorphism. For any element $x^* = (\bar{x}_1, \bar{x}_2, \ldots)$ of M^* $(\bar{x}_n \in M/M_n)$, choose

a pre-image x_n of $\bar{x}_n$ in M for each n. Then the sequence $x_1, x_2, \ldots$ is a Cauchy sequence in M, hence the image sequence $f(x_1), f(x_2), \ldots$ is a Cauchy sequence in M'. Therefore $\lim_{n\to\infty} f(x_n)$ exists in M', and this limit is easily seen to be independent of the choice of the pre-images x_n. Putting $f^*(x^*) = \lim f(x_n)$ we obtain $f^*: M^* \to M'$ as wanted.

These constructions show that $\varphi: M \to M^*$ is injective if M is separated.

(23.I) If $f: M \to N$ is a continuous homomorphism of linearly topologized A-modules M and N, and if $\varphi_M: M \to M^*$ and $\varphi_N: N \to N^*$ are the canonical homomorphisms into the completions, then there exists a unique continuous homomorphism $f^*: M^* \to N^*$ with $\varphi_N f = f^* \varphi_M$; this is a formal consequence of the definition. The map f^* is called the completion of f. Taking completions is, therefore, an additive covariant functor.

PROPOSITION. Let M be a linearly topologized A-module, N a submodule and $\varphi: M \to M^*$ the canonical map to the completion. Then (i) the completion of N (for the topology induced from M) is the closure $\overline{\varphi(N)}$ of $\varphi(N)$ in M^*, and (ii) the quotient module $M^*/\overline{\varphi(N)}$ is the completion of the quotient module M/N.

<u>Proof</u>. (i) This follows, e.g., from the second construction

of completion in (23.H).

(ii) The quotient module $M^*/\overline{\varphi(N)}$ is separated by (23.B), and complete by (23.D). The canonical map $M \to M^*$ induces a map $M/N \to M^*/\overline{\varphi(N)}$, and the universal property of this map is easily proved by a formal argument.

Remark 1. Taking $N = M$ we see that $\varphi(M)$ is dense in M^*.

Remark 2. If N is an open submodule of M then M/N is discrete, hence complete and separated. Thus $M/N \simeq M^*/\overline{\varphi(N)}$.

THEOREM 54. Let A be a noetherian ring and I an ideal. Let $0 \to L \to M \to N \to 0$ be an exact sequence of finite A-modules, and let * denote the I-adic completion. Then the sequence $0 \to L^* \to M^* \to N^* \to 0$ is also exact.

Proof. By Artin-Rees theorem, the I-adic topology of L coincides with the topology induced by the I-adic topology of M. Therefore the assertion follows from the preceding proposition.

(23.J) Let A be a linearly topologized ring. Then the completion A^* of A is not only an A-module but also a ring, the multiplication in A being extended to A^* by continuity. If $\varphi: A \to A^*$ is the canonical map and I is an ideal of A, then the closure $\overline{\varphi(I)}$ of $\varphi(I)$ in A^* is an ideal of A^*. Thus A^*

is a linearly topologized ring. Example: Let k be a ring. Put $A = k[X_1,\dots,X_n]$ and $I = \sum_1^n AX_i$. Then the ring of formal power series $k[[X_1,\dots,X_n]]$ is the I-adic completion of A.

(23.K) Let A be a ring, I a finitely generated ideal of A, A^* the I-adic completion of A and $\varphi: A \to A^*$ the canonical map. Then, for any element x^* of A^* there exists a Cauchy sequence $(x_n) = (x_0, x_1, \dots)$ in A such that $x^* = \lim \varphi(x_n)$. Replacing (x_n) by a suitable subsequence we may assume that $x_{n+1} - x_n \in I^n$ $(n = 0,1,2,\dots)$. Let $a_1,\dots,a_m$ generate I, and put $a_i' = \varphi(a_i)$. Then $x_{n+1} - x_n$ is a homogeneous polynomial of degree n in $a_1,\dots,a_m$. Thus $x^* = \varphi(x_0) + \sum_{n=0}^{\infty} \varphi(x_{n+1} - x_n)$ has a power series expansion in $a_1',\dots,a_m'$. with coefficients in $\varphi(A)$. Consider the formal power series ring $A[[X]] = A[[X_1,\dots,X_m]]$; let $u(X) \in A[[X]]$, and let $\bar{u}(X)$ denote the power series obtained by applying φ to the coefficients of $u(X)$. Since A^* is complete and separated, the series $\bar{u}(a') = \bar{u}(a_1',\dots,a_m')$ converges in A^*. The map $u(X) \mapsto \bar{u}(a')$ defines a surjective homomorphism $A[[X]] \to A^*$. Thus $A^* \simeq A[[X]]/J$ with some ideal J of $A[[X]]$. As a consequence, A^* is noetherian if A is so.

(23.L) Let A be a ring, I an ideal and M an A-module. Let * denote the I-adic completion. Then M^* is an A^*-module in a natural way, therefore there exists a canonical map $M \otimes_A A^* \to M^*$.

THEOREM 55. When A is noetherian and M is finite over A, the map $M \otimes_A A^* \to M^*$ is an isomorphism.

Proof. Take an exact sequence of A-modules $A^p \xrightarrow{f} A^q \xrightarrow{g} M \to 0$. Since completion commutes with direct sum, we get a commutative diagram

$$\begin{array}{ccccccc} A^p \otimes A^* & \longrightarrow & A^q \otimes A^* & \longrightarrow & M \otimes A^* & \longrightarrow & 0 \\ \downarrow v_1 & & \downarrow v_2 & & \downarrow v_3 & & \\ (A^*)^p & \xrightarrow{f^*} & (A^*)^q & \xrightarrow{g^*} & M^* & \longrightarrow & 0 \end{array}$$

where the vertical arrows v_i are the canonical maps and the horizontal sequences are exact by the right-exactness of tensor product and by Th.54. Since v_1 and v_2 are isomorphisms v_3 is also an isomorphism by the Five-Lemma.

COROLLARY 1. Let A be a noetherian ring and I an ideal of A. Then the I-adic completion A* of A is flat over A.

COROLLARY 2. Let A and I be as above and assume that A is I-adically complete and separated. Let M be a finite A-module. Then M is complete and separated, and any submodule N of M is closed in M, for the I-adic topology.

Proof. Since A = A* we have $M^* = M \otimes A^* = M$, i.e. M is its own completion. Similarly, a submodule N is complete in the I-adic topology, which coincides with the induced topology by Artin-Rees. Since a complete subspace of M is necessarily closed, we are done.

COROLLARY 3. Let A be a noetherian ring, M a finite A-module, N a submodule of M and I an ideal of A. Let $\varphi : M \to M^*$ be the canonical map to the I-adic completion M*. Then we have $N^* \simeq \overline{\varphi(N)} = \varphi(N)A^*$, where $\overline{\varphi(N)}$ is the closure of $\varphi(N)$ in M*.

Proof. Immediate from Th.54 and Th.55.

COROLLARY 4. Let A and I be as in Cor.3. Then the topology of the I-adic completion A* of A is the IA*-adic topology.

Proof. By construction, the topology of A* is defined by the ideals $(\varphi(I^n) \text{ in } A^*) = I^n A^* = (IA^*)^n$.

COROLLARY 5. Let A, I and A* be as above and suppose that $I = \sum_1^m a_i A$. Then $A^* \simeq A[[X_1,\dots,X_m]]/(X_1 - a_1,\dots,X_n - a_m)$.

Proof. Put $B = A[X_1,\dots,X_m]$, $I' = \sum X_i B$ and $J = \sum (X_i - a_i)B$. Then $B/J \simeq A$, and the I'-adic topology on the B-algebra B/J corresponds to the I-adic topology on A. Denoting the I'-

adic completion by $\wedge$, we thus obtain

$$A^* \simeq (B/J)^\wedge = \hat{B}/\hat{J} = \hat{B}/J\hat{B} = A[[X_1,\dots X_m]]/(X_1 - a_1,\dots,X_m - a_m).$$

24. Zariski Rings

(24.A) DEFINITION. A Zariski ring is a noetherian ring equipped with an adic topology, such that every ideal is closed in it.

THEOREM 56. Let A be a noetherian ring with an adic topology, and let I be an ideal of definition. Then the following are equivalent.

(1) A is a Zariski ring;

(2) $I \subseteq \mathrm{rad}(A)$;

(3) every finite A-module M is separated in the I-adic topology;

(4) in every finite A-module M, every submodule is closed in the I-adic topology;

(5) the completion A* of A is faithfully flat over A.

Proof. (1) $\Rightarrow$ (2): Suppose that a maximal ideal $\mathfrak{m}$ does not contain I. Then $I^n \not\subseteq \mathfrak{m}$ for all n > 0, so that $\mathfrak{m} + I^n = A$ and $\bigcap_n(\mathfrak{m} + I^n) = A \neq \mathfrak{m}$. Therefore $\mathfrak{m}$ is not closed, contradiction. (2) $\Rightarrow$ (3): By the intersection theorem (11.D). (3) $\Rightarrow$ (4): If N is a submodule of M, then M/N is separated by assumption so that N is closed in M. (4) $\Rightarrow$ (1) Trivial. (2) $\Rightarrow$ (5) Let $\mathfrak{m}$ be a maximal ideal of A. Then $\mathfrak{m} \supseteq I$, hence $\mathfrak{m}$ is open in A and so $A^*/\mathfrak{m}A^* \simeq A/\mathfrak{m}$. Thus $\mathfrak{m}A^* \neq A^*$. Since A* is flat over A by (23.L) Cor.1, this implies by (4.A) Th.2 that A* is f.f. over A.

(5) $\Rightarrow$ (2) If $\mathfrak{m}$ is a maximal ideal of A then there exists, by assumption, a maximal ideal $\mathfrak{m}'$ of A* lying over $\mathfrak{m}$. Since $IA^* \subseteq \mathfrak{m}'$ by (23.G), we have $I \subseteq IA^* \cap A \subseteq \mathfrak{m}' \cap A = \mathfrak{m}$, Q.E.D.

COROLLARY. Let A be a Zariski ring and A* its completion. Then (1) A is a subring of A*, and (2) the map $\mathfrak{m} \mapsto \mathfrak{m}A^*$ is a bijection from the set $\Omega(A)$ of all maximal ideals in A to $\Omega(A^*)$, and we have $A/\mathfrak{m} \simeq A^*/\mathfrak{m}A^*$ and $\mathfrak{m}A^* \cap A = \mathfrak{m}$.

(24.B) A noetherian semi-local ring is a Zariski ring. A noetherian ring with an adic topology which is complete and separated is also a Zariski ring.

Let A be an arbitrary noetherian ring and I a proper ideal of A. Put $S = 1 + I = \{1+x \mid x \in I\}$, $A' = S^{-1}A$ and $I' = S^{-1}I$. Then all elements of $1 + I'$ are invertible in A', and so $I' \subseteq \mathrm{rad}(A')$. We equip A with the I-adic topology and A' with the I'-adic (or what is the same, the I-adic) topology. Then the canonical map $\psi: A \to A'$ is continuous, and has the universal mapping property for continuous homomorphisms from A to Zariski rings. In fact, if $f: A \to B$ is such a homomorphism and if J is an ideal of definition for B, then $f(I^n) \subseteq J \subseteq \mathrm{rad}(B)$ for some n, hence $f(I) \subseteq \mathrm{rad}(B)$ and the elements of f(S) are invertible in B. Therefore f factors through A'. In particular, the canonical map $A \to A^*$ of A into the completion A* of A factors through A', and it follows immediately that A* is also the completion of A'.

For a prime ideal p of A, we have $p \cap S = \emptyset$ iff $p + I \neq (1)$, i.e. iff $V(p) \cap V(I) \neq \emptyset$. The localization $A \to A'$ has, geometrically, the effect of considering only the "subvarieties" of Spec(A) which intersect the closed set V(I). Since A* is faithfully flat over A', the set $\{p \in \mathrm{Spec}(A) \mid p + I \neq (1)\}$ (≈ Spec(A)) is also the image of Spec(A*) in Spec(A). The set of the maximal ideals of A* (resp. the prime ideals of A* containing IA*) is in a natural 1-1 correspondence with the set of the maximal ideals (resp. prime ideals) of A containing I.

(24.C) Let A be a semi-local ring and $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ be its maximal ideals. Put $A_i = A_{\mathfrak{m}_i}$, $\mathfrak{m}_i' = \mathfrak{m}_i A_i$ $(i = 1, \ldots, r)$, and $\mathfrak{m} = \mathrm{rad}(A) = \mathfrak{m}_1 \ldots \mathfrak{m}_r$. Then $\mathfrak{m}^n = \prod \mathfrak{m}_i^n = \bigcap \mathfrak{m}_i^n$, hence $A/\mathfrak{m}^n = A/\mathfrak{m}_1^n \times \ldots \times A/\mathfrak{m}_r^n$ by (1.C). Moreover, $A/\mathfrak{m}_i^n \simeq A_i/\mathfrak{m}_i'^n$ as $A/\mathfrak{m}_i^n$ is a local ring. Therefore

$$A^* = \varprojlim A/\mathfrak{m}^n = A_1^* \times \ldots \times A_r^*.$$

(24.D) Let $(A, \mathfrak{m})$ be a noetherian local ring and A* its completion. Then $A/\mathfrak{m}^n \simeq A^*/\mathfrak{m}^n A^*$ for all $n > 0$, hence $\mathfrak{m}^n/\mathfrak{m}^{n+1} \simeq \mathfrak{m}^n A^*/\mathfrak{m}^{n+1} A^*$ and $\mathrm{gr}(A) \simeq \mathrm{gr}(A^*)$. It follows that i) dim A = dim A*, and ii) A is regular iff A* is so.

Next, let A be an arbitrary noetherian ring, I an ideal of A and A* the I-adic completion of A. Let p be a prime ideal of A containing I. Since p is open in A, the ideal $pA^* = p^*$ is open and prime in A* and $A/p^n \simeq A^*/p^{*n}$ for all $n > 0$. Localizing both sides with respect to p/p^n and p^*/p^{*n} respectively, we get

$$A_p/p^n A_p \simeq A^*_{p^*}/p^{*n} A^*_{p^*}.$$

Therefore $(A_p)^* = \varprojlim A_p/p^n A_p \simeq (A^*_{p^*})^*$. Two local rings are said to be <u>analytically isomorphic</u> if their completions are isomorphic. Thus, if p and p^* are corresponding open prime ideals of A and A*, then the local rings A_p and $A^*_{p^*}$ are analytically isomorphic. Since all maximal ideals of A* are open, it follows that

i') $\dim A^* = \sup_{p \supseteq I} \dim A_p$,

ii') if A_p is regular for every prime ideal p containing I, then A* is regular.

As a corollary of ii') we have the following

PROPOSITION. Let A be a regular noetherian ring. Then the ring of formal power series $A[[X_1,\ldots,X_m]]$ is also regular.

Proof. $A[X] = A[X_1,\ldots,X_m]]$ is a regular ring by (17.J), and $A[[X]]$ is the $\Sigma X_i A[X]$-adic completion of $A[X]$.

(24.E) PROPOSITION. Let A be a Zariski ring and A^* its completion. Then:

i) If $\mathfrak{a}$ is an ideal of A and if $\mathfrak{a}A^*$ is principal, then $\mathfrak{a}$ itself is principal.

ii) If A^* is normal, then A is also normal.

Proof. i) Suppose $\mathfrak{a}A^* = \alpha A^*$, $\alpha \in A^*$. Then $\alpha = \Sigma a_i \xi_i$ with $a_i \in \mathfrak{a}$, $\xi_i \in A^*$. Put $I^* = IA^*$, where I is an ideal of definition of A. By Artin-Rees we have $\alpha A^* \cap I^{*n} \subseteq I^*\alpha A^*$ for n sufficiently large. Take $x_i \in A$ such that $x_i \equiv \xi_i$ (I^{*n}) and put $a = \Sigma a_i x_i$. Then $a \equiv \alpha$ (I^{*n}), and $a \in \mathfrak{a} \subseteq \alpha A^*$. Therefore $\alpha = a + \beta$ with $\beta \in \alpha A^* \cap I^{*n} \subseteq I^* \alpha A^*$, hence $\alpha A^* \subseteq aA^* + I^*\alpha A^*$, and by NAK we get $\alpha A^* = aA^*$. Then $\mathfrak{a} = \alpha A^* \cap A = aA^* \cap A = aA$.

ii) is a consequence of faithful flatness and was already proved in (21.E.iii).

We shall see in Part II that noetherian local (or semi-local) rings have many good properties.

PART II

CHAPTER 10. DERIVATION

25. Extension of a Ring by a Module

(25.A) Let C be a ring and N an ideal of C with $N^2 = (0)$; put $C' = C/N$. Then the C-module N can be viewed as a C'-module. Conversely, suppose that we are given a ring C' and a C'-module N. By an <u>extension of C' by N</u> we mean a triple (C,ε,i) of a ring C, a surjective homomorphism of rings $\varepsilon: C \to C'$ and a map $i: N \to C$, such that: (1) $\mathrm{Ker}(\varepsilon)$ is an ideal whose square is zero (hence a structure of C'-module on $\mathrm{Ker}(\varepsilon)$), and (2) the map i is an isomorphism from N onto $\mathrm{Ker}(\varepsilon)$ as C'-modules. Therefore, identifying N with i(N) we get $C' \simeq C/N$, $N^2 = (0)$. An extension is often represented by the exact sequence $0 \to N \xrightarrow{i} C \xrightarrow{\varepsilon} C' \to 0$. Two extensions (C, ε, i) and $(C_1, \varepsilon_1, i_1)$ are said to be isomorphic if there exists a ring homomorphism $f: C \to C_1$ such that $\varepsilon_1 f = \varepsilon$

and $fi = i_1$. Such f is necessarily unique.

(25.B) Given C' and N we can always construct an extension as follows: take the additive group $C' \oplus N$, and define a multiplication in this set by the formula

$$(a, x)(b, y) = (ab, ay + bx) \quad (a,b \in C'; x,y \in N).$$

This is bilinear and associative, and has (1,0) as the unit element. Hence we get a ring structure on $C' \oplus N$. We denote this ring by $C'*N$. By the obvious definitions $\varepsilon(a,x) = a$ and $i(x) = (0,x)$ the ring $C'*N$ becomes an extension of C' by N, which is called the <u>trivial extension</u>.

An extension (C, ε, i) of C' by N is isomorphic to $C'*N$ iff there exists a section, i.e. a ring homomorphism $s: C' \to C$ satisfying $\varepsilon s = id_{C'}$. In this case the extension (C, ε, i) is also said to be trivial, or to be split.

(25.C) Let us briefly mention the Hochschild extensions. An extension (C, ε, i) is called a Hochschild extension if the exact sequence of additive groups $0 \to N \xrightarrow{i} C \xrightarrow{\varepsilon} C' \to 0$ splits, i.e. if there exists an additive map $s: C' \to C$ such that $\varepsilon s = id_{C'}$. Then C is isomorphic to $C' \oplus N$ as additive group, while the multiplication is given by

$$(a,x)(b,y) = (ab, ay + bx + f(a,b)) \quad (a,b \in C'; x,y \in N)$$

where the map $f: C' \times C' \to N$ is symmetric and bilinear and

satisfies the cocycle condition (corresponding to the associativity in C)

$$af(b,c) - f(ab,c) + f(a,bc) - f(a,b)c = 0.$$

Conversely, any such function f(a,b) gives rise to a Hochschild extension. Moreover, the extension is trivial iff there exists a function $g: C' \to N$ satisfying

$$f(a,b) = ag(b) - g(ab) + g(a)b.$$

(25.D) Let A be a ring, and let $0 \to N \xrightarrow{i} C \xrightarrow{\varepsilon} C' \to 0$ be an extension of a ring C' by a C'-module N such that C and C' are A-algebras and ε is a homomorphism of A-algebras. Then C is called an extension of the A-algebra C' by N. The extension is said to be A-trivial, or to split over A, if there exists a homomorphism of A-algebras $s: C' \to C$ with $\varepsilon s = id_{C'}$.

(25.E) Let E: $0 \to M \xrightarrow{i} C \xrightarrow{\varepsilon} C' \to 0$ be an extension and let $g: M \to N$ be a homomorphism of C'-modules. Then there exists an extension $g_*(E)$: $0 \to N \to D \to C' \to 0$ of C' by N and a ring homomorphism $f: C \to D$ such that

$$\begin{array}{ccccccccc} 0 & \to & M & \to & C & \to & C' & \to & 0 \\ & & \downarrow g & & \downarrow f & & \downarrow id & & \\ 0 & \to & N & \to & D & \to & C' & \to & 0 \end{array}$$

is commutative. Such an extension $g_*(E)$ is unique up to isomorphisms. The ring D is obtained as follows: we view the

C'-module N as a C-module and form the trivial extension $C*N$. Then $M' = \{(x,-g(x)) \mid x \in M\}$ is an ideal of $C*N$, and we put $D = (C*N)/M'$. Thus, as an additive grou D is the amalgamated sum of C and N with respect to M. The uniqueness of $g_*(E)$ follows from this construction.

Similarly, if $h\colon C'' \to C'$ is a ring homomorphism then there exists an extension $h^*(E)\colon 0 \to M \to E \to C'' \to 0$ of C'' by M and a ring homomorphism $f\colon E \to C$ such that the diagram

$$\begin{array}{ccccccccc} 0 & \to & M & \to & E & \to & C'' & \to & 0 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle h} & & \\ 0 & \to & M & \to & D & \to & C' & \to & 0 \end{array}$$

is commutative. Moreover, such $h^*(E)$ is unique up to isomorphisms.

26. Derivations and Differentials

(26.A) Let A be a ring and M an A-module. A derivation D of A into M is defined as usual: it is an additive map from A to M satisfying $D(ab) = aDb + bDa$. The set of all derivations of A into M is denoted by $\mathrm{Der}(A,M)$; it is an A-module in the natural way.

For any derivation D, $D^{-1}(0)$ is a subring of A (in particular, $D(1) = 0$: this follows from $1^2 = 1$.) If A is a field, then $D^{-1}(0)$ is a subfield.

Let k be a ring and A a k-algebra. Then derivations $A \to M$ which vanish on $k \cdot 1_A$ are called <u>derivations over k</u>. The set of such derivations is denoted by $\mathrm{Der}_k(A, M)$. We write $\mathrm{Der}_k(A)$ for $\mathrm{Der}_k(A, A)$.

Suppose that A is a ring whose characteristic is a prime number p, and let A^p denote the subring $\{a^p \mid a \in A\}$. Then any derivation $D\colon A \to M$ vanishes on A^p, for $D(a^p) = pa^{p-1}D(a) = 0$.

(26.B) Let A and C be rings and N an ideal of C with $N^2 = 0$. Let $j\colon C \to C/N$ be the natural map. Let $u, u'\colon A \to C$ be two homomorphisms (of rings) satisfying $ju = ju'$, and put $D = u' - u$. Then u and u' induce the same A-module structure on N, and $D\colon A \to N$ is a derivation. In fact, we have

$$\begin{aligned} u'(ab) = u'(a)u'(b) &= (u(a) + D(a))(u(b) + D(b)) \\ &= u(ab) + aD(b) + bD(a). \end{aligned}$$

Conversely, if $u\colon A \to C$ is a homomorphism and $D\colon A \to N$ is a derivation (with respect to the A-module structure on N induced by u), then $u' = u + D$ is a homomorphism.

(26.C) Let k be a ring, A a k-algebra and $B = A \otimes_k A$. Consider the homomorphisms of k-algebras

$$\varepsilon\colon B \to A \quad \text{and} \quad \lambda_1, \lambda_2\colon A \to B$$

defined by $\varepsilon(a \otimes a') = aa'$, $\lambda_1(a) = a \otimes 1$, $\lambda_2(a) = 1 \otimes a$.

Once and for all, we make $B = A\otimes A$ an A-algebra via λ_1. We denote the kernel of ε by $I_{A/k}$ or simply by I, and we put $I/I^2 = \Omega_{A/k}$. The B-modules I, I^2 and $\Omega_{A/k}$ are also viewed as A-modules via $\lambda_1: A \to B$. Then the A-module $\Omega_{A/k}$ is called the module of differentials (or of Kähler differentials) of A over k.

We have $\varepsilon\lambda_1 = \varepsilon\lambda_2 = id_A$. Therefore, if we denote the natural homomorphism $B \to B/I^2$ by ν and if we put $d^* = \lambda_2 - \lambda_1$ and $d = \nu d^*$, then we get a derivation $d: A \to \Omega_{A/k}$. Note that we have $B = \lambda_1(A) \oplus I$, hence $B/I^2 = \nu\lambda_1(A) \oplus \Omega_{A/k}$ (as A-module). Identifying $\nu\lambda_1(A)$ with A, we get

$$B/I^2 = A \oplus \Omega_{A/k}.$$

In other words, B/I^2 is a trivial extension of A by $\Omega_{A/k}$.

PROPOSITION. The pair $(\Omega_{A/k}, d)$ has the following universal property: if D is a derivation of A over k into an A-module M, then there is a unique A-linear map $f: \Omega_{A/k} \to M$ such that $D = fd$.

Proof. In $B = A\otimes A$ we have $x\otimes y = xy\otimes 1 + x(1\otimes y - y\otimes 1) = \varepsilon(x\otimes y) + xd^*y$. Therefore, if $\Sigma x_i\otimes y_i \in I = Ker(\varepsilon)$ then $\Sigma x_i\otimes y_i = \Sigma x_i d^*y_i$. Since $d^*y \bmod I^2 = dy$, any element of $\Omega = I/I^2$ has the form $\Sigma x_i dy_i$ $(x_i, y_i \in A)$. In other words, Ω is generated by $\{dy \mid y \in A\}$ as A-module. This proves the uniqueness of f. As for the existence of f, take the trivial extension $A*M$ and define a homomorphism of A-algebras $\phi: B = A\otimes_k A \to A*M$ by $\phi(x\otimes y) = (xy, xD(y))$. Since $\phi(I) \subseteq M$ and $M^2 = 0$, we have $\phi(I^2) = 0$ so that ϕ induces a homomorphism $\bar\phi$ of A-algebras $B/I^2 = A*\Omega \to A*M$ which maps $dy \in \Omega$ to $\phi(d^*y) = \phi(1\otimes y - y\otimes 1) = (0, Dy)$. Thus the restriction of $\bar\phi$ to Ω gives an A-linear map $f: \Omega \to M$ with $f\circ d = D$. Q.E.D.

As a consequence of the proposition we get a canonical isomorphism of A-modules

$$Der_k(A, M) \simeq Hom_A(\Omega_{A/k}, M).$$

In the categorical language, the pair $(\Omega_{A/k}, d)$ represents the covariant functor $M \mapsto Der_k(A, M)$ from the category of A-modules into itself. The map $d: A \to \Omega_{A/k}$ is called the canonical derivation and is denoted by $d_{A/k}$ if necessary.

(26.D) Any ring A is a $\mathbb{Z}$-algebra in a unique way. The module $\Omega_{A/\mathbb{Z}}$ is simply written Ω_A. If A contains a field k and if F is the prime field in k, then $\Omega_{A/F} = \Omega_A$ because $A\otimes_{\mathbb{Z}} A = A\otimes_F A$.

The r-th exterior product $\bigwedge^r\Omega_{A/k}$ is denoted by $\Omega^r_{A/k}$ and is called the module of differentials of degree r. In this notation we have $\Omega_{A/k} = \Omega^1_{A/k}$.

(26.E) Example 1. Let k be a ring, and let A be a k-algebra which is generated by a set of elements $\{x_\lambda\}$ over k. Then $\Omega_{A/k}$ is generated by $\{dx_\lambda\}$ as A-module. This is clear since d is a derivation.

In particular, if A is a polynomial ring over the ring k in an arbitrary number of indeterminates $\{X_\lambda\}$: $A = k[..,X_\lambda,..]$, then $\Omega_{A/k}$ is a free A-module with $\{dX_\lambda\}$ as a basis. In fact, suppose $\Sigma P_\lambda dX_\lambda = 0$ $(P_\lambda \in A)$ and let $\partial/\partial X_\lambda$ denote the partial derivations. Then $\partial/\partial X_\lambda \in \mathrm{Der}_k(A)$, hence there exists a linear map $f: \Omega_{A/k} \to A$ such that $f(dX_\mu) = \partial X_\mu/\partial X_\lambda = \delta_{\lambda\mu}$. Applying f to $\Sigma P_\mu dX_\mu = 0$ we find $P_\lambda = 0$. As λ is arbitrary we see that the dX_λ's are linearly independent over A. Q.E.D. (Note that $\mathrm{Der}_k(A) = \mathrm{Hom}_A(\Omega_{A/k}, A) \simeq \prod_\lambda A_\lambda$, where $A_\lambda \simeq A$.)

(26.F) Example 2. Let k be a field of characteristic $p > 0$, and let k' be a subfield such that $k = k'(t)$, $t^p = a \in k'$, $t \notin k'$. Then $k = k'[X]/(X^p - a)$, and since $\partial(X^p - a)/\partial X = 0$ the derivation $\partial/\partial X$ of $k'[X]$ maps the ideal $(X^p - a)k'[X]$ into itself. It thus induces a derivation D of k over k' such that $D(t) = 1$.

Next, let k' be an arbitrary subfield such that $k^p \subseteq k' \subseteq k$. A family of elements (x_λ) of k is said to be p-independent over k' if, for any finite subset $\{x_{\lambda_1},\dots,x_{\lambda_n}\}$, we have $[k'(x_{\lambda_1},\dots,x_{\lambda_n}) : k'] = p^n$. A family (x_λ) is called a p-basis of k over k' if it is p-independent over k' and if $k'(\dots,x_\lambda,\dots) = k$. The existence of a p-basis of k over k' can be easily proved by Zorn's lemma. Moreover, any p-indep. family over k' can be extended to a p-basis. Suppose that we are given a p-basis (x_λ). Then $\Omega_{k/k'}$ is a free k-module with (dx_λ) as a basis. In fact, putting $k'_\lambda = k'(\{x_\mu \mid \mu \neq \lambda\})$ we have $k'_\lambda(x_\lambda) = k$, $x_\lambda{}^p \in k'_\lambda$ and $x_\lambda \notin k'_\lambda$, so there exists a derivation D_λ of k over k'_λ such that $D_\lambda(x_\lambda) = 1$. Therefore $D_\lambda \in \mathrm{Der}_{k'}(k)$ and $D_\lambda(x_\mu) = \delta_{\lambda\mu}$. From this we conclude the linear independence of the dx_λ's as in Example 1.

If $k^p \subseteq k' \subseteq k$ and $[k : k'] = p^m < \infty$, then $\Omega_{k/k'}$ and $\mathrm{Der}_{k'}(k)$ are vector spaces of rank m, dual to each other.

In general, if k' is an arbitrary subfield of k and $x_1, \dots, x_n \in k$, then the differentials $dx_1,\dots,dx_n$ in $\Omega_{k/k'}$ are linearly independent over k iff the family (x_i) is p-indep. over $k'(k^p)$. Proof is left to the reader.

(26.G) Example 3. Let k be a field and K a separable algebraic extension field of k. Then $\Omega_{K/k} = 0$. In fact, for any $\alpha \in K$ there is a polynomial $f(X) \in k[X]$ such that $f(\alpha) = 0$ and $f'(\alpha) \neq 0$. Since $d: K \to \Omega_{K/k}$ is a derivation we have $0 = d(f(\alpha)) = f'(\alpha)d\alpha$, whence $d\alpha = 0$. As $\Omega_{K/k}$ is generated by the $d\alpha$'s we get $\Omega_{K/k} = 0$.

Exercises.

1) If $\begin{array}{ccc} A & \longrightarrow & A' \\ \uparrow & & \uparrow \\ k & \longrightarrow & k' \end{array}$ is a commutative diagram of rings and

homomorphisms, then there is a natural homomorphism of A-modules $\Omega_{A/k} \to \Omega_{A'/k'}$, hence also a natural homomorphism of A'-modules $\Omega_{A/k} \otimes_A A' \to \Omega_{A'/k'}$.

2) If $A' = A \otimes_k k'$ in 1), then the last homomorphism is an isomorphism: $\Omega_{A'/k'} = \Omega_{A/k} \otimes_k k' = \Omega_{A/k} \otimes_A A'$.

3) If S is a multiplicative set in a k-algebra A and if $A' = S^{-1}A$, then $\Omega_{A'/k} = \Omega_{A/k} \otimes_A A' = S^{-1}\Omega_{A/k}$.

(26.H) THEOREM 57. (The first fundamental exact sequence) Let k, A and B be rings and let $k \xrightarrow{\phi} A \xrightarrow{\psi} B$ be homomorphisms. Then i) there is an exact sequence of natural homomorphisms of B-modules

$$\Omega_{A/k} \otimes_A B \xrightarrow{v} \Omega_{B/k} \xrightarrow{u} \Omega_{B/A} \to 0 ;$$

ii) the map v has a left inverse (or what amounts to the same, v is injective and Im(v) is a direct summand of $\Omega_{B/A}$ as B-module) iff any derivation of A over k into any B-module T can be extended to a derivation $B \to T$.

Proof. i) The map v is defined by $v(d_{A/k}(a) \otimes b) = b \cdot d_{B/k}\psi(a)$, and the map u by $u(b \cdot d_{B/k}(b')) = b \cdot d_{B/A}(b'))$ ($a \in A$; $b, b' \in B$). It is clear that u is surjective. Since $d_{B/A}\psi(a)) = 0$ we have $uv = 0$. It remains to prove that $\mathrm{Ker}(u) = \mathrm{Im}(v)$. To do this, it is enough to show that

$$\mathrm{Hom}_B(\Omega_{A/k} \otimes_A B,\ T) \leftarrow \mathrm{Hom}_B(\Omega_{B/k},\ T) \leftarrow \mathrm{Hom}_B(\Omega_{B/A},\ T)$$

is exact for any B-module T (take $T = \mathrm{Coker}(v)$). But we have canonical isomorphisms $\mathrm{Hom}_B(\Omega_{A/k} \otimes_A B,\ T) \simeq \mathrm{Hom}_A(\Omega_{A/k},\ T) \simeq \mathrm{Der}_k(A,\ T)$ etc., so we can identify the last sequence with

$$\mathrm{Der}_k(A,T) \leftarrow \mathrm{Der}_k(B,T) \leftarrow \mathrm{Der}_A(B,T)$$

where the first arrow is the map $D \mapsto D \circ \psi$. This sequence is exact by the definitions.

ii) A homomorphism of B-modules $M' \to M$ has a left inverse iff the induced map $\mathrm{Hom}_B(M',T) \leftarrow \mathrm{Hom}_B(M,T)$ is surjective for any B-module T. Thus, v has a left inverse iff the natural map $\mathrm{Der}_k(A,T) \leftarrow \mathrm{Der}_k(B,T)$ is surjective for any B-module T. Q.E.D.

COROLLARY. The map $v: \Omega_{A/k} \otimes_A B \to \Omega_{B/k}$ is an isomorphism iff any derivation of A over k into any B-module T can be extended uniquely to a derivation $B \to T$.

(26.I) Let k be a ring, A a k-algebra, $\mathfrak{m}$ an ideal of A and $B = A/\mathfrak{m}$. Define a map $\mathfrak{m} \to \Omega_{A/k} \otimes_A B$ by $x \mapsto d_{A/k}x \otimes 1$ ($x \in \mathfrak{m}$). It sends $\mathfrak{m}^2$ to 0, hence induces a B-linear map $\delta: \mathfrak{m}/\mathfrak{m}^2 \to \Omega_{A/k} \otimes_A B$.

THEOREM 58 (The second fundamental exact sequence). Let the notation be as above.

i) The sequence of B-modules

$$(*)\quad \mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\delta} \Omega_{A/k}\otimes_A B \xrightarrow{v} \Omega_{B/k} \to 0$$

is exact.

ii) Put $A_1 = A/\mathfrak{m}^2$. Then $\Omega_{A/k}\otimes_A B \simeq \Omega_{A_1/k}\otimes_{A_1} B$.

iii) The homomorphism δ has a left inverse iff the extension $0 \to \mathfrak{m}/\mathfrak{m}^2 \to A_1 \to B \to 0$ of the k-algebra B by $\mathfrak{m}/\mathfrak{m}^2$ is trivial over k.

<u>Proof</u>. i) The surjectivity of v follows from that of $A \to B$. Obviously the composite $v\delta = 0$. So, as in the proof of the preceding theorem, it is enough to prove the exactness of

$$\mathrm{Hom}_B(\mathfrak{m}/\mathfrak{m}^2, T) \leftarrow \mathrm{Hom}_B(\Omega_{A/k}\otimes_A B, T) \leftarrow \mathrm{Hom}_B(\Omega_{B/A}, T)$$

for any B-module T. But we can rewrite it as follows:

$$\mathrm{Hom}_A(\mathfrak{m}, T) \leftarrow \mathrm{Der}_k(A, T) \leftarrow \mathrm{Der}_k(A/\mathfrak{m}, T)$$

where the first arrow is the map $D \mapsto D|\mathfrak{m}$ ($D \in \mathrm{Der}_k(A, T)$). Then the exactness is obvious.

ii) A homomorphism of B-modules $N' \to N$ is an isomorphism iff the induced map $\mathrm{Hom}_B(N',T) \leftarrow \mathrm{Hom}_B(N,T)$ is an isomorphism for every B-module T. Applying this to the present situation we are led to prove that the natural map $\mathrm{Der}_k(A,T) \leftarrow \mathrm{Der}_k(A/\mathfrak{m}^2, T)$ is an isomorphism for every $A/\mathfrak{m}$-module T, which is obvious.

iii) By ii) we may replace A by A_1 in (*), so we assume $\mathfrak{m}^2 = 0$. Suppose that δ has a left inverse $w: \Omega_{A/k}\otimes_A B \to \mathfrak{m}$. Putting $Da = w(da\otimes 1)$ for $a \in A$ we obtain a derivation $D: A \to \mathfrak{m}$ over k such that $Dx = x$ for $x \in \mathfrak{m}$. Then the map

$f: A \to A$ given by $f(a) = a - Da$ is a homomorphism of k-algebras and satisfies $f(\mathfrak{m}) = 0$, hence induces a homomorphism $\bar{f}: B = A/\mathfrak{m} \to A$. Since $f(a) \equiv a \bmod \mathfrak{m}$, the homomorphism $\bar{f}$ is a section of the ring extension $0 \to \mathfrak{m} \to A \to B \to 0$. The converse is proved by reversing the argument.

(26.J) <u>Example</u>. Let k be a ring, A a k-algebra and $B = A[X_1, \dots, X_n]$. Let T be an arbitrary B-module and let $D \in \mathrm{Der}_k(A,T)$. Then we can extend it to a derivation $B \to T$ by putting $D(P(X)) = P^D(X)$, where P^D is obtained from P(X) by applying D to the coefficients. Thus the natural map $\Omega_{A/k}\otimes_A B \to \Omega_{B/k}$ has a left inverse, and we have

$$\Omega_{B/k} \simeq (\Omega_{A/k}\otimes_A B) \oplus BdX_1 \oplus \dots \oplus BdX_n.$$

Let $\mathfrak{m}$ be an ideal of $B = A[X_1,\dots,X_n]$, and put $C = B/\mathfrak{m}$, $x_i = X_i \bmod \mathfrak{m}$. Then we have the second fundamental exact sequence

$$\mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\delta} \Omega_{B/k}\otimes_B C = (\Omega_{A/k}\otimes_A C) \oplus \Sigma CdX_i \to \Omega_{C/k} \to 0$$

with

$$\delta(P(X)) = (dP)(x) + \sum_{i=1}^{n} \partial P/\partial X_i(x)dX_i \qquad (P(X) \in \mathfrak{m}),$$

where $(dP)(x)$ is obtained by applying $d_{A/k}$ to the coefficients of P(X) and then reducing the result modulo $\mathfrak{m}$.

Exercise 4. Let $B = k[X,Y]/(Y^2 - X^3) = k[x,y]$ (= the affine ring of the plane curve $y^2 = x^3$, which has a cusp at the origin). Calculate $\Omega_{B/k}$, and show that it is a B-module with torsion.

27. Separability

(27.A) Let k be a field and K an extension[1] of k. A transcendency basis $\{x_\lambda\}_{\lambda\in\Lambda}$ of K over k is called a separating transcendency basis if K is separably algebraic over the field $k(\ldots,x_\lambda,\ldots)$. We say that K is separably generated over k if it has a separating transcendency basis.

Put $r(K) = \mathrm{rank}_K\, \Omega_{K/k}$. Let L be a finitely generated extension of K. We want to compare r(L) and r(K). Suppose first that L = K(t). There are four typical cases.

Case 1. t is transcendental over K. Then $\Omega_{K[t]/k} = (\Omega_{K/k}\otimes_K K[t])\oplus K[t]dt$ by (26.J), so by localization we get $\Omega_{L/k} = (\Omega_{K/k}\otimes_K L)\oplus Ldt$, hence $r(L) = r(K) + 1$.

Case 2. t is separably algebraic over K. Let f(X) be the irreducible equation of t over K. Then $L = K[t] = K[X]/(f)$, $f(t) = 0$ and $f'(t) \neq 0$. By (26.J) we have $\Omega_{L/k} = ((\Omega_{K/k}\otimes_K L + LdX)/L\delta f$, where $\delta f = (df)(t) + f'(t)dX$ in the notation of (26.J). As f'(t) is invertible in L we have $\Omega_{K/k}\otimes_K L \simeq \Omega_{L/k}$. Whence r(L) = r(K). From this, or by a direct computation, one sees that any derivation of K into L can be extended uniquely to a derivation of L.

Case 3. $ch(k) = p$, $t^p = a \in K$, $t \notin K$, $d_{K/k}(a) = 0$. Then $L = K[t] = K[X]/(X^p - a)$. We have $\delta(X^p - a) = 0$, therefore $\Omega_{L/k} \simeq \Omega_{K[X]/k}\otimes L \simeq (\Omega_{K/k}\otimes_K L)\oplus Ldt$ and $r(L) = r(K) + 1$.

Case 4. Same as in case 3 with the exception that $d_{K/k}a \neq 0$. Then $\delta(X^p - a) \neq 0$, and so $r(L) = r(K)$.

1) By an extension of a field we mean an extension field; by a finite extension, a finite algebraic extension.

(27.B) THEOREM 59. i) Let k be a field, K an extension of k and L a finitely generated extension of K. Then

$$\mathrm{rank}_L\, \Omega_{L/k} \geqslant \mathrm{rank}_K\, \Omega_{K/k} + \mathrm{tr.deg}_K L.$$

ii) The equality holds in i) if L is separably generated over K.

iii) Let L be a finitely generated extension of a field k. Then $\mathrm{rank}_L\, \Omega_{L/k} \geqslant \mathrm{tr.deg}_k L$, where the equality holds iff L is separably generated over k. In particular, $\Omega_{L/k} = 0$ iff L is separably algebraic over k.

Proof. Since any finitely generated extension of K is obtained by repeating extensions of the four types just discussed, the assertions i) and ii) are now obvious. As for iii), the inequality is a special case of i). Suppose that $\Omega_{L/k} = 0$, i.e. that r(L) = 0. Then r(K) = 0 for any $k \subseteq K \subseteq L$. Therefore the cases 1,3 and 4 of (27.A) cannot happen for L and K. This means that L is separably algebraic over k. Suppose, next, that $r(L) = \mathrm{tr.deg}_k L = r$. Let $x_1,\ldots,x_r \in L$ be such that $\{dx_1,\ldots,dx_r\}$ is a basis of $\Omega_{L/k}$ over L. Then we have

$\Omega_{L/k(x_1,\ldots,x_r)} = 0$ by Th.57, so L is separably algebraic over $k(x_1,\ldots,x_r)$. Since $r = \text{tr.deg}_k L$ the elements x_i must form a transcendency basis of L over k.

Remark. Let $L = k(x_1,\ldots,x_n)$ and $\text{tr.deg}_k L = r$, and put $p = \{f(X) \in k[X_1,\ldots,X_n] \mid f(x_1,\ldots,x_n) = 0\}$. Let $f_1,\ldots,f_s$ generate the ideal p. Then L is separably generated over k iff the Jacobian matrix $\partial(f_1,\ldots,f_s)/\partial(x_1,\ldots,x_n)$ has rank $n - r$, as one can easily check. If this is the case, and if the minor determinant $\partial(f_1,\ldots,f_{n-r})/\partial(x_{r+1},\ldots,x_n) \neq 0$, then $dx_1,\ldots,dx_r$ form a basis of $\Omega_{L/k}$, and the above proof shows that $\{x_1,\ldots,x_r\}$ is a separating transcendency basis of L/k.

(27.C) LEMMA 1. Let k be a field and K an algebraic extension of k. Then the following are equivalent:

(1) K is separably algebraic over k;

(2) the ring $K \otimes_k k'$ is reduced for any extension k' of k;

(3) ditto for any algebraic extension k' of k;

(4) ditto for any finite extension k' of k.

Proof. Each of these properties holds iff it holds for any finite extension K' of k contained in K. So we may assume that $[K : k] < \infty$.

(1) $\Rightarrow$ (2): If K is finite and separable over k then $K = k(t)$ with some $t \in K$. Let f(X) be the irreducible equation of t over k. Then $K \simeq k[X]/(f)$, hence $K \otimes k' \simeq k'[X]/(f)$, and since f(X) has no multiple factors in k'[X] (because it decomposes into distinct linear factors in $\bar{k}[X]$, where $\bar{k}$ is the algebraic closure of k), $K \otimes k'$ is reduced. (More precisely, it is a direct product of finite separable extensions of k'.) (2) $\Rightarrow$ (3) $\Rightarrow$ (4) is trivial.

(4) $\Rightarrow$ (1): Suppose that ch(k) = p and that K contains an inseparable element t over k. Then the irreducible equation f(X) of t over k is of the form $f(X) = g(X^p)$ with some $g \in k[X]$. Let $a_0,\ldots,a_n$ be the coefficients of g(X) and put $k' = k(a_0^{1/p},\ldots,a_n^{1/p})$. Then $f(X) = g(X^p) = h(X)^p$ with $h(X) \in k'[X]$, and $k(t) \otimes_k k' = k'[X]/(h(X)^p)$ has nilpotent elements. Since k is a field we can view $k(t) \otimes_k k'$ as a subring of $K \otimes_k k'$, so the condition (4) does not hold.

(27.D) DEFINITION. Let k be a field and A a k-algebra. We say that A is separable (over k) if, for any algebraic extension k' of k, the ring $A \otimes_k k'$ is reduced.

The following properties are immediate consequences of the definition.

1) If A is separable, then any subalgebra of A is also separable.

2) If all finitely generated subalgebras of A are separable, then A is separable.

3) If, for any finite extension k' of k, the ring $A \otimes_k k'$ is reduced, then A is separable.

(27.E) LEMMA 2. If k' is a separably generated extension of a field k, and if A is a reduced k-algebra, then $A \otimes_k k'$ is reduced.

Proof. Enough to consider the case of a separably algebraic extension and the case of a purely transcendental extension. We may also assume that A is finitely generated over k. Then A is noetherian and reduced, so the total quotient ring ΦA of A is a direct product of a finite number of fields, and $A \otimes_k k' \subseteq \Phi A \otimes_k k'$. Thus we may assume that A is a field. Then $A \otimes_k k'$ is reduced by Lemma 1 in the separably algebraic case, and is a subring of a rational function field over A in the purely transcendental case.

COROLLARY. If k is a perfect field, then a k-algebra A is separable iff it is reduced. In particular, any extension field K of k is separable over k.

(27.F) LEMMA 3. Let k be a field of characteristic p, and K be a finitely generated extension of k. Then the following are equivalent:

(1) K is separable over k;

(2) the ring $K \otimes_k k^{1/p}$ is reduced;

(3) K is separably generated over k.

Proof. (3) $\Rightarrow$ (1): If K is separably generated over k, then $k' \otimes_k K$ is reduced for any extension k' of k by Lemma 2. (1) $\Rightarrow$ (2): Trivial. (2) $\Rightarrow$ (3): Let $K = k(x_1, \dots, x_n)$. We may suppose that $\{x_1, \dots, x_r\}$ is a transcendency basis of K/k. Suppose that $x_{r+1}, \dots, x_q$ are separable over $k(x_1, \dots, x_r)$ while x_{q+1} is not. Put $y = x_{q+1}$ and let $f(Y^p)$ be the irreducible equation of y over $k(x_1, \dots, x_r)$. Clearing the denominators of the coefficients of f we obtain a polynomial $F(X_1, \dots, X_r, Y^p)$, irreducible in $k[X_1, \dots, X_r, Y]$, such that $F(x_1, \dots, x_r, y^p) = 0$. Then there must be at least one X_i such that $\partial F/\partial X_i \neq 0$, for otherwise we would have $F(X, Y^p) = G(X, Y)^p$ with $G \in k^{1/p}[X_1, \dots, X_r, Y]$, so that $k(x_1, \dots, x_r, y) \otimes_k k^{1/p} \simeq k^{1/p}(X_1, \dots, X_r)[Y]/(G(X,Y)^p)$ would have nilpotent elements. Therefore we may suppose that $\partial F/\partial X_1 \neq 0$. Then x_1 is separably algebraic over $k(x_2, \dots, x_r, y)$, hence the same holds for $x_{r+1}, \dots, x_q$ also. Exchanging x_1 with $y = x_{q+1}$ we have that $x_{r+1}, \dots, x_{q+1}$ are separable over $k(x_1, \dots, x_r)$. By induction on q we see that we can choose a separating transcendency basis of K/k from the set $\{x_1, \dots, x_n\}$.

(27.G) PROPOSITION. Let k be a field and A a separable k-algebra. Then, for any extension k' of k (algebraic or not), the ring $A\otimes_k k'$ is reduced and is a separable k'-algebra.

Proof. Enough to prove that $A\otimes_k k'$ is reduced. We may assume that k' contains the algebraic closure $\bar{k}$ of k. Since $A\otimes\bar{k}$ is reduced by assumption, and since any finitely generated extension of $\bar{k}$ is separably generated by Lemma 3, the ring $A\otimes_k k'$ $= (A\otimes_k\bar{k})\otimes_{\bar{k}}k'$ is reduced by Lemma 2.

Exercises. 1 (MacLane). Let k be a field of characteristic p and K an extension of k. Then K is separable over k iff K and $k^{1/p}$ are linearly disjoint over k, that is, iff the canonical homomorphism from $K\otimes_k k^{1/p}$ onto the subfield $K(k^{1/p})$ of $K^{1/p}$ is an isomorphism.

2. Let k and K be as above, and suppose that K is finitely generated over k. Then there exists a finite extension k' of k, contained in $k^{p^{-\infty}}$, such that K(k') is separable over k'.

CHAPTER 11. FORMAL SMOOTHNESS

28. Formal Smoothness I

(28.A) The notion of formal smoothness is due to Grothendieck (EGA Ch.IV, 1964). It is closely connected with the differentials, and it throws new light to the theory of regular local rings. It can also be used in proving the Cohen structure theorems of complete local rings.

As a motivation for the definition of formal smoothness, we begin by a brief discussion of a typical theorem of Cohen.

Definition. Let $(A,\mathfrak{m},K)$ be a local ring. A coefficient field K' of A is a subfield of A which is mapped isomorphically onto $K = A/\mathfrak{m}$ by the natural map $A \to A/\mathfrak{m}$.

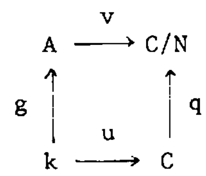
I.S.Cohen proved that any noetherian complete local ring which contains a field contains at least one coefficient field. To find a coefficient field is equivalent to finding a homomorphism $u: K \to A$ such that $ru = id_K$, where $r: A \to K$ is the natural map. Since A is complete, we have $A = \varprojlim A/\mathfrak{m}^i$. Therefore it is enough to find a system of homomorphisms $u_i: K \to A/\mathfrak{m}^i$ $(i = 1,2,\ldots)$ such that $r_i u_{i+1} = u_i$ for all i, where $r_i: A/\mathfrak{m}^{i+1} \to A/\mathfrak{m}^i$ is the natural map. Thus, the natural approach will be to try to 'lift' a given homomorphism $u_i: K \to A/\mathfrak{m}^i$ to $u_{i+1}: K \to A/\mathfrak{m}^{i+1}$. If this is always possible then one can start with $u_1 = id_K: K \to A/\mathfrak{m} = K$ and construct u_i step by step.

(28.B) Convention. Throughout the remainder of the book, we shall use the phrase topological ring to mean a topological ring whose topology is defined by the powers of an ideal, and such ideal will be called an ideal of definition. When A is a topological ring, by a discrete A-module M we shall mean an A-module such that $IM = (0)$ for some open ideal I of A. When A is a local or semi-local ring and $\mathfrak{m} = \mathrm{rad}(A)$, the topology of A will be the $\mathfrak{m}$-adic topology unless the contrary is explicitly stated.

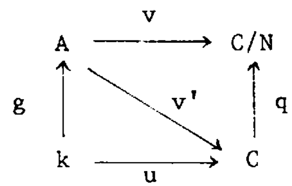
(28.C) DEFINITION. Let k and A be topological rings and $g: k \to A$ be a continuous homomorphism. We say that A is formally smooth (f.s. for short) over k, or that A is a f.s. k-algebra, if the following condition is satisfied:

(FS) For any discrete ring C, for any ideal N of C with $N^2 = (0)$ and for any continuous homomorphisms $u: k \to C$ and $v: A \to C/N$ (C/N being viewed as a discrete ring) such that the diagram

(*)



(where q is the natural map) is commutative, there exists a homomorphism $v': A \to C$ such that $v = qv'$ and $u = v'g$.



Remark. If v' exists, then we say that v can be lifted to $A \to C$ over k, and v' is called a lifting of v over k. A lifting v' is automatically continuous, for the continuity of v implies the existence of an ideal of definition I of A with $v(I) = 0$. Thus $v'(I) \subseteq N$ and $v'(I^2) = 0$. But I^2 is also an ideal of definition of A, so v' is continuous. (Similarly, the continuity of u in (*) follows from that of vg.) It follows that, if (FS) holds, then it remains true when we replace "$N^2 = 0$" by "N is nilpotent". In fact, if $N^m = 0$, then we can lift $v: A \to C/N$ successively to $A \to C/N^2$, to $A \to C/N^3$, and so on, and finally to $A \to C/N^m = C$.

Let now C be a complete and separated topological ring and N an ideal of definition of C. Consider a commutative diagram (*) with u and v continuous. Then, if A is f.s. over k, one can lift v to v': A → C. In fact one can lift v successively to $A \to C/N^2$, to $A \to C/N^3$ and so on, and then to $A \to C = \varprojlim C/N^i$.

(28.D) DEFINITION. When A is f.s. over k for the discrete topologies on k and A, we say that A is smooth over k. Thus smoothness implies formal smoothness for any adic topologies on A and k such that g: k → A is continuous.

Examples. 1. Let k be a ring and $A = k[\ldots,X_\lambda,\ldots]$ be a polynomial ring over k. Then A is smooth over k. This is clear from the definition.

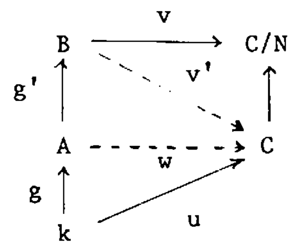
2. Let A be a noetherian k-algebra with I-adic topology (I = an ideal of A) and let A* denote the completion of A. Suppose A is f.s. over k. Then the IA*-adic ring A* is f.s. over k. In fact, a continuous homomorphism v from A* to a discrete C/N factors through $A^*/I^nA^* = A/I^n$ for some n, and $A \to A/I^n \to C/N$ can be lifted to $A \to A/I^m \to C$ for some $m \geq n$. Using $A/I^m = A^*/I^mA^*$ we get a homomorphism $A^* \to A^*/I^mA^* \to C$, which lifts the given $A^* \to C/N$.

3. In particular, if k is a noetherian ring with discrete

topology and if $B = k[[X_1,\ldots,X_n]]$ is the formal power series ring with $\sum_1^n X_iB$ -adic topology, then B is f.s. over k, because it is the completion of $A = k[X_1,\ldots,X_n]$ with respect to the $\sum X_iA$ -adic topology and A is smooth over k.

(28.E) Formal smoothness is transitive: if B is a f.s. A-algebra and A is a f.s. k-algebra, then B is f.s. over k.

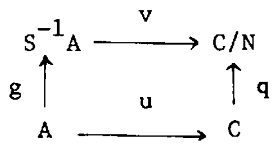
Proof.



In the diagram one first lifts vg' to w: A → C, and then lifts v to v': B → C.

(28.F) Localization. Let A be a ring and S a multiplicative set in A. Then $S^{-1}A$ is smooth over A.

Proof. Consider a commutative diagram



where g and q are the natural maps and $N^2 = 0$. Then v can be lifted to v': $S^{-1}A \to C$ iff u(s) is invertible in C for every $s \in S$. But, since $N \subseteq \text{rad}(C)$, an element x of C is a unit iff q(x) is a unit in C/N. And qu(s) = vg(s) is certainly invertible in C/N as g(s) is so in $S^{-1}A$.

(28.G) Change of base. Let k, A and k' be topological rings, and $k \to A$ and $k \to k'$ be continuous homomorphisms. Let A' denote the ring $A \otimes_k k'$ with the topology of tensor product (cf. (23.F)). If A is f.s. over k, then A' is f.s. over k'.

Proof. Look at the commutative diagram

$$\begin{array}{ccccc} A & \xrightarrow{p} & A' & \xrightarrow{v} & C/N \\ \uparrow & & \uparrow & & \uparrow q \\ k & \longrightarrow & k' & \xrightarrow[u]{} & C \end{array} .$$

One lifts the continuous homomorphism vp to $w: A \to C$, and puts $v' = w \otimes u: A \otimes_k k' = A' \to C$ to obtain a lifting of v.

(28.H) Let k be a field and A be a k-algebra. Consider a commutative diagram of rings

$$\begin{array}{ccc} A & \xrightarrow{v} & C/N \\ \uparrow & & \uparrow q \\ k & \longrightarrow & C \end{array}$$

with $N^2 = 0$, and put $E = \{(a,c) \in A \times C \mid v(a) = q(c)\}$. Then E is a k-subalgebra of $A \times C$, and is an extension of the k-algebra A by N: $0 \to N \to E \xrightarrow{p} A \to 0$ with $p(a,c) = a$. The homomorphism $v: A \to C/N$ lifts to $v': A \to C$ iff the extension $0 \to N \to E \to A \to 0$ splits over k (cf. (25.D)). Since k is a field, the extension algebra E is isomorphic to $A \oplus N$ as k-module, so it is a Hochschild extension (cf.(25.C)) and defines a symmetric cocycle $f: A \times A \to N$. We define a complex of A-modules (the 'modified Hochschild complex') $P_\cdot^! = P_\cdot^!(A/k)$:

$P_3' \xrightarrow{d_3} P_2' \xrightarrow{d_2} P_1'$ as follows: $P_3' = (A \otimes_k A \otimes_k A \otimes_k A) \oplus (A \otimes_k A \otimes_k A)$, $P_2' = A \otimes_k A \otimes_k A$, $P_1' = A \otimes_k A$ (the A-module structure on P_i' being defined by the first factor),

$$d_3(1 \otimes a \otimes b \otimes c + 1 \otimes y \otimes z) = a \otimes b \otimes c - 1 \otimes ab \otimes c + 1 \otimes a \otimes bc - c \otimes a \otimes b + 1 \otimes y \otimes z - 1 \otimes z \otimes y,$$

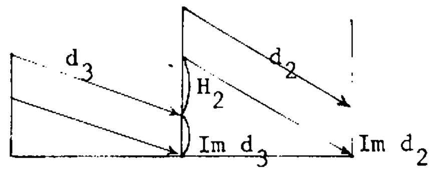
and $d_2(1 \otimes a \otimes b) = a \otimes b - 1 \otimes ab + b \otimes a$.

For any A-module N we define the cochain complex

$$\mathrm{Hom}_A(P_\cdot^!, N): \ \mathrm{Hom}_A(P_3', N) \leftarrow \mathrm{Hom}_A(P_2', N) \leftarrow \mathrm{Hom}_A(P_1', N)$$

and we denote its cohomology (at the middle term) by $H_k^2(A,N)^s$, the letter s indicating the cohomology with respect to symmetric cocycles. This cohomology vanishes iff any symmetric cocycle $f: A \times A \to N$ is a coboundary, i.e. $f(a,b) = ah(b) - h(ab) + bh(a)$ for some function $h: A \to N$. Therefore, A is smooth over k iff $H_k^2(A,N)^s = 0$ for all A-modules N.

Suppose now that A is a field K. Then every extension of K-modules splits, so we have $P_2' \simeq \mathrm{Im}(d_3) \oplus H_2(P_\cdot^!) \oplus \mathrm{Im}(d_2)$ as K-module.



It follows that $H_k^2(K, N)^s \simeq \mathrm{Hom}_K(H_2(P'_\cdot), N)$. If these are zero for all N then $H_2(P'_\cdot) = 0$, and conversely.

(28.I) PROPOSITION. Let k be a field and K an extension field of k. If K is separable over k then it is smooth over k. (The converse is also true and will be proved in Th.62.)

Proof. Suppose first that K is finitely generated over k. Then it is separably generated over k by (27.F). If K is purely transcendental over k then it is smooth over k by (28.D) Example 1, by (28.F) and by (28.E). If K is separably algebraic over k then $K = k(t) = k[X]/(f(X))$ with $f(t) = 0$, $f'(t) \neq 0$. If C is a k-algebra, if N is an ideal of C with $N^2 = 0$ and if $v: K \to C/N$ is a homomorphism of k-algebras, then v can be lifted to $K \to C$ iff there exists $x \in C$ satisfying $f(x) = 0$ and $x \bmod N = v(t)$. Take a pre-image y of v(t) in C, and let n be an element of N. Then $f(y + n) = f(y) + f'(y)n$, $f(y) \in N$, and $f'(y)$ is a unit in C because $f'(v(t)) = v(f'(t))$ is a unit in C/N. Thus, if we put $x = y + n$ with $n = -f(y)/f'(y)$, then we get $f(x) = 0$. So K is smooth over k in this case also. By the transitivity any separably generated extension is smooth.

In the general case, we have

K/k is separable

$\Leftrightarrow$ L/k is separably generated for any finitely generated subextension L/k of K/k.

$\Rightarrow$ L/k is smooth for any such L/k

$\Leftrightarrow$ $H_2(P'.(L/k)) = 0$ for any such L/k.

But, since tensor product and homology commute with inductive limits, and since $K = \varinjlim L$, we have $H_2(P'.(K/k)) = \varinjlim H_2(P'.(L/k)) = 0$. Therefore K is smooth over k by (28.H).

Remark. It is also possible to give a non-homological proof of the proposition. The above proof is due to Grothendieck and has the merit of treating the cases of $ch(k) = 0$ and of $ch(k) = p$ in a unified manner.

(28.J) THEOREM 60 (I.S.Cohen). Let $(A, \mathfrak{m}, K)$ be a complete and separated local ring containing a field k. Then A has a coefficient field. If K is separable over k then A has a coefficient field which contains k.

Proof. If K is separable over k (e.g. if $ch(K) = 0$) then it is smooth over k. Therefore one can lift $id_K: K \to A/\mathfrak{m}$ to a homomorphism of k-algebras $K \to A = \varprojlim A/\mathfrak{m}^i$ (cf.(28.A)). In the general case let k_0 be the prime field in k. Then K is separable over k_0 as the latter is perfect ((27.E) Cor.). Hence A has a coefficient field.

COROLLARY 1. Let $(A, \mathfrak{m}, K)$ be a complete and separated local ring containing a field, and suppose that $\mathfrak{m}$ is finitely generated over A. Then A is noetherian.

<u>Proof</u>. If $\mathfrak{m} = (x_1,\dots,x_n)$ and if K' is a coefficient field of A, then any element of A can be developed into a formal power series in $x_1,\dots,x_n$ with coefficients in K'. So A is a homomorphic image of $K[[X_1,\dots,X_n]]$, hence noetherian.

COROLLARY 2. Let $(A,\mathfrak{m},K)$ be a complete regular local ring of dimension d containing a field. Then $A \simeq K[[X_1,..,X_d]]$.

<u>Proof</u>. By the preceding proof we have $A \simeq K[[X_1,..,X_d]]/P$ with some prime ideal P. Comparing the dimensions we get $P = (0)$.

(28.K) THEOREM 61. Let $(A,\mathfrak{m},K)$ be a noetherian local ring containing a field k, and suppose that A is formally smooth over k. Then A is regular.

<u>Proof</u>. Let k_0 be the prime field in k. Then k is f.s. over k_0, hence A is f.s. over k_0 also. Thus we may assume that k is perfect. Let K' be a coefficient field, containing k, of the complete local ring $A/\mathfrak{m}^2$; let $\{x_1,\dots,x_d\}$ be a minimal basis of $\mathfrak{m}$. Then there is an isomorphism of k-algebras $v_1\colon A/\mathfrak{m}^2 \simeq K'[X_1,\dots,X_d]/J^2$ where $J = (X_1,\dots,X_d)$. Let $v\colon A \to K'[X]/J^2$ be the composition of v_1 with the natural map $A \to A/\mathfrak{m}^2$. By the formal smoothness one can lift v to a homomorphism of k-algebras $v'_n\colon A \to K'[X]/J^{n+1}$ for n = 2, 3, ... Since $v(x_i)$ $(1 \leqslant i \leqslant d)$ generate $J/J^2 = \bar{J}/\bar{J}^2$ (where $\bar{J} = J/J^{n+1}$), the elements $v'_n(x_i)$ generate $\bar{J}$ by NAK. Then $K'[X]/J^{n+1} = v'_n(A) + \bar{J}^2 = v'_n(A) + \sum_i v'_n(x_i)(v'_n(A) + \bar{J}^2) = v'_n(A) + \bar{J}^3 = \dots = v'_n(A) + \bar{J}^{n+1} = v'_n(A)$, i.e. v'_n is surjective. Hence we obtain $\ell(A/\mathfrak{m}^{n+1}) \geqslant \ell(K'[X_1,\dots,X_d]/J^{n+1}) = \binom{d+n}{d}$, proving $\dim A \geqslant d$. As $\mathfrak{m}$ is generated by d elements the local ring A is regular.

(28.L) THEOREM 62. Let K be a field and k a subfield. Then K is smooth over k iff it is separable over k.

<u>Proof</u>. The "if" part was already proved in (28.I). To prove the "only if", let K be smooth over k and let k' be a finite algebraic extension of k. Then $K \otimes_k k'$ is a K-algebra of finite rank, hence it is a direct product of artinian local rings: $K \otimes_k k' = A_1 \times \dots \times A_r$. Moreover, $K \otimes k'$ is smooth over k' by base change, and it follows easily that each A_i is smooth over k'. Then each A_i is regular (hence is a field) by Th.61, whence $K \otimes k'$ is reduced. Q.E.D.

(28.M) PROPOSITION. Let $(A,\mathfrak{m},K)$ be a noetherian local ring containing a field k, and let A* denote the completion of A. Suppose K is separable over k. Then the following are equivalent: (1) A is regular;

(2) $A^* \simeq K[[X_1,\dots,X_d]]$ as k-algebras, (d = dim A);

(3) A is formally smooth over k.

Proof. (1) ⇒ (2). The complete local ring A* is regular and contains a coefficient field containing k, so (2) follows from the proofs of Cor. 1 and 2 of (28.J).
(2) ⇒ (3). It follows from the definition that A is f.s. over k iff A* is so. On the other hand $K[[X_1,\dots,X_d]]$ is f.s. over K (cf.(28.D)), hence also over k by the transitivity. (3) ⇒ (1) has been proved already.

(28.N) Let $(A, \mathfrak{m})$ be a local ring containing a field k. If B is a finite A-algebra then $B/\mathfrak{m}B$ is a finite $A/\mathfrak{m}$- algebra, hence artinian. Hence B is a semi-local ring. In particular if k' is any finite extension of k, then $A' = A\otimes_k k'$ is a semi-local ring.

We say that A is geometrically regular over k if the semi-local ring $A' = A\otimes_k k'$ is regular for every finite extension k' of k. If the residue field of A is separable over k, the preceding proposition shows that

A is regular ⇔ A is f.s. over k ⇒ A' is f.s. over k'
⇒ A' is regular.

Thus geometrical regularity is equivalent to regularity for such A. But in general these two are not equal.

PROPOSITION. Let $(A,\mathfrak{m},K)$ be a noetherian local ring containing a field k. If A is f.s. over k, then A is geometrically regular over k. The converse is also true if K is finitely generated over k.
(Remark: actually the converse is always true, so that geometrical regularity and formal smoothness are the same thing; cf. EGA 0_{IV} (22.5.8)).

Proof. The first assertion is immediate from Th.61. As for the second, take a finite radical extension[1)] k' of k such that K(k') is separable over k' (cf. p.196 Ex.2). The ring $A' = A\otimes_k k'$ is a noetherian local ring with residue field K(k'), and is regular by assumption. Thus A' is f.s. over k' by the preceding proposition. Thus our proposition is proved by the following lemma.

(28.O) LEMMA. Let A be a topological ring containing a field k, and let k' be a k-algebra (with discrete topology). Put $A' = A\otimes_k k'$. Then A is f.s. over k if (and only if) A' is f.s. over k'.

Proof. Let C be a discrete k-algebra, N an ideal of C with $N^2 = 0$ and $v: A \to C/N$ a continuous homomorphism of k-

1) By a radical extension of a field k we mean a purely inseparable extension of k if ch(k)=p, and k itself if ch(k)=0.

algebras. Then $v' = v \otimes id_{k'}: A' \to C/N \otimes_k k' = (C \otimes k')/(N \otimes k')$ is a continuous homomorphism of k'-algebras, so there is a lifting $w: A' \to C' = C \otimes k'$ of v' over k'. Choose a k-submodule V of k' such that $k' = k \oplus V$. Then $C' = C \oplus (C \otimes V)$ and $C \otimes V$ is a C-submodule of C'. Write $w(a) = u(a) + r(a)$ ($u(a) \in C$, $r(a) \in C \otimes V$) for $a \in A$. Since $w(a) \bmod N \otimes k' = v(a) \in C/N$ we have $r(a) \in N \otimes V$. Thus $r(a)r(b) = 0$ for $a, b \in A$. It follows that $u: A \to C$ is a k-algebra homomorphism which lifts v. Q.E.D.

(28.P) (Structure of complete local rings: unequal characteristic case) Let $(A, \mathfrak{m}, k)$ be a local ring. There are four possibilities:

I) $ch(A) = 0$, $ch(k) = 0$; II) $ch(A) = p$, $ch(k) = p$;

III) $ch(A) = 0$, $ch(k) = p$; IV) $ch(A) = p^n > p$, $ch(k) = p$.

(If A is an integral domain then the last possibility is excluded.) If I) or II) occurs (so-called equal characteristic case) then A contains a field, and conversely. A subring R of A is called a <u>coefficient ring</u> if it satisfies the following conditions:

1) R is a noetherian complete local ring with maximal ideal $\mathfrak{m} \cap R$;

2) we have $R/\mathfrak{m} \cap R \simeq A/\mathfrak{m} = k$ by the canonical map (i.e. $A = R + \mathfrak{m}$);

3) $R \cap \mathfrak{m} = pR$, where $p = ch(k)$.

Therefore, R is nothing but a coefficient field in the equal characteristic case. In case III, $rad(R) = pR$ is not nilpotent, hence R must be a regular local ring of dimension 1, i.e. a principal valuation ring. In case IV the ring R is an artinian ring.

THEOREM (I.S.Cohen). Let A be a complete, separated local ring. Then A has a coefficient ring R. In case IV, R is of the form $R = W/p^nW$, where W is a complete principal valuation ring with maximal ideal pW.

In the equal characteristic case it was proved in Th.60. By lack of space we omit the proof of the unequal characteristic case. A concise proof can be found in P.Samuel: ALGEBRE LOCALE (Paris, 1953) pp.45-48. Grothendieck's proof (which depends on the theory of formal smoothness) is in EGA 0_{IV}19.8.

The above theorem has two important corollaries:

COROLLARY 1. Let $(A, \mathfrak{m})$ be a complete, separated local ring such that $\mathfrak{m}$ is finitely generated. Then A is a homomorphic image of a complete regular local ring. Consequently, A is not only noetherian but also universally catenarian.

(cf. p.84, p.110 Th.33, and p.121 Th.36.)

COROLLARY 2. Let $(A, \mathfrak{m})$ be a noetherian complete local domain. Then A contains a complete regular local ring A_0 over which A is finite.

Proof of Cor.2. Let R be a coefficient ring of A. Since A is an integral domain, R is either a field or a principal valuation ring with maximal ideal pR. Choose a system of parameters $x_1,\ldots,x_r$ of A which is arbitrary in the first case and is such that $x_1 = p$ in the second case. Put $A_0 = R[[x_1,\ldots,x_r]] \subseteq A$. (We have $A_0 = R[[x_2,\ldots,x_r]]$ if $x_1 = p \in R$.) Then A_0 is a noetherian complete local ring with maximal ideal $\mathfrak{m}_0 = \sum_1^r x_iA_0$. Since $A = R + \mathfrak{m}$ and since $\mathfrak{m}^\nu \subseteq \mathfrak{m}_0 A$ for large ν, $A/\mathfrak{m}_0A$ is finite over $A_0/\mathfrak{m}_0$. Then A is finite over A_0 by the lemma below. Hence $\dim A = \dim A_0 = r$ by (13.C) Th.20, and as $\mathfrak{m}_0$ is generated by r elements, A_0 is regular.

LEMMA. Let A be a ring, I an ideal of A and M an A-module. Suppose that (a) A is complete and separated in the I-adic topology, (b) M is separated in the I-adic topology and (c) M/IM is finite over A (or what is the same thing, over A/I). Then M is finite over A.

Proof is easy and left to the reader.

29. Jacobian Criteria

(29.A) Let k be a field, and I be an ideal of $k[X_1,\ldots,X_n]$. Let P be a prime ideal containing I, and put $A = k[X_1,\ldots,X_n]$, $B = A/I$ and $p = P/I$. Then $B_p = A_P/IA_P$; let κ denote the common residue field of A_P and B_p. Put $\dim A_P = m$ and $ht(IA_P) = r$. Since A is catenarian we have $\dim B_p = m - r$. We know that A_P is a regular local ring, and that B_p is regular iff IA_P is a prime ideal generated by a subset of a regular system of parameters of A_P (cf.(17.F) Th.36). We have

$\mathrm{rank}_\kappa(P/P^2 \otimes_A \kappa) = m$, and

$\mathrm{rank}_\kappa(p/p^2 \otimes_B \kappa) = m - \mathrm{rank}_\kappa((P^2 + I)/P^2 \otimes_A \kappa) \geqslant \dim B_p = m - r.$

Therefore

$$\mathrm{rank}_\kappa((P^2 + I)/P^2 \otimes_A \kappa) \leqslant r,$$

and the equality holds iff B_p is regular. The left hand side is the rank of the image of the natural map $\nu\colon I/I^2 \otimes_A \kappa \to P/P^2 \otimes_A \kappa$.

To each polynomial $f(X) \in P$ we assign the vector in κ^n $(\partial f/\partial X_1,\ldots,\partial f/\partial X_n) \bmod P$. Then we get a κ-linear map $P/P^2 \otimes_A \kappa \to \kappa^n$. If we identify κ^n with $\Omega_{A/k} \otimes_A \kappa = \Omega_{A_P/k} \otimes_{A_P} \kappa = \sum_1^n \kappa dX_i$, the map just defined is nothing but the map δ of the second fundamental exact sequence (cf.(26.I))

$$P/P^2 \otimes \kappa = PA_P/P^2A_P \xrightarrow{\delta} \Omega_{A_P/k} \otimes \kappa \to \Omega_{\kappa/k} \to 0.$$

If $I = (f_1(X),\ldots,f_s(X))$, then the image of $\delta\nu\colon I/I^2 \otimes \kappa \to$

$\Omega_{A/k}\otimes\kappa$ is generated by the vectors $(\partial f_i/\partial X_1,\ldots,\partial f_i/\partial X_n)$ mod P, $1 \leq i \leq s$, so that $\mathrm{rank}_\kappa(\mathrm{Im}(\delta\nu)) = \mathrm{rank}(\partial(f_1,\ldots,f_s)/\partial(X_1,\ldots,X_n) \bmod P)$, where the right hand side is the rank of the Jacobian matrix evaluated at the point P; we write the matrix $(\partial(f)/\partial(X))(P)$ for short. Thus, if we have

$$(*)\qquad \mathrm{rank}\ (\partial(f_1,\ldots,f_s)/\partial(X_1,\ldots,X_n))(P) = r,$$

then we must have $\mathrm{rank}\ \mathrm{Im}(\nu) = r$ also, and hence B_p is regular. When the residue field κ is separable over k we have

$$\mathrm{rank}_\kappa\ \Omega_{\kappa/k} = \mathrm{tr.deg}_k\ \kappa = n - \mathrm{ht}(P) = n - m$$

by (27.B) Th.59, while $\mathrm{rank}\ P/P^2\otimes\kappa = m$. So the map δ: $P/P^2\otimes\kappa \to \Omega_{A/k}\otimes\kappa$ is injective. In this case the condition (*) is equivalent to the regularity of B_p.

The condition (*) is nothing but the classical definition of a simple point. The above consideration shows that, when k is perfect, the point p is simple on Spec(B) iff its local ring B_p is regular. In the general case note that (*) is invariant under any extension of the ground field k. Thus, if k' denotes the algebraic closure of k and if P' is a prime ideal of $A' = k'[X_1,\ldots,X_n]$ lying over P, then p is simple on Spec(B) iff the local ring $B'_{p'} = (A'/IA')_{P'/IA'}$ is regular. Since κ is finitely generated over k, it is also easy to see that (*) is equivalent to the geometrical regularity of B_p over k.

(29.B) The results of the preceding paragraph can be more fully described by the notion of formal smoothness. We begin by proving lemmas.

LEMMA 1. Let $k \to B$ be a continuous homomorphism of topological rings and suppose B is formally smooth over k. Then, for any open ideal J of B, $\Omega_{B/k}\otimes(B/J)$ is a projective B/J-module.

(In such case we say that the B-module $\Omega_{B/k}$ is <u>formally projective</u>.)

<u>Proof</u>. Let $u\colon L \to M$ be an epimorphism of B/J-modules. We have to prove that $\mathrm{Hom}_B(\Omega_{B/k}, L) \to \mathrm{Hom}_B(\Omega_{B/k}, M)$ is surjective, i.e. that $\mathrm{Der}_k(B,L) \to \mathrm{Der}_k(B,M)$ is surjective. Let $D \in \mathrm{Der}_k(B,M)$, and consider the commutative diagram

$$\begin{array}{ccc} B & \xrightarrow{\ v\ } & (B/J)*M \\ \uparrow & & \uparrow j \\ k & \dashrightarrow & (B/J)*L \end{array}$$

where $j(x,y) = (x,uy)$ and $v(b) = (b \bmod J, D(b))$. Let $v'\colon B \to (B/J)*L$ be a lifting of v. Then we have $v'(b) = (b \bmod J, D'(b))$ with a derivation $D' \in \mathrm{Der}_k(B,L)$, and $uD' = D$.

LEMMA 2. Let B be a ring, J an ideal of B and $u\colon L \to M$ a homomorphism of B-modules. Suppose M is projective. Furthermore, assume either that (α) J is nilpotent, or that (β) L is a finite B-module and $J \subseteq \text{rad}(B)$. Then u is left-invertible iff $\bar{u}$: $L/JL \to M/JM$ is so.

Proof. "Only if" is trivial, so suppose $\bar{u}$ has a left-inverse $\bar{v}$: $M/JM \to L/JL$. Since M is projective we can lift $\bar{v}$ to v: $M \to L$; put $w = vu$. Then $L = w(L) + JL$, hence $L = w(L)$ by NAK. Then w is an automorphism. [In fact, it is generally true that a surjective endomorphism f of a finite B-module L is an automorphism. Here is an elegant proof due to Vasconcelos: Let B[T] operate on L by $T\xi = f(\xi)$. Then $L = TL$, hence by NAK there exists $\phi(T) \in B[T]$ such that $(1 + T\phi(T))L = 0$; then $T\xi = 0$ implies $\xi = 0$.] Therefore $w^{-1}v$ is a left-inverse of u.

(29.C) THEOREM 63. Let k and A be topological rings (cf. 28.B) and g: $k \to A$ a continuous homomorphism. Let Q be an ideal of definition of A, let I be an ideal of A and put

$$B = A/I, \qquad q = (Q + I)/I.$$

Suppose that A is noetherian and formally smooth over k. Then the following are equivalent:

(1) B (with the q-adic topology) is f.s. over k;

(2) the canonical maps

$$\delta_n: (I/I^2) \otimes_B (B/q^n) \to \Omega_{A/k} \otimes_A (B/q^n) \quad (n = 1,2,..)$$

derived from the map $\delta: I/I^2 \to \Omega_{A/k} \otimes B$ of Th.58 are left-invertible;

(3) the map $\delta_1: (I/I^2) \otimes (B/q) \to \Omega_{A/k} \otimes (B/q)$ is left-invertible. (When q is a maximal ideal, this condition says simply that δ_1 is injective.)

Proof. (2) $\Rightarrow$ (3) is trivial, while (3) $\Rightarrow$ (2) follows from the preceding lemmas. (2) $\Rightarrow$ (1) is easy and left to the reader. We prove (1) $\Rightarrow$ (2). Put $B_n = B/q^n$. The map δ_n is left-invertible iff, for any B_n-module N, the induced map

$$\text{Hom}(I/I^2, N) \leftarrow \text{Der}_k(A, N)$$

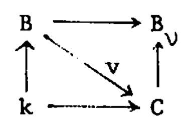
is surjective. So fix a B_n-module N and a homomorphism $g \in \text{Hom}_B(I/I^2, N)$. Since A is noetherian there exists, by Artin-Rees, an integer $\nu > n$ such that $I \cap Q^\nu \subseteq Q^n I$. Then g induces a map g_ν: $(I + Q^\nu)/(I^2 + Q^\nu) \to I/(I^2 + (Q^\nu \cap I)) \to I/(I^2 + Q^n I) \to N$, which is a homomorphism of B_ν-modules. Let E denote the extension

$$0 \to (I + Q^\nu)/(I^2 + Q^\nu) \to A/(I^2 + Q^\nu) \to B_\nu \to 0$$

of the discrete k-algebra B_ν, and let

$$0 \to N \to C \to B_\nu \to 0$$

be the extension $g_{\nu *}(E)$ (cf. 25.E). The ring C is a discrete k-algebra. Since B is f.s. over k, there exists a continuous homomorphism v: $B \to C$ such that



is commutative. On the other hand, by the definition of $g_{\nu*}(E)$ we have a canonical homomorphism of k-algebras u: $A \to A/(I^2 + Q^\nu) \to C$ such that

$$\begin{array}{ccc} B & \longrightarrow & B_\nu \\ \uparrow & u & \uparrow \\ A & \longrightarrow & C \end{array}$$

commutes. Denoting the natural map $A \to B = A/I$ by r, we get a derivation $D = u - vr \in \mathrm{Der}_k(A,N)$. It is easy to check that $D(x) = u(x) = g(x \bmod I^2)$ for $x \in I$. Q.E.D.

COROLLARY. If, in the notation of Th.63, B is also f.s. over k, then the B-module I/I^2 is formally projective.

(29.D) LEMMA 3 (EGA 0_{IV} 19.1.12). Let B be a ring, L a finite B-module, M a projective B-module and $u: L \to M$ a B-linear map. Then the following conditions on $p \in \mathrm{Spec}(B)$ are equivalent, and the set of the points p satisfying the conditions is open in Spec(B).

(1) $u_p: L_p = L \otimes B_p \to M_p = M \otimes B_p$ is left-invertible.

(2) there exist $x_1, \dots, x_m \in L$ and $v_1, \dots, v_m \in \mathrm{Hom}_B(M,B)$ such that $L_p = \Sigma x_i B_p$ and $\det(v_i(u(x_j))) \notin p$.

(3) there exists $f \in B - p$ such that $u_f: L_f = L \otimes B_f \to M_f = M \otimes B_f$ is left-invertible.

Proof. The module M is a direct summand of a free B-module F. Since L is finitely generated u(L) is contained in a free submodule F' of F of finite rank which is a direct summand of F. Now the conditions (1), (2), (3) are not affected if we replace M by F, and then F by F'. Therefore we may assume that M is free of finite rank.

(1) ⇒ (2): The assumption (1) implies that L_p is B_p-projective, hence B_p-free. Let $x_i \in L$ ($1 \leq i \leq m$) be such that their images in L_p (which are denoted by the same letters x_i) form a basis. Then $\{u_p(x_1), \dots, u_p(x_m)\}$ is a part of a basis of M_p, so there exist linear forms $v_i': M_p \to B_p$ such that $v_i'(u_p(x_j)) = \delta_{ij}$. Since M is free of finite rank we can write $v_i' = s_i^{-1} v_i$, $s_i \in B - p$, $v_i \in \mathrm{Hom}_B(M,B)$. Then $\det(v_i(u(x_j))) \notin p$.

(2) ⇒ (3); Since L is finite over B and since $L_p = \sum_1^m x_i B_p$ it is easy to find $g \in B - p$ such that $L_g = \Sigma x_i B_g$. Put $d = \det(v_i(u(x_j)))$ and $f = gd$. Then $L_f = \Sigma x_i B_f$, and d is a unit in B_f. It follows that $M_f = u_f(L_f) + V$ with $V = \bigcap \mathrm{Ker}(v_i)$. Moreover, $u(x_i)$ ($1 \leq i \leq m$) are linearly independent over B_f, so that u_f is injective. Thus u_f is left-invertible.

(3) ⇒ (1): Trivial. Lastly, the set of the points p which satisfy (3) is obviously open in Spec(B). Q.E.D.

(29.E) THEOREM 64. Let k be a ring, and A be a noetherian, smooth k-algebra. Let I be an ideal of A, $B = A/I$, $p \in$

Spec(B), P = the inverse image of p in A, q = $P \cap k$ and $\kappa(p)$ = the residue field of B_p and A_P. Then the following are equivalent:

(1) B_p is smooth over k (or what amounts to the same, over k_q);

(2) the local ring B_p (with the topology as a local ring) is formally smooth over the discrete ring k or k_q;

(2') the local ring B_p is f.s. over the local ring k_q;

(3) $(I/I^2)\otimes_B \kappa(p) \rightarrow \Omega_{A/k}\otimes_A \kappa(p)$ is injective;

(4) $(I/I^2)\otimes_B B_p \rightarrow \Omega_{A/k}\otimes_A B_p$ is left-invertible;

(5) there exist $F_1,\ldots,F_r \in I$ and $D_1,\ldots,D_r \in \mathrm{Der}_k(A,B)$ such that $\sum_1^r F_i A_P = IA_P$ and $\det(D_i F_j) \notin p$;

(6) there exists $f \in B - p$ such that B_f is smooth over k.

Consequently, the set $\{p \in \mathrm{Spec}(B) \mid B_p \text{ is smooth over k}\}$ is open in Spec(B).

Proof. (1) $\Rightarrow$ (2): trivial. (2) $\Rightarrow$ (2') is also trivial (cf. 28.C). (2) $\Rightarrow$ (3): we know that the local ring A_P is (smooth, hence a fortiori) f.s. over k, and we have $B_p = A_P/IA_P$ and $\Omega_{A_P/k} = \Omega_{A/k}\otimes_A A_P$. So apply Th.63.

(3) $\Rightarrow$ (4): since $\Omega_{A/k}$ is A-projective by Lemma 1, $\Omega_{A/k}\otimes B_p$ is B_p-projective. Apply Lemma 2.

(4) $\Rightarrow$ (5): apply Lemma 3 to the B-linear map $I/I^2 \rightarrow \Omega_{A/k}\otimes_A B$.

(5) $\Rightarrow$ (6): by Lemma 3 and Th.63.

(6) $\Rightarrow$ (1): trivial.

Remark 1. The theorem has two important consequences. First, if, in the theorem, k is a field, then A is smooth over the prime field k_0 in k also, and B_p is smooth over k_0 iff it is regular. Therefore the set $\{ p \mid B_p \text{ is regular}\}$ is open in Spec(B).

Secondly, let k be a noetherian ring and B a k-algebra of finite type. Then B_p ($p \in \mathrm{Spec}(B)$) is smooth over k iff it is f.s. over k. In fact B is of the form A/I, $A = k[X_1, \ldots, X_n]$, so we can apply the theorem.

Remark 2. When the conditions of Th.64 hold, the number r of (5) is equal to the height of IA_P.

(29.F) Nagata gave a similar Jacobian criterion for rings of the form $B = k[[X_1,\ldots,X_n]]/I$, where k is a field (Ill. J. Math. vol.1 (1957), 427-432). By lack of space we just quote the main result in the form found in EGA:

THEOREM (cf. EGA 0_{IV} 22.7.3). Let k be a field, and let $(A,\mathfrak{m},K)$ be a noetherian complete local ring. Let I be an ideal of A, B = A/I, P a prime ideal containing I and p = P/I. Suppose that

(1) $[k: k^p] < \infty$ if $ch(k) = p > 0$,

(2) K is a finite extension of a separable extension K_0 of k, and

(3) A has a structure of a formally smooth K_0-algebra.

Then the local ring B_p is f.s. over k iff there exist $F_1, \ldots, F_m \in I$ and $D_1, \ldots, D_m \in Der_k(A)$ such that $IA_P = \Sigma F_i A_P$ and such that $Det(D_i(F_j)) \notin P$.

COROLLARY (cf. EGA 0_{IV} 22.7.6). Let B be a noetherian complete local ring containing a field. Then the set $\{p \in Spec(B) \mid B_p \text{ is regular}\}$ is open in Spec(B).

30. Formal Smoothness II

(30.A) DEFINITION. Let $\Lambda \xrightarrow{g} k \xrightarrow{f} A$ be continuous homomorphisms of topological rings (cf. 28.B). We say that A is <u>formally smooth over k relative to Λ</u> (f.s. over k rel.Λ, for short) if, given any commutative diagram

$$\begin{array}{ccccc} & & A & \xrightarrow{v} & C/N \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle j} \\ \Lambda & \xrightarrow{g} & k & \xrightarrow{i} & C \end{array}$$

where C and C/N are discrete rings, N an ideal of C with $N^2 = 0$ and the homomorphisms are continuous, the map v can be lifted to a k-algebra homomorphism $A \to C$ whenever it can be lifted to a Λ-algebra homomorphism $A \to C$.

THEOREM 65. Let $\Lambda \xrightarrow{g} k \xrightarrow{f} A$ be as above. Then the following are equivalent:

(1) A is f.s. over k rel. Λ;

(2) for any A-module N such that $IN = 0$ for some open ideal I of A, the map $Der_\Lambda(A,N) \to Der_\Lambda(k,N)$ induced by f is surjective;

(3) $\Omega_{k/\Lambda} \otimes_k (A/I) \to \Omega_{A/\Lambda} \otimes_A (A/I)$ is left-invertible for any open ideal I of A.

<u>Proof</u>. (1) ⇒ (2): Put $C = (A/I)*N$, take $D \in Der_\Lambda(k,N)$ and define $i: k \to C$ by $i(\alpha) = (vf(\alpha), D(\alpha))$ $(\alpha \in k)$ where $v: A \to A/I$ is the natural map. Then v can be lifted to the Λ-homomorphism $a \longmapsto (v(a), 0) \in C$, hence it can also be lifted to a k-homomorphism $a \longmapsto (v(a), D'(a))$, and then $D': A \to N$ is a derivation satisfying $D = D'f$. (2) ⇒ (1) is also easy, and (2) ⇔ (3) is obvious.

(30.B) THEOREM 66. Let $\Lambda \to k \to A$ be as above, let J be an ideal of definition of A and suppose A is formally smooth over Λ. Then A is f.s. over k iff

$$\Omega_{k/\Lambda} \otimes_k (A/J) \to \Omega_{A/\Lambda} \otimes_A (A/J)$$

is left-invertible.

<u>Proof</u>. By assumption, A is f.s. over k iff it is f.s. over k rel. Λ. On the other hand, for any open ideal I of A the

A/I-module $\Omega_{A/\Lambda}\otimes(A/I)$ is projective by (29.B) Lemma 1. Thus the condition (3) of the preceding theorem is equivalent to the present condition by (29.B) Lemma 2.

COROLLARY. Let $(A, \mathfrak{m}, K)$ be a regular local ring containing a field k. Then A is f.s. over k iff

$$\Omega_k \otimes_k K \to \Omega_A \otimes_A K$$

is injective.

Proof. Since A is f.s. over the prime field in k, the assertion follows from the theorem.

(30.C) LEMMA 1. Let k be a field of characteristic p. Let $F = \{k_\alpha\}$ be a family of subfields of k, directed downwards (i.e. for any two members of F there exists a third which is contained in both of them), such that $k^p \subseteq k_\alpha \subseteq k$, $\bigcap_\alpha k_\alpha = k^p$. Let $u_\alpha\colon \Omega_k \to \Omega_{k/k_\alpha}$ be the canonical homomorphisms. Then $\bigcap_\alpha \mathrm{Ker}(u_\alpha) = (0)$.

Proof. Let (x_i) be a p-basis of k. Then Ω_k is a free k-module with (dx_i) as a basis. Suppose that $0 \neq \sum_1^n c_i dx_i \in \bigcap_\alpha \mathrm{Ker}(u_\alpha)$. Then the monomials $\{x_1^{\nu_1}\cdots x_n^{\nu_n} \mid 0 \leq \nu_i < p\}$ must be linearly dependent over k_α for all α. But since they are linearly independent over k^p and since $\bigcap k_\alpha = k^p$, it is easily seen that they are linearly indep. over some k_α.

THEOREM 67. Let $(A, \mathfrak{m}, K)$ be a regular local ring containing a field k of characteristic p. Let $F = \{k_\alpha\}$ be as in the above lemma. Then A is f.s. over k iff A is f.s. over k rel. k_α for all α.

Proof. "Only-if" is trivial. Conversely, suppose the condition holds, and look at the commutative diagram

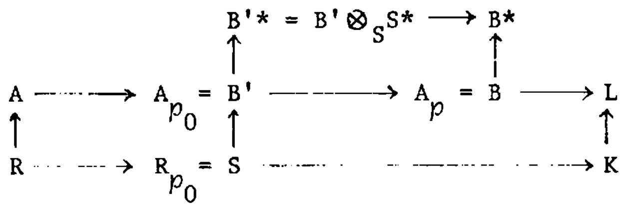
$$\begin{array}{ccc} \Omega_k \otimes_k K & \xrightarrow{w} & \Omega_A \otimes K \\ {\scriptstyle u'_\alpha}\downarrow & & \downarrow \\ \Omega_{k/k_\alpha} \otimes K & \xrightarrow{w_\alpha} & \Omega_{A/k_\alpha} \otimes K. \end{array}$$

Here w_α is injective by Th.65 and $u'_\alpha = u_\alpha \otimes 1_K$. Thus $\mathrm{Ker}(w) \subseteq \bigcap \mathrm{Ker}(u'_\alpha) = (\bigcap \mathrm{Ker}(u_\alpha)) \otimes K = (0)$.

(30.D) THEOREM 68 (Grothendieck). Let A be a noetherian complete local ring and p a prime ideal of A; put $B = A_p$ and let B^* denote the completion of B. Let $q' \in \mathrm{Spec}(B)$ and put $L = \kappa(q') = B_{q'}/q'B_{q'}$. Then, for any prime ideal Q of B^* lying over q', the 'local ring of Q on the fibre' $B^*_Q \otimes_B L = B^*_Q/q'B^*_Q$ (cf. 21.A) is formally smooth (hence geometrically regular) over L.

Proof. Step I. Put $q = q' \cap A$, $\bar{A} = A/q$, $\bar{B} = B/qB = B/q'$, $\bar{B}^*$ =(the completion of the local ring $\bar{B}$) $= B^*/q'B^*$ and $\bar{Q} = Q/q'B^*$. Then the 'local ring of Q on the fibre' remains the same when we replace A, B, B*, Q by $\bar{A}$, $\bar{B}$, $\bar{B}*$, $\bar{Q}$ respectively. Thus we may assume that A is an integral domain and $Q \cap B = q' = (0)$.

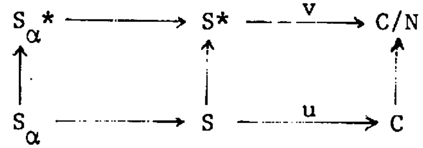
Step II (Reduction to the case that B is regular). Take a complete regular local ring $R \subseteq A$ over which A is finite. Put $p_0 = p \cap R$, $S = R_{p_0}$ and $B' = A_{p_0}$. Then B' is finite over S, and $B = A_p$ is a localization of the semi-local ring B' by a maximal ideal. Hence B* is a localization (and a direct factor) of $B'* = B' \otimes_S S*$. Let L (resp. K) be the quotient field of A, B' and B (resp. R and S).



We are given $Q \in \mathrm{Spec}(B*)$ such that $Q \cap B = (0)$. Then $B*_Q$ is a localization of $L \otimes_{B'} B'* = L \otimes_S S* = L \otimes_K (K \otimes_S S*)$, and L is a finite extension of the field K. In general if T is a K-algebra, if $M \in \mathrm{Spec}(L \otimes_K T)$ and $m = M \cap T$, and if T_m is f.s. over K, then $(L \otimes T)_M$ is a localization of $L \otimes_K T_m$ and hence is f.s. over L. Thus it suffices to show that $S*_{Q \cap S*}$ is f.s. over K. Thus the problem is reduced to proving that, if R is a complete regular local ring with quotient field K, if $p \in \mathrm{Spec}(R)$ and $S = R_p$, and if Q is a prime ideal of S* such that $Q \cap S = (0)$, then $S*_Q$ is f.s. over K.

Step III. The local ring $S*_Q$ is regular, so if ch(K) = 0 we are done. If ch(K) = p we apply the preceding theorem. In this case R is an equicharacteristic complete regular local ring, hence $R = k[[X_1, \ldots, X_n]]$ for some subfield k of R. Let $\{k_\alpha\}$ be the family of all subfields k_α of k such that $[k: k_\alpha] < \infty$ and $k^p \subseteq k_\alpha \subseteq k$. Put $R_\alpha = k_\alpha[[X_1{}^p, \ldots, X_n{}^p]]$, $p_\alpha = R_\alpha \cap p$, $S_\alpha = (R_\alpha)_{p_\alpha}$ and $K_\alpha = \Phi R_\alpha = k_\alpha((X_1{}^p, \ldots, X_n{}^p))$. Then $\bigcap_\alpha k_\alpha = k^p$, hence it is elementary to see that $\bigcap_\alpha K_\alpha = K^p$ (see below). By the preceding theorem we have only to show that, for each α, $S*_Q$ is f.s. over K rel. K_α.

Since $R^p \subseteq R_\alpha \subseteq R$, p is the only prime ideal of R lying over p_α. Hence $S = R_p = R_{p_\alpha} = R \otimes_{R_\alpha} S_\alpha$, and so S is finite over S_α. Therefore $S* = S \otimes_{S_\alpha} S_\alpha*$. Suppose we are given diagram



where $N^2 = (0)$ and u and v are homomorphisms, and a lifting $v': S* \to C$ of v over S_α. Put $v* = v'|S_\alpha*$ and $v'' = u \otimes v*$: $S* = S \otimes_{S_\alpha} S_\alpha* \to C$. Then v'' is a lifting of v over S. Thus S* is formally smooth over S rel. S_α with respect to the discrete topology. Then it follows immediately from the definition that $S*_Q$ is f.s. over K rel. K_α as a discrete ring, hence a fortiori as a local ring. Q.E.D.

(30.E) A Digression. Let A be a ring and M an A-module. We say that M is <u>injectively free</u> if, for any non-zero element x of M, there exists a linear form $f \in \mathrm{Hom}_A(M,A)$ with $f(x) \neq 0$ (in other words, if the canonical map from M to its double dual is injective).

LEMMA 2. Let B be an A-algebra which is injectively free as A-module. Then $B[X_1,\ldots,X_n]$ (resp. $B[[X_1,\ldots,X_n]]$) is injectively free over $A[X_1,\ldots,X_n]$ (resp. $A[[X_1,\ldots,X_n]]$).

<u>Proof</u>. Just extend a suitable A-linear map $\ell: B \to A$ to $B[X_1,\ldots,X_n]$ (resp. ..) by letting it operate on the coefficients.

LEMMA 3. Let $A \subset B$ be integral domains, and suppose B is injectively free over A. Let K and L be the quotient fields of A and B respectively, and X be an indeterminate. Then

$$\Phi(B[[X]]) \cap K((X)) = \Phi(A[[X]]).$$

<u>Proof</u>. $\supseteq$ is trivial. To see $\subseteq$, let $\xi \in \Phi(B[[X]]) \cap K((X))$. As an element of K((X)) we can write (the Laurent expansion)

$$\xi = X^m(r_0 + r_1X + r_2X^2 + \ldots), \quad m \in \mathbb{Z}, \quad r_i \in K.$$

We may assume m = 0. Since $\xi \in \Phi(B[[X]])$ there exists $0 \neq \phi \in B[[X]]$ such that $\phi\xi = \psi \in B[[X]]$. Write

$$\phi = \sum_0^\infty \alpha_i X^i, \quad \psi = \sum_0^\infty \beta_k X^k, \quad \alpha_i, \beta_j \in B.$$

Then $\sum_{i+j=k} \alpha_i r_j = \beta_k$. Take a linear map $\ell: B \to A$ with $\ell(\alpha_i) \neq 0$ for some i. Then $\sum_{i+j=k} \ell(\alpha_i) r_j = \beta_k$. Writing $\ell(\phi) = \sum \ell(\alpha_i)X^i$ and $\ell(\psi) = \sum \ell(\beta_k)X^k$ we therefore get $\ell(\phi) \neq 0$ and $\xi = \ell(\psi)/\ell(\phi) \in \Phi(A[[X]])$.

PROPOSITION. Let k be a field and $\{k_\alpha\}$ a family of subfields of k. Put $k_0 = \bigcap_\alpha k_\alpha$. Then we have

$$\bigcap_\alpha k_\alpha((X_1,\ldots,X_n)) = k_0((X_1,\ldots,X_n)).$$

<u>Proof</u>. When n = 1, the uniqueness of the Laurent expansion proves the assertion. Induction on n. Put

$$A = k_0[[X_1,\ldots,X_{n-1}]], \qquad B_\alpha = k_\alpha[[X_1,\ldots,X_{n-1}]],$$
$$K = \Phi A = k_0((X_1,\ldots,X_{n-1})), \quad L_\alpha = \Phi B_\alpha = k_\alpha((X_1,\ldots,X_{n-1})).$$

Then we have

$$\bigcap_\alpha k_\alpha((X_1,\ldots,X_n)) \subseteq \bigcap_\alpha L_\alpha((X_n)) = (\bigcap_\alpha L_\alpha)((X_n)) = K((X_n))$$

by the induction hypothesis, whence

$$\begin{aligned}\bigcap_\alpha k_\alpha((X_1,\ldots,X_n)) &\subseteq k_\alpha((X_1,\ldots,X_n)) \cap K((X_n)) \\ &= \Phi(B_\alpha[[X_n]]) \cap K((X_n)) \\ &= \Phi(A[[X_n]]) \\ &= k_0((X_1,\ldots,X_n)).\end{aligned}$$

Q.E.D.

CHAPTER 12. NAGATA RINGS

31. Nagata Rings

(31.A) DEFINITIONS. Let A be an integral domain and K its quotient field. We say that A is N-1 if the integral closure of A in K is a finite A-module; and that A is N-2 if, for any finite extension L of K, the integral closure A_L of A in L is a finite A-module. If A is N-1 (resp. N-2), so is any localization of A. The first example of a noetherian domain that is not N-1 was given by Y. Akizuki (Proc. Phys-Math. Soc. Japan 17(1935), 327-336).

We say that a ring B is a Nagata ring[1)] if it is noetherian and if B/p is N-2 for every $p \in \mathrm{Spec}(B)$. If B is a Nagata ring then any localization of B and any finite B-algebra are again Nagata.

1) pseudo-geometric ring in Nagata's terminology, and (noetherian) universally Japanese ring in EGA (cf. EGA IV. 7.7.2).

(31.B) PROPOSITION. Let A be a noetherian normal domain with quotient field K, let L be a finite separable extension of K and let A_L denote the integral closure of A in L. Then A_L is finite over A.

Proof. Enlarging L if necessary, we may assume L is a finite Galois extension of K. Let $G = \{\sigma_1, \dots, \sigma_n\}$ be its group, and choose a basis $\omega_1, \dots, \omega_n$ of L from A_L. Take $\alpha \in A_L$ and write $\alpha = \sum_1^n u_j \omega_j$, $u_j \in K$. Then $\sigma_i(\alpha) = \sum_j u_j \sigma_i(\omega_j)$ for $1 \leq i \leq n$, and the determinant $D = \det(\sigma_i(\omega_j))$ is not zero. The element $c = D^2$ is G-invariant, hence belongs to K. Solving the linear equations $\sigma_i(\alpha) = \sum_j u_j \sigma_i(\omega_j)$, we get $u_i = D_i/D = c_i/c$, where $D_i \in A_L$ and $c_i = DD_i \in A_L \cap K = A$. Thus A_L is contained in the finite A-module $\Sigma A(\omega_i/c)$. Therefore A_L itself is finite over A.

COROLLARY 1. Let A be a noetherian domain of characteristic zero. Then A is N-2 iff it is N-1.

COROLLARY 2. Let A be a noetherian domain with quotient field K. Then A is N-2 if, for any finite radical extension E of K, the integral closure of A in E is finite over A.

Proof. If L is a finite extension of K, the smallest normal extension L' of K containing L is also finite over K, and if E is the subfield of Aut(L'/K)-invariants then L'/E is separable and E/K is radical. Thus the assertion follows from the Proposition.

(31.C) THEOREM 69 (Tate). Let A be a noetherian normal domain and let $x \neq 0$ be an element of A such that xA is a prime ideal. Suppose further that A is xA-adically complete and separated, and that A/xA is N-2. Then A itself is N-2.

Proof. We may assume that $ch(A) = p > 0$. Let L be a finite radical extension of the quotient field K of A, and let B be the integral closure of A in L. Then there exists a power $q = p^f$ of p such that $L^q \subseteq K$, and we have $B = \{b \in L \mid b^q \in A\}$ by the normality of A. By enlarging L if necessary, we may assume that there exists $y \in B$ with $y^q = x$. Put $\mathfrak{p} = xA$, and let P be a prime ideal of B lying over $\mathfrak{p}$. Then we have $P = \{b \in B \mid b^q \in \mathfrak{p}\} = yB$. Thus $A_{\mathfrak{p}}$ and B_P are local domains whose maximal ideals are principal and $\neq (0)$. Hence they are principal valuation rings. Then it is well known (and easy to see) that $[\kappa(P): \kappa(\mathfrak{p})] \leq [L: K]$, where $\kappa(P)$ and $\kappa(\mathfrak{p})$ are the residue fields of B_P and $A_{\mathfrak{p}}$ respectively. Since B/P is contained in the integral closure of $A/\mathfrak{p}$ in $\kappa(P)$, and since $A/p = A/xA$ is N-2, the ring B/P is finite over A/xA. Since $P = yB$, we have $P^i/P^{i+1} \simeq B/P$ for each i, hence $B/xB = B/P^q$ is also a finite module over A/xA. Moreover, B is separated in the xB-adic topology. In fact, the xB-adic topology is equal to the yB-adic topology, and since y is not a zero-divisor in B one immediately verifies that $y^m B_P \cap B = y^m B$ $(m = 1,2,\ldots)$. Therefore $\bigcap^{\infty} y^m B \subseteq \bigcap^{\infty} y^m B_P = (0)$. Now the theorem follows from the lemma of (28.P).

COROLLARY 1. If A is a noetherian normal domain which is N-2, then the formal power series ring $A[[X_1,\ldots,X_n]]$ is N-2 also.

COROLLARY 2 (Nagata). A noetherian complete local ring A is a Nagata ring.

Proof. If $p \in \operatorname{Spec}(A)$ then A/p is also a complete local ring. Thus we have only to prove that a noetherian complete local domain A is N-2. But then A is a finite module over a complete regular local ring A_0 by (28.P), and A_0 is N-2 by the theorem (use induction on dim A_0). Hence A is N-2.

(31.D) Let A be a noetherian semi-local ring and A* its completion. If A* is reduced then A is said to be analytically unramified. A prime ideal p of A is said to be analytically unramified if $A^*/pA^* = (A/p)^*$ is reduced.

LEMMA 1. Let A be a noetherian semi-local domain and $p \in \operatorname{Spec}(A)$. Suppose that (1) A_p is a principal valuation ring, and (2) p is analytically unramified. Then, for any $p^* \in \operatorname{Ass}_{A^*}(A^*/pA^*)$, the ring $A^*_{p^*}$ is a principal valuation ring.

Proof. By (1) there exists $\pi \in A$ such that $pA_p = \pi A_p$, and by (2) we get $p^*A^*_{p^*} = pA^*_{p^*} = (pA_p)A^*_{p^*} = \pi A^*_{p^*}$. Since π is A*-regular by the flatness of A* over A, the local ring $A^*_{p^*}$ is regular of dimension 1.

LEMMA 2. Let A be a noetherian semi-local domain and let $0 \neq x \in \operatorname{rad}(A)$. Suppose (1) A/xA has no embedded primes, and (2) for each $p \in \operatorname{Ass}_A(A/xA)$, A_p is regular and p is analytically unramified. Then A is analytically unramified.

Proof. Let $\operatorname{Ass}_A(A/xA) = \{p_1,\ldots,p_r\}$ and $\operatorname{Ass}_{A^*}(A^*/p_iA^*) = \{P_{i1},\ldots,P_{in_i}\}$. Then $p_iA^* = \bigcap_j P_{ij}$ by (2). Let Q_{ij} be the kernel of the canonical map $A^* \to A^*_{P_{ij}}$. Since $A^*_{P_{ij}}$ is regular by Lemma 1, Q_{ij} is a prime ideal of A*. Therefore, A* is reduced if $\bigcap_{i,j} Q_{ij} = (0)$. Put $N = \bigcap Q_{ij}$. The formula $\operatorname{Ass}_{A^*}(A^*/xA^*) = \bigcup_{p \in \operatorname{Ass}(A/xA)} \operatorname{Ass}_{A^*}(A^*/pA^*) = \{P_{ij}\}$ shows that $xA^* = \bigcap_{i,j} P'_{ij}$ where P'_{ij} is P_{ij}-primary. We have

$Q_{ij} \subseteq P'_{ij}$ by the definition of Q_{ij}. Hence $N \subsetneq xA^*$. But x is A^*-regular, so that $x \notin Q_{ij}$. Hence we get $N = xN$, and since $x \in rad(A^*)$ we conclude $N = (0)$.

THEOREM 70. Let A be a noetherian semi-local domain. If A is a Nagata ring then it is analytically unramified.

Proof. We use induction on dim A. Let B be the integral closure of A in its quotient field. Then B is finite over A, hence for any $P \in Spec(B)$ the domain B/P is finite over $A/P \cap A$ which is assumed to be N-2. Thus B is a Nagata ring. Moreover, if $\mathfrak{m} = rad(A)$ then the (rad(B)-adic) topology of B is equal to the $\mathfrak{m}$-adic topology, hence A is a subspace of B by Artin-Rees so that $A^* \subseteq B^*$. Therefore we may assume that A is a normal domain. Let $0 \neq x \in rad(A)$. Since A is normal the A-module A/xA has no embedded primes. If $\mathfrak{p} \in Ass_A(A/xA)$, then $A/\mathfrak{p}$ is a Nagata domain and $\dim A/\mathfrak{p} < \dim A$, hence $\mathfrak{p}$ is analytically unramified by the induction hypothesis. Moreover, $A_{\mathfrak{p}}$ is regular because $ht(\mathfrak{p}) = 1$. Thus the conditions of Lemma 2 are satisfied, and A is analytically unramified.

(31.E) For any ring R, we shall denote by R' the integral closure of R in its total quotient ring ΦR. Let A be a

noetherian local ring, and suppose A is analytically unramified. Then $(0) = P_1 \cap \ldots \cap P_r$ in A^*, where the P_i are the minimal prime ideals of A^*. Hence $\Phi A^* = K_1 \times \ldots \times K_r$ with $K_i = \Phi(A^*/P_i)$, and $A^{*\prime} = (A^*/P_1)' \times \ldots \times (A^*/P_r)'$. Since A^*/P_i is a complete local domain, it is a Nagata ring and $(A^*/P_i)'$ is finite over A^*/P_i, or what amounts to the same, over A^*. Therefore $A^{*\prime}$ is finite over A^*. This property implies, in turn, that A' is finite over A. Indeed, since A^* is faithfully flat over A we have $A' \otimes_A A^* \subseteq (\Phi A) \otimes_A A^* \subseteq \Phi A^*$, and hence $A' \otimes_A A^* \subseteq A^{*\prime}$. Thus $A' \otimes A^*$ is finite over A^*, and we can find elements a'_i $(1 \leq i \leq m)$ of A' such that $A' \otimes A^* = \Sigma a'_i A^*$. Then $(A'/\Sigma a'_i A) \otimes_A A^* = 0$, so that $A' = \Sigma a'_i A$ by the faithful flatness of A^*. Summing up, we have the following implications for a noetherian local ring A.

A is complete $\Rightarrow$ A is a Nagata ring,

A is a Nagata domain $\Rightarrow$ A is analytically unramified $\Rightarrow$ $A^{*\prime}$ is finite over A^* $\Rightarrow$ A' is finite over A, i.e. A is N-1.

(31.F) THEOREM 71. Let A be a semi-local Nagata domain. Let $P_1, \ldots, P_r$ be the minimal prime ideals of the completion A^* of A, and let K (resp. L_i) denote the quotient field of A (resp. of A^*/P_i). Then each L_i is separable over K.

Proof. Take any finite extension L of K. Since A^* is reduced by Th.70 we have $\Phi A^* = L_1 \times \dots \times L_r$, and it suffices to show that $\Phi A^* \otimes_K L = (L_1 \otimes L) \times \dots \times (L_r \otimes L)$ is reduced. Since L is flat over A we have $A^* \otimes_A L \subseteq \Phi A^* \otimes_A L = \Phi A^* \otimes_K L \subseteq \Phi(A^* \otimes_A L)$, so it is enough to see that $A^* \otimes_A L$ is reduced. Let B denote the integral closure of A in L. Then B is finite over A, hence $B^* = A^* \otimes_A B$ and so $\Phi B^* \supseteq A^* \otimes_A \Phi B = A^* \otimes_A L$. But B is a semi-local Nagata domain, so that B* is reduced by Th.70. Hence ΦB^* and $A^* \otimes_A L$ are reduced. Q.E.D.

(31.G) For any scheme X, let Nor(X) denote the set of points x of X such that the local ring at x is normal.

LEMMA 3. Let A be a noetherian domain, and put $X = \operatorname{Spec}(A)$. Suppose there exists $0 \neq f \in A$ such that $A_f = A[1/f]$ is normal. Then Nor(X) is open in X.

<u>Proof</u>. If $f \notin p \in X$ then A_p is a localization of A_f, hence $p \in \operatorname{Nor}(X)$. Put $E = \{p \in \operatorname{Ass}_A(A/fA) \mid$ either $\operatorname{ht}(p) = 1$ and A_p is not regular, or $\operatorname{ht}(p) > 1\}$. Then E is of course a finite set, and by the criterion of normality (Th.39) it is not difficult to see that

$$\operatorname{Nor}(X) = X - \bigcup_{p \in E} V(p).$$

Therefore Nor(X) is open.

LEMMA 4. Let B be a noetherian domain with quotient field K, such that there exists $0 \neq f \in B$ such that $B_f = B[1/f]$ is normal. Suppose that B_p is N-1 for each maximal ideal p of B. Then B is N-1.

<u>Proof</u>. We denote the integral closure in K by '. Let p be a maximal ideal of B and write $(B_p)' = \sum_1^n B_p \omega_i$ with $\omega_i \in B'$. This is possible because $(B_p)' = B'_p = B_p[B']$. Put $C^{(p)} = B[\omega_1, \dots, \omega_n]$. Then $C^{(p)}$ is finite over B, hence is noetherian. Let P be any prime of $C^{(p)}$ lying over p. Then $(C^{(p)})_P \supseteq (C^{(p)})_p \supseteq C^{(p)}$, and $(C^{(p)})_p = (B_p)'$ is normal. Thus $(C^{(p)})_P$ is a localization of the normal ring $(B_p)'$, hence is itself normal. Put $X_p = \operatorname{Spec}(C^{(p)})$, $F_p = X_p - \operatorname{Nor}(X_p)$ and $X = \operatorname{Xpec}(B)$; let $\pi_p: X_p \to X$ be the morphism corresponding to the inclusion map $B \to C^{(p)}$. Since $C^{(p)}[1/f] = B_f$, the set F_p is closed in X_p by Lemma 3. Since $C^{(p)}$ is finite over B, the map π_p is a closed map. Thus $\pi_p(F_p)$ is a closed set in X, and $p \notin \pi_p(F_p)$ by what we have just seen. Therefore the intersection $\bigcap_{\text{all max } p} \pi_p(F_p)$ is a closed set in X which contains no closed point (= maximal ideal of B), so that we have $\bigcap \pi_p(F_p) = \emptyset$. As affine schemes are quasi-compact, there exist $p_1, \dots, p_r$ such that $\bigcap_{i=1}^r \pi_{p_i}(F_{p_i}) \neq \emptyset$. Put $C^{(i)} = C^{(p_i)}$ and $C = B[C^{(1)}, \dots, C^{(r)}]$. Then C is finite over B. We claim that C_Q is normal for any $Q \in \operatorname{Spec}(C)$. In fact we

have $Q \cap B \not\in \pi_{\mathfrak{p}_i}(F_{\mathfrak{p}_i})$ for some i, hence $Q \cap C^{(i)} \in \mathrm{Nor}(X_{\mathfrak{p}_i})$. Putting $C^{(i)} \cap Q = \mathfrak{q}$ we have $C_Q = C^{(i)}_{\mathfrak{q}}$, and since $C^{(i)}_{\mathfrak{q}}$ is normal we have $C^{(i)}_{\mathfrak{q}} \supseteq C$, hence $C_Q = C^{(i)}_{\mathfrak{q}}$. Thus our claim is proved and C is normal. Therefore B'= C, so B' is finite over B.

(31.H) THEOREM 72 (Nagata). Let A be a Nagata ring and B an A-algebra of finite type. Then B is also a Nagata ring.

Proof. The canonical image of A in B is also a Nagata ring, so we may assume that $A \subseteq B$. Then $B = A[x_1,\dots,x_n]$ with some $x_i \in B$, and by induction on n it is enough to consider the case $B = A[x]$.

Let $P \in \mathrm{Spec}(B)$. Then $B/P = (A/A \cap P)[\bar{x}]$ where $A/A \cap P$ is a Nagata domain, and we have to prove that B/P is N-2. Thus the problem is reduced to proving the following:

(*) If A is a Nagata domain, and if $B = A[x]$ is an integral domain generated by a single element x over A, then B is N-2.

Let K be the quotient field of A. It is easy to see that we may replace A by its integral closure in K. So we can assume in (*) that A is normal.

Case 1. x is transcendental.over A.

Then B is normal. Therefore if ch(B) = 0 we are done. Suppose ch(B) = p, and take a finite radical extension $L = K(x, \alpha_1, \dots, \alpha_r)$ of $\Phi B = K(x)$. Let $q = p^e$ be such that $\alpha_i^q \in K(x)$ for all i. Then there exists a finite radical extension K' of K such that $\alpha_i \in K'(x^{1/q})$. If $\tilde{A}$ (resp. $\tilde{B}$) is the integral closure of A in K' (resp. of B in L), then $\tilde{A}[x^{1/q}]$ is normal and we have $B = A[x] \subseteq \tilde{B} \subseteq \tilde{A}[x^{1/q}]$. Since $\tilde{A}[x^{1/q}]$ is finite over B, $\tilde{B}$ is also finite over B.

Case 2. x is algebraic over A.

Let L be a finite extension of ΦB. Then $[L: K] < \infty$, and if $\tilde{A}$ (resp. $\tilde{B}$) is the integral closure of A (resp. B) in L then $\tilde{A}$ is finite over A, hence $\tilde{A}[x]$ is finite over $A[x] = B$, and $B = A[x] \subseteq \tilde{A}[x] \subseteq \tilde{B}$. Therefore we have only to prove:

(†) Let A be a normal Nagata domain with quotient field K, and let $B = A[x]$, $x \in K$. Then B is N-1.

Write $x = b/a$ with $a, b \in A$. Then $B_a = B[1/a] = A[1/a]$ is normal because it is a localization of the normal ring A. Thus by Lemma 4 it is enough to prove that B_P is N-1 for any maximal ideal P of B. Put $P' = P \cap A$. Then $B/P = (A/P')[\bar{x}]$ is a field, so the image $\bar{x}$ of x in B/P is algebraic over A/P'. Hence there exists a monic polynomial $f(X) \in A[X]$ such that $f(x) \in P$. Let K" be the field obtained by adjoining all roots of f(X) to K, let A" denote the integral closure of A in K" and put $B'' = A''[x]$. Then A" is Nagata and B" is finite over B. Let P" denote any prime of B" lying over P. If $B''_{P''}$ is

N-1 for all such P" then B''_P is N-1 by Lemma 4 and it follows easily that B_P is N-1. Thus replacing A, B and P by A", B" and P" respectively we may assume that $f(X) = \Pi(X - a_i)$ with $a_i \in A$. Then $\bar{x} = \bar{a}_i$ for some i, and as we can replace x by $x - a_i$ we may assume that $x \in P$.

Let Q be the kernel of the homomorphism $A[X] \to A[x] = B$ which maps X to x. Then Q is generated by the linear forms $aX - b$ such that $x = b/a$. (For, if $F(X) = a_0X^n + a_1X^{n-1} + \dots + a_n \in Q$, then a_0x is integral over A, hence $a_0x = b \in A$ by the normality of A. Then $F(X) - (a_0X - b)X^{n-1} \in Q$, and our assertion is proved by induction on $n = \deg F(X)$.) Let I be the ideal of A generated by such b, in other words $I = xA \cap A$. We have $B/xB \simeq A[X]/(XA[X] + Q) = A[X]/(XA[X]+I) \simeq A/I$.

We want to apply Lemma 2 of (31.D) to the local ring B_P and to $x \in PB_P$. If this is possible then B_P is analytically unramified, so by (31.E) B_P is N-1, as wanted. Now the conditions of Lemma 2 are: (1) B_P/xB_P has no embedded primes, and (2) if $p \in \mathrm{Spec}(B_P)$ is any associated prime of B_P/xB_P then $(B_P)_p$ is regular and p is analytically unramified. Let us check these conditions.

Since A is a noetherian normal ring we have $A = \bigcap_{ht(q)=1} A_q$. Therefore, if $q_1, \dots, q_s$ are the prime ideals of height 1 such that $x \in q_iA_{q_i}$, then $I = xA \cap A = \bigcap_{i=1}^{s} (xA_{q_i} \cap A)$. Hence

A/I = B/xB has no embedded primes, proving (1).

Let p be an associated prime of B_P/xB_P. Then $ht(p) = 1$, and $p \cap A$ is an associated prime of $A/(xB_P \cap A) = A/I$. Thus $A_{(p \cap A)}$ is a principal valuation ring and so $(B_P)_p = A_{(p \cap A)}$. Lastly, B_P/p is a localization of $B/p \cap B$ and $B/p \cap B \simeq A/p \cap A$ since $x \in p$. Thus B_P/p is a Nagata local domain, hence is analytically unramified. Thus the condition (2) is verified and our proof is completed.

CHAPTER 13. EXCELLENT RINGS

32. Closedness of the Singular Locus

(32.A) Let A be a noetherian ring; put X = Spec(A), Reg(X) = $\{p \in X \mid A_p$ is regular$\}$ and Sing(X) = X − Reg(X). We ask whether Reg(X) is open in X.

LEMMA 1. In order that Reg(X) is open in X,
(i) it is necessary and sufficient that for each $p \in$ Reg(X), the set $V(p) \cap$ Reg(X) contains a non-empty open set of $V(p)$;
and (ii) it is sufficient that, if $p \in$ Reg(X) and Y = Spec(A/p), then Reg(Y) contains a non-empty open set of Y.

Proof. (i) This follows from (22.B) Lemma 2.
(ii) We derive the condition of (i) from (ii). Let $p \in$ Reg(X), and choose $a_1, \ldots, a_r \in p$ which form a regular system of parameters of A_p; put $I = \Sigma a_i A$. As $IA_p = pA_p$, there exists

$f \in A$ such that $IA_f = pA_f$. Then $D(f) = X - V(f) \simeq \mathrm{Spec}(A_f)$ is an open neighborhood of p in X. So, replacing A by A_f we may assume that $I = p$. Now put $Y = \mathrm{Spec}(A/p)$, and identify it with the closed subset $V(p)$ of X. By assumption, there exists a non-empty open set Y_0 of Y contained in Reg(Y). If $q \in Y_0$, then A_q/pA_q is regular and $pA_q = \sum_1^r a_i A_q$ is generated by an A_q-regular sequence. Thus $\dim A_q = \dim A_q/pA_q + r$, so that A_q is regular. Therefore $Y_0 \subseteq Y \cap \mathrm{Reg}(X)$, and the condition (i) is proved.

(32.B) Let A be a noetherian ring. We say that A is J-0 if Reg(Spec(A)) contains a non-empty open set of Spec(A), and that A is J-1 if Reg(Spec(A)) is open in Spec(A). Thus J-1 implies J-0 if A is a domain, but not in general. We say that A is J-2 if the conditions of the following theorem are satisfied.

THEOREM 73. For a noetherian ring A, the following conditions are equivalent:

(1) any finitely generated A-algebra B is J-1;

(2) any finite A-algebra B is J-1;

(3) for any $p \in \mathrm{Spec}(A)$, and for any finite radical extension K' of $\kappa(p)$, there exists a finite A-algebra A' satisfying $A/p \subseteq A' \subseteq K'$ which is J-0 and whose quotient field is K'.

Proof. (1) ⇒ (2) ⇒ (3): trivial. (3) ⇒ (1): Step I. Let p and A' be as in (3), and let $\omega_1, \ldots, \omega_n \in A'$ be a linear basis of K' over $\kappa(p)$. Then there exists $0 \neq f \in A/p$ such that $A'_f = \sum_1^n (A/p)_f \omega_i$. From this and from Th.51 (i) it follows easily that A/p is J-0. Therefore A/p (and A itself) is J-1 by Lemma 1.

Step II. In view of Lemma 1, the condition (1) is equivalent to (1'): Let B be a domain which is finitely generated over A/p for some $p \in \mathrm{Spec}\, A$. Then B is J-0.

We will prove (1'). Replacing A by A/p we may assume $A \subseteq B$. Since A is J-0 by Step I we may also assume that A is regular. Let K and K' be the quotient fields of A and B respectively.

Case 1. K' is separable over K. In this case we use only the assumption that A is regular. Let $t_1, \ldots, t_n \in B$ be a separating transcendency basis of K' over K, and put $A_1 = A[t_1, \ldots, t_n]$, $K_1 = K(t_1, \ldots, t_n)$. Then A_1 is a regular ring. There exists a basis $\omega_1, \ldots, \omega_r$ of K' over K_1 such that each $\omega_i \in B$. Replacing A by some $(A_1)_f$ ($f \in A_1$) and B by B_f, we may assume B is finite and free over A: $B = \sum_1^r \omega_i A$. Put $d = \det(\mathrm{tr}_{K'/K}(\omega_i\omega_j))$. Then $d \neq 0$ as K' is separably algebraic over K. We claim that B_d is a regular ring. Indeed, if $d \notin p' \in \mathrm{Spec}(B)$ and $p = p' \cap A$, then $B_p = \sum_1^r \omega_i A_p$, and putting $\bar{B} = B \otimes \kappa(p) = \sum_1^r \bar{\omega}_i \kappa(p)$ we get $\det(\mathrm{tr}_{\bar{B}/\kappa(p)}(\bar{\omega}_i\bar{\omega}_j)) = \bar{d} \neq 0$ in $\kappa(p)$. Therefore $\bar{B} = B \otimes \kappa(p)$ is a product of fields, and so $B_{p'} \otimes \kappa(p) = B_{p'}/pB_{p'}$ is a field. Since A_p is regular and $\dim A_p = \dim B_{p'}$, it follows that B_p is regular.

Case 2. General case. We may suppose ch(K) = p. There exists a finite purely inseparable extension K_1 of K such that $K_1' = K'(K_1)$ is separable over K_1. Choose $A_1 \subseteq K_1$ as in (3). Then A_1 is J-0, and so $A_1[B]$ is J-0 by Case 1. Since $A_1[B]$ is finite over B, B itself is J-0 as in Step I. Q.E.D.

Remark. The condition (3) is satisfied if A is a Nagata ring of dimension 1. Indeed, A/p is either a field -- in which case (3) is trivial -- or a Nagata domain of dimension 1, and then the integral closure A' of A in K' is finite over A and is a regular ring.

(32.C) THEOREM 74. Let A be a noetherian complete local ring. Then A is J-2.

Proof. Any finite A-algebra B is a finite product of complete local rings: $B = B_1 \times \dots \times B_s$, and B is J-1 iff each B_i is so. Therefore, by Th.73 and Lemma 2, it suffices to prove that a noetherian complete local domain A is J-0.

Case I. ch(A) = 0. The ring A is finite over a suitable subring B which is a regular local ring, and by the case 1 of Step II of the preceding proof we see that A is J-0.

Case II. ch(A) = p. Then A contains the prime field,

hence also a coefficient field K, so that A is of the form $K[[X_1,\dots,X_n]]/I$. Therefore A is J-1 by the Jacobian criterion of Nagata (29.F).

33. Formal Fibres and G-Rings

(33.A) In this section all rings are tacitly assumed to be noetherian.

DEFINITIONS. Let A be a ring containing a field k. We say that A is geometrically regular over k if, for any finite extension k' of k, the ring $A \otimes_k k'$ is regular. This is equivalent to saying that "A_m is geometrically regular over k for each $m \in \Omega(A)$", because if $m' \in \Omega(A \otimes k')$ and $m = m' \cap A$ then $(A \otimes k')_{m'}$ is a localization of $A_m \otimes_k k'$.

We say that a homomorphism $\phi: A \to B$ is regular (or that B is regular over A) if it is flat and if for each $p \in \operatorname{Spec}(A)$ the fibre $B \otimes_A \kappa(p)$ is geometrically regular over $\kappa(p)$. This is equivalent to saying that

> B is flat, and for any finite extension L of $\kappa(p)$, the ring $B \otimes_A L = (B \otimes_A \kappa(p)) \otimes_{\kappa(p)} L$ is a regular ring.

A noetherian ring A is called a G-ring if for any $p \in \operatorname{Spec}(A)$, the canonical map $A_p \to (A_p)^*$ of the local ring A_p into its completion is regular. (The fibres of $A_p \to (A_p)^*$ are called the formal fibres of A_p.) It is clear that, if A is a G-ring, then any localization $S^{-1}A$ and any homomorphic image A/I of A are G-rings.

Th.68 of (30.D) implies that a noetherian complete local ring is a G-ring.

(33.B) LEMMA 1. Let $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ be homomorphisms of rings.

(i) If ϕ and ψ are regular, so is $\psi\phi$.

(ii) If $\psi\phi$ is regular and if ψ is faithfully flat, then ϕ is regular.

Proof. (i) Clearly $\psi\phi$ is flat. Let $p \in \mathrm{Spec}(A)$, $K = \kappa(p)$ and L = a finite extension of K. Put $B_{(L)} = B \otimes_A L$ and $C_{(L)} = C \otimes_A L$. It is easy to see that

$$\psi_L = \psi \otimes \mathrm{id}_L : B_{(L)} \to C_{(L)}$$

is regular. Moreover, if $P' \in \mathrm{Spec}(C_{(L)})$ and $P = P' \cap B_{(L)}$, then $B_{(L)P}$ is a regular local ring (as ϕ is regular). Then $C_{(L)P'}$ is regular by (21.D) Th.51(ii) as it is flat over $B_{(L)P}$.

(ii) Again the flatness of ϕ is obvious. Using the same notation as above, for any $P \in \mathrm{Spec}(B_{(L)})$ there exists $P' \in \mathrm{Spec}(C_{(L)})$ lying over P (because ψ_L is f.f.), and the local ring $C_{(L)P'}$ is regular and flat over $B_{(L)P}$. Therefore the

local ring $B_{(L)P}$ is regular by (21.D) Th.51(i).

LEMMA 2. Let $\phi: A \to B$ be a faithfully flat, regular homomorphism. Then:

(i) A is regular (resp. normal, resp. C.M., resp. reduced) iff B has the same property.

(ii) If B is a G-ring, so is A.

Proof. (i) follows from (21.D) and (21.E).

(ii) Suppose B is a G-ring, and let $p \in \mathrm{Spec}(A)$. Take a prime ideal P of B lying over p, and consider the commutative diagram

$$\begin{array}{ccc} (A_p)^* & \xrightarrow{f^*} & (B_P)^* \\ \uparrow{\scriptstyle\alpha} & & \uparrow{\scriptstyle\beta} \\ A_p & \xrightarrow{f} & B_P \end{array}$$

where f is the local homomorphism derived from ϕ, and α and β are the natural maps. Since f and β are flat, $f^*\alpha = \beta f$ is flat also. Then, by the local criterion of flatness Th.49(5), f^* is flat (hence faithfully flat). On the other hand $f^*\alpha = \beta f$ is regular as f and β are so, hence by Lemma 1 we see that α is regular, which was to be proved.

(33.C) THEOREM 75. Let A be a noetherian ring. If, for every maximal ideal m of A, the natural map $A_m \to (A_m)^*$ is regular, then A is a G-ring.

Proof. We can assume that A is a local ring with $A \to A^*$ regular. Then A^* is a G-ring by Th.68, Hence A is a G-ring by Lemma 2.

(33.D) THEOREM 76.*) i) Let A,B be noetherian rings and $f: A \to B$ be a faithfully flat and regular homomorphism. If B is J-1 (i.e. Reg(B) is open in Spec(B)), so is A.

ii) A semi-local G-ring is J-1.

Proof. i) Put X = Spec(B) and Y = Spec(A). Then the canonical map $f: X \to Y$ is submersive by (6.H) Th.7. On the other hand we have $f^{-1}(\mathrm{Reg}(A)) = \mathrm{Reg}(B)$ by Lemma 2 (i). Since Reg(B) is open in Y, Reg(A) must be open in X.

ii) Apply the above to $A \to A^*$ and use Th.74.

(33.E) LEMMA 3. A noetherian semi-local ring A is a G-ring iff, for any local domain C which is a localization of a finite A-algebra B with respect to a maximal ideal, and for any prime ideal Q of C^* with $Q \cap C = (0)$, the local ring C^*_Q is regular.

Proof. "Only if". Let A be a G-ring. Then the image of A in B is also a G-ring, hence we may assume that $A \subseteq B$. We may also assume that B is a domain. Let $L = \Phi B$ and $K = \Phi A$. Since $B^* = B \otimes_A A^*$ and since C^* is a component of B^*, we have

$$C^*_Q = (L \otimes_B B^*)_{Q'} = (L \otimes_K (K \otimes_A A^*))_{Q'} = (L \otimes_K A^*_q)_{Q'}$$

with $Q' = QC^*_Q \cap (L \otimes B^*)$ and $q = Q \cap A^*$. Since A^*_q is geometrically regular over K we see that C^*_Q is regular.

"If". Let $p \in \mathrm{Spec}(A)$ and let L be a finite extension of $\kappa(p)$. Then it is clear that we can find a finite A-algebra B such that $A/p \subseteq B \subseteq L$ and $\Phi B = L$. We have $L \otimes_A A^* = L \otimes_B (B \otimes_A A^*) = L \otimes_B B^*$, and the local rings of this ring are of the form B^*_Q with $Q \cap B = (0)$, hence regular. Q.E.D.

*) We may replace J-1 by J-2 in the theorem in view of Lemma 4 below.

LEMMA 4. Let $A \to B$ be a regular homomorphism and let A' be an A-algebra of finite type. Put $B' = A' \otimes_A B$. Then $A' \to B'$ is regular.

Proof. Let $P' \in \mathrm{Spec}(A')$, and put $P = P' \cap A$, $k = \kappa(P)$ and $K = \kappa(P')$. Let L be a finite extension of K. Then $L \otimes_{A'} B' = L \otimes_A B = L \otimes_k (k \otimes_A B)$. Since K is finitely generated over k, L is also finitely generated over k. Thus there exists a finite radical extension k' of k such that L(k') is separably generated over k'. Put $M = L(k')$, $T = k' \otimes_A B$. By assumption T is a regular ring. We have $M \otimes_{A'} B' = M \otimes_A B = M \otimes_{k'} (k' \otimes_A B) = M \otimes_{k'} T$, and M is finitely generated and separable over k'. Then it is easy to see that the homomorphism $T \to M \otimes_{k'} T$ is regular, and since T is regular the ring $M \otimes_{A'} B' = M \otimes_{k'} T$ is regular by Lemma 2. Since $M \otimes_{A'} B' = M \otimes_L (L \otimes_{A'} B')$ is flat over $L \otimes_{A'} B'$, the ring $L \otimes_{A'} B'$ is regular by Th.51. Q.E.D.

(33.F) LEMMA 5. Let A be a noetherian ring and put X =

Spec(A). Let Z be a non-empty, locally closed set in X. Then Z contains a point p such that $\dim(A/p) \leqslant 1$. (Geometrically speaking, Z contains either a 'point' or a 'curve'.)

<u>Proof</u>. Shrinking Z if necessary, we may suppose that Z is of the form $D(f) \cap V(P)$ with $f \in A$ and $P \in X$ such that $f \notin P$. Then Z is homeomorphic to $\mathrm{Spec}((A/P)_{\bar{f}})$ where $\bar{f}$ is the image of f in A/P. Let m be a maximal ideal of the ring $(A/P)_{\bar{f}}$, and let p be the inverse image of m in A. Then

$$A_f/pA_f = (A/P)_{\bar{f}}/m = \text{a field},$$

hence if g is the image of f in A/p then $A_f/pA_f = (A/p)[g^{-1}]$ is a field. This means that all non-zero prime ideals of the noetherian domain A/p contain g, which is impossible if $\dim A/p > 1$ because a noetherian domain of dimension > 1 has infinitely many prime ideals of height 1 (cf. (1.B) and (12.I)).

(33.G) THEOREM 77 (Grothendieck). Let A be a G-ring and B a finitely generated A-algebra. Then B is a G-ring.

<u>Proof</u>. Step I. We may assume that B = A[t]. Let P be a maximal ideal of B and put $p = P \cap A$. We are to prove that $B_P \to (B_P)^*$ is regular. Since B_P is a localization of $A_p[t]$ we may assume that A is a local ring and $P \cap A = \mathrm{rad}(A)$. Put $\mathfrak{m} = \mathrm{rad}(A)$.

Step II. The map $B \to B' = B \otimes_A A^*$ induced by $A \to A^*$ is regular by Lemma 4 and f.f., and if P' is a maximal ideal of B' lying over P, the proof of Lemma 2(ii) shows that $B_P \to (B_P)^*$ is regular if $B'_{P'} \to (B'_{P'})^*$ is regular. The ring $B' = A[t] \otimes_A A^*$ is of the form $A^*[t]$. So we may assume that $(A, \mathfrak{m})$ is a complete local ring, B = A[t] and P is a maximal ideal of B lying over $\mathfrak{m}$. Putting $C = B_P$, we want to show that $C \to C^*$ is regular, in other words (Th.75) that C is a G-ring. By Lemma 3 it suffices to show the following: if D is a finite C-algebra which is a domain, and if Q is a prime ideal of D^* with $Q \cap D = (0)$, then the local ring D^*_Q is regular. The various rings considered are related as follows.

$$A = A^* \longrightarrow B = A[t] \longrightarrow C = B_P \xrightarrow{\text{finite}} D \longrightarrow D^* \longrightarrow D^*_Q.$$

Denote the kernel of $C \to D$ by I. Since D is a domain, I is a prime ideal. Replacing A by $A/(A \cap I)$, B by $B/(B \cap I)$ and P by P/I, we may further assume that A is a complete local domain.

Step III. Put $X = \mathrm{Spec}(D)$ and $X' = \mathrm{Spec}(D^*)$, and let $f: X' \to X$ be the canonical map. It suffices to prove $f^{-1}(\mathrm{Reg}(X)) = \mathrm{Reg}(X')$. Indeed, since D is a domain we have $f(Q) = Q \cap D = (0) \in \mathrm{Reg}(X)$, and our goal was $Q \in \mathrm{Reg}(X')$.

Step IV. Proof of $f^{-1}(\mathrm{Reg}(X)) = \mathrm{Reg}(X')$.

Suppose that they are not equal. Since the complete local

ring A is J-2 by Th.74, $B = A[t]$ and $C = B_P$ are also J-2. Hence D is J-1, i.e. Reg(X) is open in X. On the other hand Reg(X') is open in X' by Th.74. So $f^{-1}(\mathrm{Reg}(X)) \cap \mathrm{Sing}(X')$ is locally closed, and we have assumed that the intersection is not empty. We want to derive a contradiction from this.
By Lemma 5 there exists $p' \in f^{-1}(\mathrm{Reg}(X)) \cap \mathrm{Sing}(X')$ such that $\dim(D^*/p') \leq 1$. The prime p' of D^* is not a maximal ideal, because otherwise $f(p') = D \cap p'$ would be a maximal ideal of D and $f(p') \in \mathrm{Reg}(X)$ would imply that $D_{f(p')}$ is regular. Then $D^*_{p'} = D_{f(p')}^*$ must be regular, contrary to the assumption that $p' \in \mathrm{Sing}(X)$. Therefore we have $\dim(D^*/p') = 1$.

Put $p = p' \cap D$. Then D_p is regular and $D^*_{p'}$ is not regular, and $D_p \to D^*_{p'}$ is faithfully flat. Hence, by (21.D) Th. 51, $D^*_{p'} \otimes_D (D/p)$ is not regular. Replacing D^* by D^*/pD^*, D by D/p, C by $C/C \cap p$ etc., we may assume that $p = (0)$.
Thus we have

$$A = A^* \hookrightarrow B = A[t] \hookrightarrow C = B_P \xrightarrow{\text{finite}} D \hookrightarrow D^*/p'.$$

We distinguish two cases.
<u>Case</u> 1. D^*/p' is finite over A. Then D is also finite over A, hence D is complete. Thus $D^* = D$, hence $p' = (0)$ and $D^*_{p'}$ is a field, contrary to the assumption $p' \in \mathrm{Sing}(X')$.
<u>Case</u> 2. D^*/p' is not finite over A. Put $E = D^*/p'$, $\mathfrak{m}_A = \mathrm{rad}(A)$, $\mathfrak{m}_E = \mathrm{rad}(E)$ etc.. Since P is a maximal ideal of $B = A[t]$, lying over $\mathfrak{m}_A$ the residue field $C/\mathfrak{m}_C$ is finite over $A/\mathfrak{m}_A$. Moreover, $E/\mathfrak{m}_E$ is a homomorphic image of $D^*/\mathfrak{m}_{D^*} = D/\mathfrak{m}_D$ and $D/\mathfrak{m}_D$ is finite over $C/\mathfrak{m}_C$. Hence $E/\mathfrak{m}_E$ is finite over $A/\mathfrak{m}_A$. Therefore, if $\mathfrak{m}_A E$ contains a power of $\mathfrak{m}_E$ then $E/\mathfrak{m}_A E$ is also finite over $A/\mathfrak{m}_A$, and E itself must be finite over A by the Lemma at the end of §28. Thus $\mathfrak{m}_A E$ does not contain any power of $\mathfrak{m}_E$. But E is a noetherian local domain of dimension 1, so we must have $\mathfrak{m}_A E = (0)$. Hence also $\mathfrak{m}_A = (0)$, i.e. A is a field. Then we get $\dim D \leq 1$ by construction. Therefore $\dim D^* = 1$ and p' (not being maximal) must be a minimal prime of D^*. Now D is a Nagata ring by Th.72, hence D^* is reduced. Therefore $D^*_{p'}$ is a field and we get a contradiction again. Q.E.D.

(33.H) THEOREM 78. Let A be a G-ring which is J-2. Then A is a Nagata ring.

<u>Proof</u>. Let $p \in \mathrm{Spec}(A)$, and let K be the quotient field of A/p, L a finite extension of K and B the integral closure of A in L. We have to prove that B is finite over A. Let A' be a finite A-algebra such that $A/p \subseteq A' \subseteq B$ and $\Phi A' = L$. Then A' is a G-ring by Th.76 and is J-2. Thus, replacing A by A', the problem is reduced to proving that a noetherian J-2 domain which is a G-ring is N-1 (i.e. the integral closure

B of A in K = ΦA is finite over A). Put X = Spec(A). Then Reg(X) is non-empty and open in X, and is of course contained in Nor(X). So, by (31.G) Lemma 4 we have only to show that $A_{\mathfrak{m}}$ is N-1 for each maximal ideal $\mathfrak{m}$ of A. But $A_{\mathfrak{m}}$ is reduced and $A_{\mathfrak{m}} \to (A_{\mathfrak{m}})^*$ is regular, so by (33.B) Lemma 2 the ring $(A_{\mathfrak{m}})^*$ is reduced. Therefore $A_{\mathfrak{m}}$ is N-1 by (31.E). Q.E.D.

(33.I) THEOREM 79 (Analytic normality of normal G-rings). Let A be a G-ring and I an ideal of A. Let B denote the I-adic completion of A. Then the canonical map A → B is regular. Consequently, B is normal (resp. regular, resp. C.M., resp. reduced) if A is so.

Proof. It is clear from the definition that A → B is regular iff, for any maximal ideal $\mathfrak{m}'$ of B, the map $A_{\mathfrak{m}} \to B_{\mathfrak{m}'}$ ($\mathfrak{m} = \mathfrak{m}' \cap A$) is regular. Now, since $\mathfrak{m}'$ is maximal, $\mathfrak{m}$ is a maximal ideal of A containing I by (24.A). Furthermore the local rings $A_{\mathfrak{m}}$ and $B_{\mathfrak{m}'}$ have the same completion (cf.24.D). Thus in the diagram

$$A_{\mathfrak{m}} \xrightarrow{h} B_{\mathfrak{m}'} \xrightarrow{g} (B_{\mathfrak{m}'})^* = (A_{\mathfrak{m}})^*,$$

gh is regular and g is f.f., so that h is regular by (33.B) Lemma 1. Thus A → B is regular. The second assertion follows from this by (33.B) Lemma 2.

34. Excellent Rings

(34.A) DEFINITION. We say that a ring A is excellent (resp. quasi-excellent) if the following conditions (resp. (1),(3) and (4)) are satisfied:

(1) A is noetherian;

(2) A is universally catenary (cf. pp.84-86);

(3) A is a G-ring (cf. 33.B);

(4) A is J-2 (cf. 32.B Th.73).

Each of these conditions is stable under the two important operations on rings: the localization and the passage to a finitely generated algebra. (Stability of J-2 under localization follows from the criterion (3) of Th.73.) Thus the class of (quasi-)excellent rings is stable under these operations. Note also that (2),(3),(4) are conditions on A/P, P ε Spec(A). Thus a noetherian ring A is (quasi-)excellent iff A_{red} is so.

A quasi-excellent ring is a Nagata ring (Th.78).

If A is a local ring and if it satisfies (1) and (3) then it is quasi-excellent (Th.76, Th.77 and Th.73). In the general case, note that the conditions (2) and (3) are of local nature (in the sense that if they hold for $A_{\mathfrak{p}}$ for all $\mathfrak{p}$ ε Spec(A), then they hold for A), while (4) is not.

(34.B) Noetherian complete semi-local rings are excellent ((28.P), Th.68, Th.74). In particular, formal power series rings over a field are excellent. Convergent power series rings over $\mathbb{R}$ or $\mathbb{C}$ are excellent (cf. Th.102 and the remark after that). It is easy to see that a Dedekind domain (i.e. noetherian normal domain of dimension one) of characteristic zero is excellent. On the other hand, there exists a regular local ring of dimension one and of characteristic p which is not excellent. [Take a field k of char. p with $[k:k^p] = \infty$, put $R = k[[x]]$ and let A be the subring of R consisting of the power series $\Sigma a_i x^i$ such that $[k^p(a_0,a_1,\ldots):k^p] < \infty$. Then A is regular and $A^* = R$. Since $R^p \subseteq A$ the quotient field ΦR is purely inseparable over ΦA. Thus A is not a G-ring, not even a Nagata ring by Th.71.]

Let K be a field, $ch(K) \neq 2$. Then there exist a regular local ring R of dimension 2 containing K and a prime element z of R such that $S = R[z^{1/2}]$ is a normal local ring whose completion S^* has zero-divisors. (Nagata, LOCAL RINGS p.210, (E7.1)). Thus R is not Nagata.

C. Rotthaus (Math. Z. 152 (1977), 107-125) constructed a regular local ring R of dimension three which contains a field and which is Nagata but not quasi-excellent.

The ring A of p.88 is a G-ring which is not u.c..

(34.C) One can ask the following questions:

(A) If A is quasi-excellent, is A[[X]] quasi-excellent ?

(A') If A is as above and I is an ideal, is the I-adic completion A^* of A qusi-excellent ?

(B) If (A, I) is a complete Zariski ring with A/I quasi-excellent, is A also quasi-excellent ?

Of course (A) and (A') are equivalent, and (B) is stronger. These questions are still open in the general case, cf. §43.

Appendix

35. Eakin's Theorem

A module is said to be noetherian (resp. artinian) if the ascending (resp. descending) chain condition for submodules holds. It is easy to see that if $0 \to M' \to M \to M''$ $\to 0$ is exact and if M' and M'' are noetherian (resp. artinian), so is M. A module is noetherian iff all submodules are finitely generated.

A module is called faithful if $Ann(M) = (0)$.

LEMMA. Let A be a ring and M an A-module. If M is faithful and noetherian, then A is a noetherian ring.

Proof. Let $M = A\omega_1 + \ldots + A\omega_n$. Then A is embedded in M^n as A-module by the map $a \to (a\omega_1,\ldots,a\omega_n)$. Since M^n is noetherian, so is A.

THEOREM 80 (E. Formanek, Proc. AMS 41 (1973), 381-383). Let A be a ring and B be a faithful and finite A-module. If the ascending chain condition holds for the submodules of the form IB, where I is an ideal of A, then A is noetherian.

Proof. It suffices to prove that B is a noetherian A-module. Assume the contrary. Then the set $\{IB \mid I$ is an ideal of A and B/IB is a non-noetherian A-module$\}$ is not empty, hence it has a maximal element I_0B. Replacing B and A by B/I_0B and $A/\mathrm{Ann}(B/I_0B)$, we may assume that B is not noetherian but B/IB is noetherian for every non-zero ideal I of A. Put $\Gamma = \{N \mid N$ is a submodule of B and B/N is faithful$\}$. If $B = A\omega_1 + \dots + A\omega_n$ then a submodule N of B belongs to Γ iff $\{a\omega_1, \dots, a\omega_n\} \not\subset N$ for every $0 \neq a \in A$. Therefore we can use Zorn to conclude that Γ has a maximal element N_0. Replacing B by B/N_0 we get the situation where (1) B is not noetherian (for, otherwise A and our original B would be noetherian), (2) B/IB is noetherian for every non-zero ideal I of A, and (3) B/N is not faithful for every non-zero submodule N of B. But this is absurd. In fact, there exists by (1) a submodule N of B which is not finite over A. Then there exists $0 \neq a \in A$ such that $aB \subset N$ by (3). Since B/aB is noetherian, the A-module N/aB must be finitely generated. Therefore N itself is finite over A, contradiction.

COROLLARY (Eakin). If B is a noetherian ring and A is a subring of B such that B is finite over A, then A is noetherian.

36. A Flatness Theorem

(36.A) LEMMA. Let A be a ring and M be an A-module. Let x be an element of A which is M-regular and A-regular, and N be an A-module with $xN = 0$. Put $A' = A/xA$, $M' = M/xM$. Then:

(1) $\mathrm{Tor}_n^A(M, N) \simeq \mathrm{Tor}_n^{A'}(M', N)$ for all $n \geq 0$,

(2) $\mathrm{Ext}_A^n(M, N) \simeq \mathrm{Ext}_{A'}^n(M', N)$ for all $n \geq 0$,

(3) $\mathrm{Ext}_A^{n+1}(N, M) \simeq \mathrm{Ext}_{A'}^n(N, M')$ for all $n \geq 0$, and $\mathrm{Hom}_A(N, M) = 0$.

Proof. (1) and (2): The exact sequence $0 \to A \xrightarrow{x} A \to A' \to 0$ is a free resolution of A'. Since $0 \to M \xrightarrow{x} M \to M \otimes_A A' \to 0$ is also exact, we have $\mathrm{Tor}_i^A(M, A') = 0$ for all $i > 0$. Let $L_\cdot \to M \to 0$ be a free resolution of M. Since $H_i(L_\cdot \otimes_A A') = \mathrm{Tor}_i^A(M, A') = 0$ $(i > 0)$, $L_\cdot \otimes_A A'$ is a free resolution of the A'-module M'. Now (1) and (2) are immediate.

(3): $\mathrm{Hom}_A(N,M) = 0$ is obvious. For $n \geq 0$, put $T^n(N) = \mathrm{Ext}_A^{n+1}(N, M)$ and view them as functors on A'-modules. From $0 \to M \xrightarrow{x} M \to M' \to 0$ we get $T^0(N) = \mathrm{Hom}_{A'}(N, M')$. Since $\mathrm{proj.dim}_A A' = 1$ we have $T^n(A') = 0$ for $n > 0$, hence $T^n(N) = 0$ for $n > 0$ if N is projective over A'. If $0 \to N' \to N \to N'' \to 0$ is an exact sequence of A'-modules, then we have the long exact sequence $0 \to T^0(N'') \to T^0(N) \to T^0(N') \to T^1(N'') \to T^1(N) \to T^1(N') \to T^2(N'') \to \dots$. Thus $T^i(-)$ are the derived functors of $\mathrm{Hom}_{A'}(-, M')$, i.e. $T^i(-) = \mathrm{Ext}^i_{A'}(-, M')$.

(36.B) Let (A, m) and (B, n) be noetherian local rings and $\phi : A \to B$ be a local homomorphism. Put $F = B/mB$. If B is flat over A, we have $\dim B = \dim A + \dim F$ by Th.19. The converse is also true in some case. (Cf. Th.46.)

THEOREM 81. Let the notation be as above. Assume that A is regular, B is Cohen-Macaulay and $\dim B = \dim A + \dim F$. Then B is flat over A.

<u>Proof</u>. Induction on dim A. If $\dim A = 0$ then A is a field. Suppose $\dim A > 0$, and take $x \in m - m^2$. Put $A' = A/xA$, $B' = B/xB$. Then $\dim B' \leqslant \dim A' + \dim F = \dim A - 1 + \dim F = \dim B - 1$ by Th.19, but $\dim B' \geqslant \dim B - 1$ (by (12.F), or consider system of parameters of B'). Therefore $\dim B' = \dim B - 1$, x is B-regular and B' is CM. Hence B' is flat over A' by induction hypothesis, and so $\mathrm{Tor}_1^{A'}(A/m, B') = 0$. Since x is A-regular and B-regular, we have $\mathrm{Tor}_1^A(A/m, B) = \mathrm{Tor}_1^{A'}(A/m, B') = 0$. Therefore B is flat over A by Th.49. (Cf. EGA IV (6.1.5).)

37. Coefficient Rings

In this section we will prove the Cohen structure theorem (p.211) in the unequal characteristic case by the method of Grothendieck.

THEOREM 82. Let $(A, \mathfrak{m}, k)$ be a local ring and let B be a flat A-algebra. Put $B_0 = B/\mathfrak{m}B = B \otimes_A k$. If B_0 is smooth over k then B is formally smooth over A with respect to the $\mathfrak{m}B$-adic topology.

<u>Proof</u>. By the definition of formal smoothness we have only to show that $B/\mathfrak{m}^iB$ is smooth over $A/\mathfrak{m}^i$ for every i. Thus we can assume that $\mathfrak{m}$ is nilpotent. Then B is free over A by (3.G), and so any A-algebra extension of B by a B-module is a Hochschild extension, cf. (25.C). Therefore the proof of smoothness of B reduces, as in (28.H), to showing that every symmetric 2-cocycle $f: B \times B \to N$ with values in a B-module N is a coboundary. Suppose first that N satisfies $\mathfrak{m}N = 0$. In this case f is essentially a cocycle on B_0; namely, there exists a symmetric 2-cocycle $f_0: B_0 \times B_0 \to N$ such that $f(x,y) = f_0(\bar{x},\bar{y})$. Since B_0 is smooth over k we have $f_0 = \delta g_0$ for some k-linear map $g_0: B_0 \to N$. Putting $g(x) = g_0(\bar{x})$ we have $f = \delta g$. In the general case let $\phi: N \to N/\mathfrak{m}N$ denote the natural map. Then $\phi \circ f: B \times B \to N/\mathfrak{m}N$

splits, i.e., there exists an A-linear map $\bar{g}: B \to N/\mathfrak{m}N$ such that $\phi \circ f = \delta\bar{g}$. As B is projective over A the map $\bar{g}$ can be lifted to an A-linear map $g: B \to N$, and $f - \delta g$ is a 2-cocycle with values in $\mathfrak{m}N$. Repeating the same argument we can find $h: B \to \mathfrak{m}N$ such that $f - \delta(g+h)$ has values in $\mathfrak{m}^2N$, and so on. Since $\mathfrak{m}$ is nilpotent we see that f is a coboundary.

THEOREM 83. Let (A,tA,k) be a principal valuation ring and K be an extension field of k. Then there exists a principal valuation ring B containing A with maximal ideal generated by t and with residue field k-isomorphic to K.

Proof. Let $\{x_\lambda\}_{\lambda\in\Lambda}$ be a transcendency basis of K over k and put $k_1 = k(\{x_\lambda\})$. Let $\{X_\lambda\}_{\lambda\in\Lambda}$ be a set of independent indeterminates and put $A[\{X_\lambda\}] = A'$, $A_1 = A'_{tA'}$. Then A' is a free A-module, so that A' and A_1 are separated in the t-adic topology. Therefore A_1 is a principal valuation ring with residue field k_1. So we can assume that K is algebraic over k. Let L be the algebraic closure of the quotient field of A. Let $\mathfrak{F}$ denote the set of the pairs (B, ϕ) of a subring B of L containing A and an A-algebra homomorphism $\phi: B \to K$ such that B is a principal valuation ring with rad(B) = Ker ϕ = tB, and define an order in $\mathfrak{F}$ by

$$(B,\phi) < (C,\psi) \iff B \subset C \text{ and } \phi = \psi|B.$$

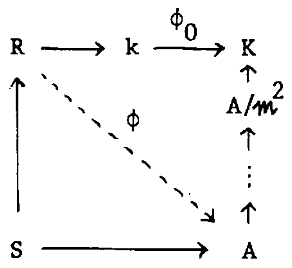
One can easily check that $\mathfrak{F}$ satisfy the condition of Zorn's lemma, therefore there exists a maximal element (B,ϕ) in $\mathfrak{F}$. If $\phi(B) \neq K$, take an element $a \in K - \phi(B)$, let $\bar{f}(X)$ be the irreducible equation of a over $\phi(B)$ and lift it to a monic polynomial $f(X) \in B[X]$. Since B is normal, f is irreducible over the quotient field of B. Let α be a root of f in L and put $B' = B[\alpha]$; then $B' = B[X]/(f)$, so that we have $B'/tB' = B[X]/(t,f) = \phi(B)(a)$. Since B' is integral over B all maximal ideals of B' must contain tB', therefore B' is a local ring with tB' as maximal ideal. Clearly B' is a noetherian domain, so B' must be a principal valuation ring. This contradicts the maximality of (B,ϕ) in $\mathfrak{F}$. Thus $\phi(B) = K$.

Remark 1. If (A, tA) is a principal valuation ring and M is an A-module, then M is flat over A iff t is M-regular. This is an immediate consequence of (3.A) Th.1 (3). In particular the ring B of the above theorem is flat over A.

Remark 2. In EGA 0_{III} (10.3.1) the following more general theorem is proved: if $(A,\mathfrak{m},k)$ is a noetherian local ring and K is an extension field of k, then one can find a noetherian local ring B containing A and flat over A such that $\text{rad}(B) = \mathfrak{m}B$, $B/\mathfrak{m}B \simeq K$.

THEOREM 84. Let $(A,\mathfrak{m},K)$ be a complete, separated local ring, (R,pR,k) be a principal valuation ring and $\phi_0: k \to K$ be a homomorphism of fields. Then there exists a local homomorphism $\phi: R \to A$ which induces ϕ_0.

Proof. Put $S = Z_{pZ}$ and let k_0 be the prime field in k. Since ch(K) = ch(k) = p, the canonical homomorphism $Z \to A$ can be extended to a local homomorphism $S \to A$. Similarly R is an S-algebra, which is flat by Remark 1. Since R/pR = k is separable (hence smooth) over k_0, R is formally smooth over S in the pR-adic topology by Th.82. Therefore we can lift the map $R \to k \to K$ to $\phi: R \to A$.



THEOREM 85. A complete separated local ring has a coefficient ring. (Cf. p.211.)

Proof. This follows from Th.83 and Th.84.

38. p - Basis

(38.A) Let R be a ring of characteristic p > 0, and let R^p denote the subring $\{x^p \mid x \in R\}$. Let S be a subring of R. A subset $B \subseteq R$ is said to be p-independent (in R) over S if the monomials $b_1^{e_1}\dots b_n^{e_n}$, where $b_1,\dots,b_n$ are distinct elements of B and $0 \leqslant e_i < p$, are linearly independent over $R^p[S]$. When A is a ring of characteristic p, a polynomial (or a monomial) $f \in A[X_1,\dots,X_n]$ is said to be reduced if it is of degree < p in each variable X_i. B is called a p-basis of R over S if it is p-independent over S and $R^p[S,B] = R$, i.e. if every element a of R can be written uniquely as a reduced polynomial $a = f(b_1,\dots,b_n)$ in distinct elements b_i of B with coefficients in $R^p[S]$.

If B is a p-basis and M is an R-module, then any map $\phi: B \to M$ is uniquely extended to a derivation $D: R \to M$ over S by $D(a) = D(f(b)) = \sum_i \partial f/\partial b_i\ \phi(b_i)$, where $a = f(b)$ is the unique representation of $a \in R$ as a reduced polynomial in elements of B with coefficients in $R^p[S]$. It follows that $\Omega_{R/S}$ is a free R-module with basis $\{db \mid b \in B\}$.

(38.B) If k,k' are subfields of a field K, the subfield generated by them will be denoted by kk'; thus kk' = k(k') = k'(k). Let K be a field of characteristic p and K' be a subfield containing K^p. If $[K:K^p]$ is finite it is a power p^n of p; its exponent n is called the p-degree of K/K' and will be denoted by $(K:K')_p$. This is equal to the smallest number of generators of K over K', and also equal to the rank of the K-module $\Omega_{K/K'}$.

Let K be a field of characteristic p and k be a subfield. Since $K^p[k] = K^p(k) = K^pk$, a subset B of K is p-independent over k iff, for every finite subset B' of B, we have $(K^pk(B'):K^pk)_p = \mathrm{Card}(B')$. Also B is a p-basis of K/k iff it is p-independent over k and $K^pk(B) = K$. By Zorn's lemma any p-independent subset is contained in a p-basis.

THEOREM 86. Let K and k be as above, B be a subset of K and let dB denote the subset $\{db \mid b \in B\}$ in $\Omega_{K/k}$. Then:

i) B is p-independent over k $\Leftrightarrow$ dB is linearly indep./K,

ii) B is a p-basis of K/K $\Leftrightarrow$ dB is a basis of $\Omega_{K/k}$ over K.

Proof. If B is a p-basis we have already seen that $\Omega_{K/k}$ is a free K-module with basis dB. If B is p-independent then there exists a p-basis containing B, hence dB is lin. indep. over K. On the other hand if B is not p-independent then there exist $b, b_1,\dots,b_n \in B$ such that $b \in K^pk(b_1,\dots,b_n)$, and then $db \in \Sigma\, Kdb_i$. Therefore if dB is linearly independent then B is p-independent, and there exists a p-basis B' containing B. If dB is a basis of $\Omega_{K/k}$ then B = B'.

(38.C) Let K be an arbitrary field and k be a subfield. The K-module $\Omega_{K/k}$ is generated over K by dK, therefore there exists a subset B such that $dB = \{db \mid b \in B\}$ is a basis of $\Omega_{K/k}$. Such a subset B is called a differential basis of K/k. The concept of differential basis coincides with that of p-basis in the case of characteristic p as we have just seen. In case ch(K) = 0 it coincides with that of transcendency basis by the following theorem.

THEOREM 87. Let $K \supset k$ be fields of characteristic 0. Then:

i) $B \subset K$ is algebraically dependent over k iff dB is linearly independent over K in $\Omega_{K/k}$,

ii) $B \subset K$ is a transcendency basis of K/k iff dB is a linear basis of $\Omega_{K/k}$ over K.

Proof. Similar to the proof of the preceding theorem.

(38.D) THEOREM 88. Let K/k be a field extension. Then the following is equivalent:

(1) K is separable over k,

(2) for any subfield k' of k, the canonical map $\Omega_{k/k'} \otimes_k K \to \Omega_{K/k'}$ is injective,

(3) the canonical map $\Omega_k \otimes_k K \to \Omega_K$ is injective,

(4) any derivation D from k to a K-module M can be extended to a derivation $K \to M$.

Proof. It is clear that (2) and (4) are equivalent. But (4) is also equivalent to (3). If ch(K) = 0 then (3) holds by the preceding theorem, so (1), (2), (3) and (4) are all true. If ch(K) = p, (1) is equivalent to $K \otimes_k k^{p^{-1}} \simeq Kk^{p^{-1}}$ by MacLane's theorem (p.196), or what is the same, to linear disjointness of K^p and k over k^p. Therefore, K is separable over k $\Leftrightarrow$ the reduced monomials in the elements of a p-basis B of k/k^p are linearly independent over K^p $\Leftrightarrow$ dB is linearly independent over K in Ω_K $\Leftrightarrow$ $\Omega_k \otimes K \to \Omega_K$ is injective.

THOREM 89. Let K be a separable extension of a field k of characteristic p, and let B be a p-basis of K/k. Then B is algebraically independent over k.

Proof. Assume the contrary and suppose $b_1,\dots,b_n \in B$ are algebraically dependent over k. Take an algebraic relation

$$f(b_1,\dots,b_n) = 0, \qquad f \in k[X_1,\dots,X_n]$$

of lowest possible degree. Put deg f = d. Write

$$f(X) = \sum_{0 \leq \nu_1,\dots,\nu_n < p} g_{\nu_1,\dots,\nu_n}(X^p)\, X_1^{\nu_1}\cdots X_n^{\nu_n},$$

where $g_{(\nu)}$ are polynomials with coefficients in k. Since

$b_1,\dots,b_n$ are p-independent over k, we must have $g_{(\nu)}(b^p) = 0$ for all (ν). By the choice of f this happens only if

$$f(X_1,\dots,X_n) = g_{0,\dots,0}(X_1^p,\dots,X_n^p).$$

But then we would have $f(X) = h(X)^p$ with $h \in k^{p^{-1}}[X_1,\dots,X_n]$. Hence h(b) = 0. By MacLane's theorem (p.196), however, K and $k^{p^{-1}}$ are linearly disjoint over k. The monomials of degree $< d$ in $b_1,\dots,b_n$ are linearly independent over k, hence they must be linearly independent over $k^{p^{-1}}$ also. This is a contradiction.

(38.E) We defined formal smoothness (p.199) by the condition of liftability (FS). If we further require that the lifting v' of v is unique, then we say that A is <u>formally etale</u> over k. Here we are mainly concerned with field extensions, so that we consider only discrete topologies.

Let K/k be an extension of fields. If ch(K) = 0, then "formally smooth" and "separably algebraic" are the same thing. If ch(K)= p, however, "formally etale" is weaker than "separably algebraic". (Consider the case where both K and k are perfect. Then K is formally etale over k.) In any case, the following are easily seen to be equivalent:

(1) K is formally etale over k,

(2) K is smooth over k and $\Omega_{K/k} = 0$,

(3) $\Omega_k \otimes_k K \simeq \Omega_K$,

(4) for any subfield k' of k, $\Omega_{k/k'} \otimes K \simeq \Omega_{K/k'}$,

(5) any derivation from k into a K-module M can be uniquely extended to a derivation $K \to M$.

THEOREM 90. Let K be a separable extension field of a field k, and let B be a differential basis of K/k. Then k(B) is purely transcendental over k and K is formally etale over k(B).

Proof. Immediate from Th.87 and Th.89.

(38.F) Let $(A, \mathfrak{m}, K)$ be a local ring and k be a subfield of A such that K/k is formally etale. In this case we call k a quasi-coefficient field of A.

THEOREM 91. Every local ring containing a field contains quasi-coefficient fields. If k is a quasi-coefficient field of a local ring A, then the completion A* of A contains a unique coefficient field K containing k.

Proof. If $(A, \mathfrak{m}, K)$ is a local ring and k_0 is a perfect field (e.g. the prime field) contained in A, then let B be a differential basis of K over k_0 and choose a representative x_i in A for each $b_i \in B$. Since B is algebraically independent over k_0 by Th.89, A contains the quotient field k' of $k_0[\{x_i\}]$, and $k' \simeq k_0(B)$. Then K is formally etale over k'. By the definition of formal etaleness, the identity map $K \to A/\mathfrak{m}$ can be uniquely lifted to a homomorphism $K \to \varprojlim A/\mathfrak{m}^\nu = A^*$ over k', which proves the second half of the theorem.

One can define "quasi-coefficient rings" in the unequal characteristic case as follows: a subring I of a local ring $(A, \mathfrak{m}, K)$ with $ch(K) = p$ is a quasi-coefficient ring of A if (1) I is a noetherian local ring with $rad(I) = pI$, and (2) K is formally etale over I/pI. One can prove that any local ring of unequal characteristic has quasi-coefficient rings. Cf. H.Matsumura, Nagoya Math. J. 68 (1977).

(38.G) Not much is known about p-bases for rings. If k is a field of characteristic p and A is a reduced local ring containing k, and if A has a p-basis over A^p, then A must be regular by a theorem of Kunz which will be discussed later. If A is a regular local ring essentially of finite type over k, then A has a p-basis over A^p (cf. Kimura-Niitsuma, to appear in J. Japan Math. Soc.). The following interesting conjecture of Kunz (1975) is still open in the general case.

> Let R be a regular local ring of characteristic p and S be a regular subring of R over which R is finite. Does R have a p-basis over S ?

The answer is yes if p = 2 or 3 (proof is easy). If dim R = 2 there is a geometric proof by Rudakov-Shafarevich (Izvestija Akad. Nauk SSSR, t.40, No.6, 1976).

The following proposition is a converse of (38.A) in the case of noetherian local rings.

PROPOSITION. Let (R,m_R) be a noetherian local ring of characteristic p, and S be a subring of R containing R^p such that R is finite over S. Put $m_S = m_R \cap S$, $K = R/m_R$ and $K' = S/m_S$. If $\Omega_{R/S}$ is a free R-module with $dx_1,\ldots,dx_r$ ($x_i \in R$) as a basis, then $x_1,\ldots,x_r$ form a p-basis of R over S.

Proof. First we consider the case $\Omega_{R/S} = 0$. Suppose $K \neq K'$. Then, since $K' \supsetneq K^p$, there would exist $0 \neq \overline{D} \in \mathrm{Der}_{K'}(K)$, and composing it with the natural homomorphism $R \to K$ we would have a derivation $0 \neq D \in \mathrm{Der}_S(R,K)$. Therefore $K = K'$, i.e., $R = S + m_R$. Then $R/(m_SR + m_R^2) = K + m_R/(m_SR + m_R^2)$, and the right-hand side is a direct sum. Let p_2 de-ote the projection onto the second summand. Then the composition $R \to R/(m_SR + m_R^2) \overset{p_2}{\to} m_R/(m_SR + m_R^2)$ is a derivation of R over S, which must be zero. Therefore $m_R = m_SR + m_R^2$, and by NAK we have $m_R = m_SR$. Therefore $R = S + m_SR$, hence $R = S$ by NAK.

In the general case put $T = S[x_1,\ldots,x_r]$. If $x_1,\ldots,x_r$ are not p-independent over S, take a reduced polynomial $f(X_1,\ldots,X_r) \in S[X]$ of lowest degree such that $f(x_1,\ldots,x_r) = 0$. Then $\Sigma(\partial f/\partial x_i)dx_i = 0$ in $\Omega_{R/S}$, contradiction. Thus $x_1,\ldots,x_r$ is a p-basis of T over S and $\Omega_{T/S}$ is a free T-module with dx_i as basis, so that $\Omega_{T/S}\otimes_T R \simeq \Omega_{R/S}$. Then $\Omega_{R/T} = 0$, and so $R = T$ by what we have already seen.

Remark. In connection with the above proof, it is worthwhile to note the following more general result of Berger and Kunz. Let $(R, \mathfrak{m}, K)$ be a local ring, S a subring of R, $\mathfrak{n} = \mathfrak{m} \cap S$, $k = S/\mathfrak{n}$. If K/k is separable then the following sequence is exact: $0 \to \mathfrak{m}/(\mathfrak{n}R + \mathfrak{m}^2) \to \Omega_{R/S}\otimes K \to \Omega_{K/k} \to 0$. If ch(R) = p then put $\mathfrak{n}' = \mathfrak{m} \cap R^p[S]$. Then the following sequence is exact: $0 \to \mathfrak{m}/(\mathfrak{n}'R + \mathfrak{m}^2) \to \Omega_{R/S}\otimes K \to \Omega_{K/k} \to 0$. For the proof, cf. Berger-Kunz, Math. Z. 77 (1961).

39. Cartier's Equality and Geometric Regularity

(39.A) Let $k \subseteq K \subseteq L$ be fields. The kernel of the natural map $\Omega_{K/k} \otimes L \to \Omega_{L/k}$ is denoted by $\Gamma_{L/K/k}$ and is called the <u>module of imperfection</u> for $L/K/k$. Thus we have the following exact sequence:

$$0 \to \Gamma_{L/K/k} \to \Omega_{K/k} \otimes L \to \Omega_{L/k} \to \Omega_{L/K} \to 0.$$

LEMMA. If $k \subseteq K \subseteq L' \subseteq L$ are fields, we have the following exact sequence.

$$0 \to \Gamma_{L'/K/k} \otimes_{L'} L \to \Gamma_{L/K/k} \to \Gamma_{L/L'/k} \to \Omega_{L'/K} \otimes_{L'} L$$
$$\to \Omega_{L/K} \to \Omega_{L/L'} \to 0.$$

<u>Proof</u>. Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccccc}
0 & \to & \Gamma_{L'/K/k} \otimes L & \to & \Omega_{K/k} \otimes L & \to & \Omega_{L'/k} \otimes L & \to & \Omega_{L'/K} \otimes L & \to & 0 \\
 & & \downarrow & & \| & & \downarrow & & \downarrow & & \\
0 & \to & \Gamma_{L/K/k} & \to & \Omega_{K/k} \otimes L & \to & \Omega_{L/k} & \to & \Omega_{L/K} & \to & 0
\end{array}$$

For simplicity we write
$$\begin{array}{ccccccccccc}
0 & \to & X & \to & Z & \to & A & \to & B & \to & 0 \\
 & & \downarrow & & \| & & \downarrow f & & \downarrow g & & \\
0 & \to & Y & \to & Z & \to & A' & \to & B' & \to & 0
\end{array}$$

Applying the 'snake lemma' (cf. e.g. Bourbaki, Alg. Comm., Ch.1) to the induced diagram

$$\begin{array}{ccccccccc}
0 & \to & Z/X & \to & A & \to & B & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & Z/Y & \to & A' & \to & B' & \to & 0
\end{array}$$

we get the exact sequence $0 \to Y/X \to \operatorname{Ker} f \to \operatorname{Ker} g \to 0$, which shows the exactness of $0 \to X \to Y \to \operatorname{Ker} f \to B \to B' \to \operatorname{Coker} g \to 0$. This is what we wanted.

(39.B) THEOREM 92 (Cartier's equality). Let L be a finitely generated extension of a field K. Then

$$\operatorname{rank}_L \Omega_{L/K} = \operatorname{tr.deg.}_K L + \operatorname{rank}_L \Gamma_{L/K}.$$

<u>Proof</u>. If $L \supseteq L' \supseteq K$ and if the theorem holds for L/L' and for L'/K, then the validity of the theorem for L/K is an immediate consequence of the lemma. On the other hand any finitely generated extension is composed of simple extensions of the following types: (1) $L = K(\alpha)$ with α transcendental over K, (2) $L = K(\alpha)$ with α separably algebraic over K, (3) $L = K(\alpha)$, $ch(K) = p$, $\alpha^p = a \in K$, $\alpha \notin K$. Therefore it suffices to prove the theorem in each of these cases. Cases (1) and (2) are easy; cf. p.190. In case (3) we have $L = K[X]/(X^p - a)$, and then $\Omega_L = (\Omega_{K[X]} \otimes L)/Ld\alpha = (\Omega_K/Kda) \otimes L + Ld\alpha$, $d\alpha \neq 0$. Since $da \neq 0$ in Ω_K, we have $\operatorname{rank} \Gamma_{L/K} = \operatorname{rank} \Omega_{L/K} = 1$ and the theorem holds in this case also.

(39.C) THEOREM 93. Let $(A, \mathfrak{m}, K)$ be a noetherian local ring containing a field k. Then A is formally smooth over k in the $\mathfrak{m}$-adic topology iff A is geometrically regular over k.

Proof. The 'only if' part is known (28.N). In order to prove the 'if' part we may assume, by (28.N), that ch(k) = p. According to Cor. of Th.66 it suffices to show that $\Omega_k \otimes K \to \Omega_A \otimes K$ is injective. Therefore let $x_1, \ldots, x_r$ be p-independent elements in k. We will show that $dx_1, \ldots, dx_r$ are linearly independent in $\Omega_A \otimes K$ over K. Put $\alpha_i = x_i^{1/p}$, $k' = k(\alpha_1, \ldots, \alpha_r)$. Then $B = A \otimes_k k' = A[T_1, \ldots, T_r] / (T_1^p - x_1, \ldots, T_r^p - x_r)$ is a noetherian local ring. Let $\mathfrak{m}$ and L denote its maximal ideal and its residue field respectively. Since L is smooth over the prime field the sequence $0 \to \mathfrak{m}/\mathfrak{m}^2 \to \Omega_B \otimes L \to \Omega_L \to 0$ is exact by Th.58. Similarly the sequence $0 \to \mathfrak{m}/\mathfrak{m}^2 \to \Omega_A \otimes K \to \Omega_L \to 0$ is exact. Consider the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & \mathfrak{m}/\mathfrak{m}^2 & \to & \Omega_B \otimes L & \to & \Omega_L & \to & 0 \\ & & \uparrow \psi_1 & & \uparrow \psi_2 & & \uparrow \psi_3 & & \\ 0 & \to & (\mathfrak{m}/\mathfrak{m}^2) \otimes_K L & \to & \Omega_A \otimes L & \to & \Omega_K \otimes L & \to & 0 \end{array}$$

By the snake lemma we get an exact sequence of L-modules $0 \to \mathrm{Ker}\,\psi_1 \to \mathrm{Ker}\,\psi_2 \to \mathrm{Ker}\,\psi_3 \to \mathrm{Coker}\,\psi_1 \to \mathrm{Coker}\,\psi_2 \to \mathrm{Coker}\,\psi_3 \to 0$. Since A and B are regular by hypothesis and have the same dimension, we have $\mathrm{rank}\, \mathfrak{m}/\mathfrak{m}^2 = \dim A = \mathrm{rank}\, \mathfrak{m}/\mathfrak{m}^2$, so that $\mathrm{rank\,Ker}\,\psi_1 = \mathrm{rank\,Coker}\,\psi_1 < \infty$. Since L is finite algebraic over K we also have $\mathrm{rank\,Ker}\,\psi_3 = \mathrm{rank\,Coker}\,\psi_3 < \infty$ by Cartier's equality. It follows from these and from the above exact sequence that $\mathrm{rank\,Ker}\,\psi_2 = \mathrm{rank\,Coker}\,\psi_2 < \infty$.

On the other hand, we have $\mathrm{Coker}\,\psi_2 = \Omega_{B/A} \otimes L$ and $\Omega_{B/A} = BdT_1 + \ldots + BdT_r \simeq B^r$ by Th.58, hence $\mathrm{rank\,Ker}\,\psi_2 = r$. Putting $J = (T_1^p - x_1, \ldots, T_r^p - x_r)$ we have the exact sequence $J/J^2 \to \Omega_{A[T_1,\ldots,T_r]} \otimes B = \Omega_A \otimes B + \Sigma\, BdT_i \to \Omega_B \to 0.$ It remains exact after tensoring with L over B, so $\mathrm{Ker}\,\psi_2$ is generated by $dx_1, \ldots, dx_r$. Therefore $dx_1, \ldots, dx_r$ are linearly independent in $\Omega_A \otimes L$ over L, and a fortiori so in $\Omega_A \otimes K$ over K. QED.

(This proof is due to G.Faltings, Arch. Math.30 (1978.)

40. Jacobian Criteria and Excellent Rings

(40.A) Let A be a ring and let $x_1, \ldots, x_r \in A$, $D_1, \ldots, D_s \in \mathrm{Der}(A)$. We shall denote the Jacobian matrix $(D_i x_j)$ by $J(x_1, \ldots, x_r; D_1, \ldots, D_s)$. If P is an ideal of A, we shall write $J(x_1, \ldots, x_r; D_1, \ldots, D_s)(P)$ for $(D_i x_j \bmod P)$. When P is a prime ideal containing the x's, the rank of the above matrix depends on the ideal $I = \Sigma A x_i$ rather than the elements x_i themselves, so we denote it by $\mathrm{rank}\, J(I; D_1, \ldots, D_s)(P)$. If Δ is a set of derivations of A we define $\mathrm{rank}\, J(I; \Delta)(P)$ to be the supremum of $\mathrm{rank}\, J(I; D_1, \ldots, D_s)(P)$ when $\{D_1, \ldots, D_s\}$ runs over the set of all finite subset of Δ.

When A is an integral domain with quotient field K and M is an A-module, by rank M we understand $\mathrm{rank}_K\, M \otimes_A K$.

THEOREM 94. Let $(R,\mathfrak{m})$ be a regular local ring, P be a prime ideal of height r and Δ be a subset of Der(R). Then:

i) $\operatorname{rank} J(P;\Delta)(\mathfrak{m}) \leq \operatorname{rank} J(P;\Delta)(P) \leq r$,

ii) if $\operatorname{rank} J(f_1,\ldots,f_r; D_1,\ldots,D_r)(\mathfrak{m}) = r$ and $f_1,\ldots, f_r \in P$, then $P = (f_1,\ldots,f_r)$ and R/P is regular.

Proof. i) The first inequality is trivial, and the second is a consequence of the fact that PR_P is generated by r elements. ii) The condition implies that the images of f_i's are linearly independent over $R/\mathfrak{m}$ in $\mathfrak{m}/\mathfrak{m}^2$, hence the f_i's generate a prime ideal of height r. Our assertion follows.

THEOREM 95. Let R, P and Δ be as in the preceding theorem. Then the following two conditions are equivalent:

(1) $\operatorname{rank} J(P;\Delta)(P) = \operatorname{ht} P$,

(2) let Q be a prime ideal contained in P, then R_P/QR_P is regular iff $\operatorname{rank} J(Q;\Delta)(P) = \operatorname{ht} Q$.

Proof. (1) is the special case Q = P of (2). Conversely, suppose (1) holds. If $\operatorname{rank} J(Q;\Delta)(P) = \operatorname{ht} Q$ then R_P/QR_P is regular by the preceding theorem. If R_P/QR_P is regular then there exists $f_1,\ldots,f_r \in P$ such that $(f_1,\ldots,f_r)R_P = PR_P$, $(f_1,\ldots,f_s)R_P = QR_P$, $r = \operatorname{ht} P$, $s = \operatorname{ht} Q$. Then $\operatorname{rank} J(f_1,\ldots, f_r;\Delta)(P) = r$, and so $\operatorname{rank} J(f_1,\ldots,f_s;\Delta)(P) = s$.

(40.B) We shall say that a subfield k' of a field k is cofinite if $[k:k'] < \infty$.

LEMMA 1. Let $k \subseteq K$ be fields of characteristic p and let $\mathcal{F} = \{k_\alpha\}_{\alpha\in I}$ be a downwards-directed family of cofinite subfields of K containing k. Then the following are equivalent:

(1) $\bigcap_\alpha k_\alpha K^p = kK^p$.

(2) The natural map $\Omega_{K/k} \to \varprojlim \Omega_{K/k_\alpha}$ is injective.

(3) For every finite subset $\{u_1,\ldots,u_n\}$ of K which is p-independent over k, there exists $k_\alpha \in \mathcal{F}$ over which this set is p-independent.

(4) There exists a p-basis B of K over k such that for each finite subset F of B there exists $k_\alpha \in \mathcal{F}$ over which F is p-independent.

Proof. (2) $\Leftrightarrow$ (3) is easy, and (3) $\Rightarrow$ (4) is trivial. (1) $\Rightarrow$ (3): The proof of (30.C) Lemma 1 applies mutatis mutandis. (4) $\Rightarrow$ (2): Let $0 \neq \omega \in \Omega_{K/k}$. Then $\omega = c_1 db_1 + \ldots + c_n db_n$, $b_i \in B$, $0 \neq c_i \in K$, and if $b_1,\ldots,b_n$ are p-independent over k_α then the image of ω in Ω_{K/k_α} is not 0. (3) $\Rightarrow$ (1): Suppose $a \notin kK^p$. Then a is p-independent over k, therefore it is so over some k_α, i.e. $a \notin k_\alpha K^p$.

LEMMA 2. Let k, K and $\mathcal{F}$ be as in lemma 1 and let L be a finitely generated extension over K. If $\bigcap_\alpha k_\alpha K^p = kK^p$ holds, then $\bigcap_\alpha k_\alpha L^p = kL^p$ holds also.

<u>Proof</u>. It suffices to check the 4 cases of (27.A). i) If $L = K(t)$ with t transcendental, then $\bigcap k_\alpha L^p = \bigcap k_\alpha K^p(t^p) = kK^p(t^p) = kL^p$ is obvious. ii) If L is separably algebraic over K then a p-basis of K over k is also a p-basis of L over k, and we can use the criterion (4) of Lemma 1. iii) $L = K(t)$, $t^p = a \in K$, $d_{K/k}a = 0$. Then $\Omega_{L/k} = \Omega_{K/k} \otimes L + Ldt$, and $\Omega_{L/k_\alpha} = \Omega_{K/k_\alpha} \otimes L + Ldt$. Therefore $\Omega_{L/k} \to \varprojlim \Omega_{L/k_\alpha}$ is injective. iv) $L = K(t)$, $t^p = a \in K$, $d_{K/k}a \neq 0$. Then $\Omega_{L/k} = (\Omega_{K/k} \otimes L)/Ld_{K/k}a + Ldt$; if $B' \subset K$ is such that $\{a\} \cup B'$ is a p-basis of K/k and $a \notin B'$, then $\{t\} \cup B'$ is a p-basis of L/k. So if $b_1, \ldots, b_m \in B'$ and $\{a, b_1, \ldots, b_m\}$ is p-indep. in K over k_α, then $\{t, b_1, \ldots, b_m\}$ is p-indep. in L over k_α.

(40.C) Let k be a field of characteristic p, $R = k[[X_1, \ldots, X_n]]$, $P \in \mathrm{Spec}(R)$ and $A = R/P$. Let $y_1, \ldots, y_r$ ($r = \dim A$) be a system of parameters of A and put $B = k[[y_1, \ldots, y_r]]$. Then A is finite over B. Let k' be a cofinite subfield of k and put $C' = k'[[y_1^p, \ldots, y_r^p]]$. Since every derivation $D \in \mathrm{Der}(A)$ is continuous (in any ideal-adic topology), we have $\mathrm{Der}_{k'}(A) = \mathrm{Der}_{C'}(A)$, and A is finite over C'. Let L, K, K' denote the quotient fields of A, B, C'. Then it is easy to see that $\mathrm{rank}\ \mathrm{Der}_{k'}(A) = (L:K')_p = \mathrm{rank}\ \Omega_{L/K'}$, and similarly

$\mathrm{rank}\ \mathrm{Der}_{k'}(B) = (K:K')_p = \mathrm{rank}\ \Omega_{K/K'}$. If E is a p-basis of k over k' then $E \cup \{y_1, \ldots, y_r\}$ is a p-basis of B over C'. Therefore $\mathrm{rank}\ \Omega_{K/K'} = \dim A + (k:k')_p$, and in general we have by Th.59

$$\mathrm{rank}\ \mathrm{Der}_{k'}(A) = \mathrm{rank}\ \Omega_{L/K'} \geqslant \mathrm{rank}\ \Omega_{K/K'} = \dim A + (k:k')_p.$$

THEOREM 96. Let k, R and A be as above, and let $F = \{k_\alpha\}_{\alpha\in I}$ be a family of cofinite subfields of k, directed downwards, such that $\bigcap k_\alpha = k^p$. Then there exists $k_\alpha \in F$ such that, for every cofinite subfield k' of k_α, we have

$$\mathrm{rank}\ \mathrm{Der}_{k'}(A) = \dim A + (k:k')_p.$$

<u>Proof</u>. If $L = K$ then the theorem is obvious, so we will prove the existence of α such that $(L:K')_p = (K:K')_p$ for $k' \subseteq k_\alpha$ by induction on $(L:K)$. Suppose that our claim is proved for every proper subfield L' of L containing K, and let L' be maximal among such subfields. If L is separable over L' then $\Omega_{L/K'} = \Omega_{L'/K'} \otimes L$ and we are done. So we can suppose $L = L'(t)$, $t^p = a \in L'$. Then $a \notin L'^p$. Put $K_\alpha = k_\alpha((y_1^p, \ldots, y_r^p))$. Then $\bigcap K_\alpha = k^p((y_1^p, \ldots, y_r^p)) = K^p$ by p.229, hence $\bigcap K_\alpha L'^p = L'^p$ by Lemma 2. Therefore there exists α such that $a \notin K_\alpha L'^p$ and such that $(L':K')_p = (K:K')_p$ for $k' \subseteq k_\alpha$. Then for $k' \subseteq k_\alpha$ we have $a \notin K'L'^p$, i.e. $d_{L'/K'}a \neq 0$, hence $\Omega_{L/K'} = (\Omega_{L'/K'} \otimes L)/Ld_{L'/K'}a + Ldt$, and so $\mathrm{rank}\ \Omega_{L/K'} = \mathrm{rank}\ \Omega_{L'/K'} = \mathrm{rank}\ \Omega_{K/K'}$.

THEOREM 97 (Nagata). Let k be a field, $R = k[[X_1,\dots,X_n]]$ and $P \in \mathrm{Spec}(R)$. Then $\mathrm{rank}\ J(P;\ \mathrm{Der}(R))(P) = \mathrm{ht}\ P$.

<u>Proof</u>. Here we consider only the case $\mathrm{ch}(k) = p$. The case $\mathrm{ch}(k) = 0$ is easier, and we will prove a much more general result soon.

Put $A = R/P$ and $r = \dim A$. By the preceding theorem there exists a cofinite subfield k' of k such that

$$\mathrm{rank}\ \mathrm{Der}_{k'}(A) = r + (k:k')_p.$$

Put $s = (k:k')_p$. If $\{u_1,\dots,u_s\}$ is a p-basis of k/k' then $\{u_1,\dots,u_s,X_1,\dots,X_n\}$ is a p-basis of R over $k'[[X_1^p,\dots,X_n^p]]$. Let $\phi : R \to A$ denote the natural map and put $X_i = u_{s+i}$, $D_i = \phi\cdot\partial/\partial u_i$ $(1 \le i \le n+s)$. Then $\mathrm{Der}_{k'}(R,A)$ is a free A-module of rank $n + s$ with $D_1,\dots,D_{n+s}$ as a basis. Let now $\bar{D}$ be an arbitrary element of $\mathrm{Der}_{k'}(A)$, and put $\bar{D}(\phi u_i) = \bar{c}_i \in A$. Then $\bar{D}$ is induced by $D = \Sigma\bar{c}_i D_i \in \mathrm{Der}_{k'}(R,A)$ in the sense that $\bar{D}\cdot\phi = D$. The derivation $\bar{D}$ is determined by $\bar{c}_i$ $(1 \le i \le n+s)$, and these must satisfy

$$\sum_{i=1}^{n+s} \bar{c}_i D_i(f) = 0 \qquad \text{for all } f \in P.$$

Conversely, if $\bar{c}_i$ satisfy these linear equations then $D = \Sigma\bar{c}_i D_i$ induces a derivation of A over k'. Therefore $r + s = \mathrm{rank}\ \mathrm{Der}_{k'}(A) = n + s - \mathrm{rank}\ J(P;\ \mathrm{Der}_{k'}(R))(P)$, whence we get $\mathrm{rank}\ J(P;\ \mathrm{Der}_{k'}(R))(P) = n - r = \mathrm{ht}\ P$. Since $\mathrm{rank}\ J(P;\mathrm{Der}(R))(P) \le \mathrm{ht}\ P$ by Th.94, we are done.

(40.D) Let $(A,\mathfrak{m})$ be a noetherian complete local ring containing a field. Let k be a coefficient field of A and let $\mathfrak{m} = (x_1,\dots,x_n)$. Putting $R = k[[X_1,\dots,X_n]]$ we then have $A = R/I$ with some ideal I of R. Let $\mathfrak{p} = P/I \in \mathrm{Spec}(A)$. If $A_{\mathfrak{p}} = R_P/IR_P$ is regular, then $IR_P = QR_P$ for some $Q \in \mathrm{Spec}(R)$, $Q \subseteq P$, and we have $\mathrm{rank}\ J(I;\ \mathrm{Der}(R))(P) = \mathrm{ht}\ Q = \mathrm{ht}\ IR_P$ by Th.95 and Th.97. Put $r = \mathrm{ht}\ IR_P$ and let $f_1,\dots,f_r \in I$ and $D_1,\dots,D_r \in \mathrm{Der}(R)$ be such that $\det(D_i f_j) \notin P$. Then $IR_P = QR_P = \Sigma f_i R_P$, hence there exists $g \in R - P$ such that $IR_g = \Sigma_1^r f_i R_g$. Put $h = \det(D_i f_j)$. If $P'/I = \mathfrak{p}' \in \mathrm{Spec}(A)$ is such that $hg \notin P'$, then $R_{P'}/IR_{P'} = A_{\mathfrak{p}'}$ is regular by Th.94 (note that $IR_{P'}$ is generated by r elements). Thus Reg(A) contains the open neighborhood $\{\mathfrak{p}' \mid \overline{hg} \notin \mathfrak{p}'\}$ of $\mathfrak{p}$. Therefore Reg(A) is open in Spec(A), and we have proved the Cor. on p.222.

(40.E) THEOREM 98. Let $(A,\mathfrak{m})$ be a noetherian local <u>domain</u> containing $\mathbb{Q}$. Let k be a quasi-coefficient field of A, i.e. a subfield of A such that $A/\mathfrak{m}$ is algebraic over k. Then:

$$\mathrm{rank}\ \mathrm{Der}_k(A) \le \dim A.$$

<u>Proof</u>. We will prove that $\mathrm{Der}_k(A)$ is isomorphic to a submodule of A^n, where $n = \dim A$. Take a system of parameters $x_1,\dots,x_n$ of A. We claim that the map $\phi\colon \mathrm{Der}_k(A) \to A^n$ defined by $\phi(D) = (Dx_1,\dots,Dx_n)$ is injective. Suppose that $D \in \mathrm{Der}_k(A)$ and $Dx_1 = \dots = Dx_n = 0$. By continuity D is uniquely extended

to the completion A^*. Now A^* is finite over the subring $k[[x_1,\dots,x_n]]$, on which D vanishes. Let $a \in A$. As an element of A^* it satisfies a polynomial relation $f(a) = 0$ with coefficients in $k[[x_1,\dots,x_n]]$. Choose such a polynomial $f(T)$ of lowest degree. Then $0 = D(f(a)) = f'(a)Da$ and $f'(a) \neq 0$. Since $Da \in A$ and since the non-zero elements of A are not zero divisors in A^*, we must have $Da = 0$. Thus $D = 0$.

THEOREM 99. Let $(R, \mathfrak{m})$ be a regular local ring of dimension n containing a field. Let R^* be the completion of R and k be a coefficient field of R^* containing a quasi-coefficient field k_0 of R. Let $x_1,\dots,x_n$ be a regular system of parameters of R. Then $R^* = k[[x_1,\dots,x_n]]$, a formal power series ring over k, and $\mathrm{Der}_k(R^*)$ is a free R^*-module with the partial derivations $\partial/\partial x_1,\dots,\partial/\partial x_n$ as a basis. Then the following conditions are all equivalent:

(1) $\partial/\partial x_i$ $(1 \leq i \leq n)$ map R into R, i.e. $\partial/\partial x_i \in \mathrm{Der}_{k_0}(R)$;

(2) there exist $D_1,\dots,D_n \in \mathrm{Der}_{k_0}(R)$ and $a_1,\dots,a_n \in R$ such that $D_i a_j = \delta_{ij}$;

(3) there exist $D_1,\dots,D_n \in \mathrm{Der}_{k_0}(R)$ and $a_1,\dots,a_n \in R$ such that $\det(D_i a_j) \notin \mathfrak{m}$;

(4) $\mathrm{Der}_{k_0}(R)$ is a free R-module of rank n;

(5) $\mathrm{rank}\ \mathrm{Der}_{k_0}(R) = n$.

(<u>Remark</u>. Since $\mathrm{Der}_{k_0}(k) = 0$ we have $\mathrm{Der}_{k_0}(R) = \mathrm{Der}_k(R^*) \cap \mathrm{Der}(R)$. If we define $\mathrm{Der}_k(R)$ by $\mathrm{Der}_k(R^*) \cap \mathrm{Der}(R)$ then Th.98 and Th.99 hold for any coefficient field k of R^* and the mention to quasi-coefficient field is superfluous.)

<u>Proof</u>. Let K and L denote the quotient fields of R and R^*. The implications (1) ⇒ (2) ⇒ (3) and (4) ⇒ (5) are trivial.

(3) ⇒ (4): Clearly $D_1,\dots,D_n$ are linearly independent over R as well as over R^*. So every $D \in \mathrm{Der}_{k_0}(R)$ can be written as $D = \Sigma c_i D_i$ with $c_i \in L$. Solving the equations $Da_j = \Sigma c_i D_i a_j$, we get $c_i \in R$.

(5) ⇒ (1): Let $D_1,\dots,D_n$ be linearly independent over R. This means that there exists $a_1,\dots,a_n \in R$ with $\det(D_i a_j) \neq 0$. Therefore $D_1,\dots,D_n$ are linearly independent over R^* also. Hence $\partial/\partial x_i = \Sigma_j c_{ij} D_j$ with c_{ij} in L. Then $\delta_{ik} = \Sigma_j c_{ij} D_j x_k$, therefore the matrix (c_{ij}) is the inverse of $(D_j x_k)$ and so $c_{ij} \in K$. Then $(\partial/\partial x_i)(R) \subseteq K \cap R^* = R$.

(40.F) We will say that (WJ) (= weak Jacobian condition) holds in a regular ring R if $\mathrm{rank}\ J(P;\mathrm{Der}(R))(P) = \mathrm{ht}\ P$ for every $P \in \mathrm{Spec}(R)$. The reasoning of (40.D) and Th.95 show that, if A is a homomorphic image of a regular ring R in which (WJ) holds, then Reg(A) is open in Spec(A). For the definition and the theory of the strong Jacobian condition (SJ), we refer to our article 'Noetherian rings with many deriva-

tions', in Contributions to Algebra (dedicated to E. Kolchin), ed. by H. Bass et al., Academic Press, 1977.

THEOREM 100. Let $(R,\mathfrak{m},K)$ be a regular local ring of dimension n containing a field k of characteristic 0. Assume that (1) K is algebraic over k, and (2) rank $\mathrm{Der}_k(R) = n$. Then:

i) (WJ) holds in R,

ii) if $P \in \mathrm{Spec}(R)$ then every element of $\mathrm{Der}_k(R/P)$ is induced by an element of $\mathrm{Der}_k(R)$,

iii) rank $\mathrm{Der}_k(R/P) = \dim R/P$.

Proof. The argument is essentially the same as in Th.97. We use the notation of Th.99. Then there exists $D_1,\dots,D_n \in \mathrm{Der}_k(R)$ and $x_1,\dots,x_n \in \mathfrak{m}$ such that $D_i x_j = \delta_{ij}$, and $\mathrm{Der}_k(R)$ is a free R-module with $D_1,\dots,D_n$ as a basis. Put $A = R/P$ and let $\phi: R \to A$ denote the natural map. Then $\mathrm{Der}_k(R,A)$ is a free A-module with $\phi\circ D_i$ $(1 \le i \le n)$ as a basis. If $\overline{D} \in \mathrm{Der}_k(A)$ let $c_i \in R$ be such that $\phi(c_i) = \overline{D}\phi(x_i)$. Then $D = \sum c_i D_i \in \mathrm{Der}_k(R)$ induces $\overline{D}$ in the sense that $\phi\circ D = \overline{D}\circ\phi$. Let $(u_1,\dots,u_n) \in A^n$. Then $\sum u_i \phi\circ D_i$ induces a derivation $D \in \mathrm{Der}_k(A)$ iff $\sum u_i \phi(D_i f) = 0$ for all $f \in P$. Thus

$$\text{rank } \mathrm{Der}_k(A) = n - \text{rank } J(P; \mathrm{Der}_k(R))(P).$$

The left-hand side is $\le \dim A = n - \mathrm{ht}\, P$ by Th.98, and the right-hand side is $\ge n - \mathrm{ht}\, P$ by Th.94. Therefore we have i) and iii).

THEOREM 101. Let R be a regular ring containing Q. If (WJ) holds in R, then R is excellent.

Proof. Since R is Cohen-Macaulay it is universally catenary. We have already remarked that (WJ) implies the openness of $\mathrm{Reg}(R/P)$ in $\mathrm{Spec}(R/P)$ for every $P \in \mathrm{Spec}(R)$, and as R contains Q this proves that R is J-2 by Th.73(3), p.246. To prove that R is a G-ring we can assume that R is a regular local ring, and we have to show that the formal fibres of R are regular. Let P be a prime ideal of the completion R^* and put $p = P \cap R$. Let $r = \mathrm{ht}\, p$. Then there exist $D_1,\dots,D_r \in \mathrm{Der}(R)$ such that rank $J(p; D_1,\dots,D_r)(p) = r$. We can extend the derivations D_i to R^* and view the matrix $J(p; D_1,\dots,D_r)(p)$ as $J(pR^*; D_1,\dots,D_r)(P)$. On the other hand, we have $\mathrm{ht}\, pR^* = \mathrm{ht}\, p = r$ by (13.B). Therefore R^*_P/pR^*_P is regular, Q.E.D.

THEOREM 102. Let k be a field of characteristic 0, and R be a regular ring containing k. Suppose that (1) for any maximal ideal $\mathfrak{m}$ of R, the residue field $R/\mathfrak{m}$ is algebraic over k and ht $\mathfrak{m} = n$, and (2) there exist $D_1,\dots,D_n \in \mathrm{Der}_k(R)$ and $x_1,\dots,x_n \in R$ such that $D_i x_j = \delta_{ij}$. Then R is excellent.

Proof. By Th.100 it is clear that (WJ) holds in R. Q.E.D.

Remark. Convergent power series rings over R or C, formal power series rings over a field k of characteristic 0, and more generally the rings of type $k[X_1,\dots,X_n][[Y_1,\dots,Y_m]]$ where k is a field of char. 0, are examples of regular rings to which the theorem applies. Formal power series rings over a convergent power series ring also belong to the class. On the other hand there are excellent regular rings containing a coefficient field k of char. 0, such that $\mathrm{Der}_k(R) = 0$.

Example: Let k be a field of char.0 and let f(X) be a formal power series such that f(X), f'(X) and X are algebraically independent over k (e.g. f = exp(exp(X)) will do). Let $f = \Sigma a_i X^i$, $a_i \in k$, and put $y_i = \Sigma_{j=i}^{\infty} a_j X^{j-i}$ $(i = 0,1,2,\dots)$. Then $y_0 = f(X)$ and $y_i = a_i + Xy_{i+1}$. Put $R = k[X,y_0,y_1,\dots]$. Then $R/XR = k$, so that XR is a prime ideal. Put $A = R_{XR}$. Since A is a subring of k[[X]] it is X-adically separated, so it is a regular local ring of dimension 1 and ch(A) = 0, hence A is excellent. Its completion A* is k[[X]] and d/dX maps f to f' which is not in $k(X, y_o)$, hence not in A. By Th.99 we see that $\mathrm{Der}_k(A) = 0$.

THEOREM 103. Let R be a regular ring. If (WJ) holds in $R[X_1,\dots,X_n]$ for every $n \geqslant 0$, then R is excellent.

Proof. The condition implies that Reg(B) is open in Spec(B) for every finitely generated R-algebra B, i.e. that R is J-2.

To prove that R is a G-ring we may assume that R is local, and we have to prove that the formal fibres are geometrically regular. By (33.E) Lemma 3, it suffices to prove that, if C is a localization of a finite R-algebra which is a domain, and if Q is a prime ideal of C* such that $Q \cap C = (0)$, then C^*_Q is regular. Now C is a homomorphic image of a localization of some $R[X_1,\dots,X_n]$, and our assertion is proved by the same argument as in the proof of Th.101.

Remark. It is easy to see that, if R contains $\mathbb{Q}$, then (WJ) in R implies (WJ) in R[X]. But this is not so in the case of characteristic p. In fact, the ring A of (34.B) is a counter-example.

41. Krull Rings and Marot's Theorem

(41.A) Let A be an integral domain and put $P = \{p \in \mathrm{Spec}\, A \mid \mathrm{ht}\, p = 1\}$. We call A a Krull ring if

(1) A_p is a principal valuation ring for all $p \in P$, and

(2) every non-zero principal ideal aA is the intersection of a finite number of primary ideals of height 1.

A normal noetherian domain is a Krull ring by Th.37 and Th.38. We will give a sufficient condition for the converse to hold. First we list a few elementary properties of Krull rings. Let A be a Krull ring with quotient field K.

I) Let $a,b \in A$, $a \neq 0$, $x = b/a$. By (2) we have

$aA = q_1 \cap \cdots \cap q_r$, $q_i = aA_{p_i} \cap A$, $p_i \in P$. Therefore $x \in A$ $\Leftrightarrow b \in q_i$ for all i $\Leftrightarrow b \in aA_p$ for all $p \in P$ $\Leftrightarrow x \in A_p$ for all $p \in P$. Hence $A = \bigcap_{p \in P} A_p$. Moreover, if $0 \neq x \in K$, then x is a unit in A_p for all but a finite number of $p \in P$.

II) By (1) each primary ideal q of height 1 is a symbolic power of its radical. Therefore every principal ideal $aA \neq 0$ is of the form $aA = p_1^{(n_1)} \cap \cdots \cap p_r^{(n_r)}$, $p_i \in P$.

III) If $p \in P$, let $v_p(\ )$ denote the normalized valuation associated to A_p (i.e. if $pA_p = t_p A_p$ then $v_p(x) = n$ means $xA_p = t_p^n A_p$). Then for each $0 \neq x \in K$ there exists at most a finite number of $p \in P$ with $v_p(x) \neq 0$. If $a \in A$ we can write

$$aA = \bigcap p^{(v_p(a))}.$$

IV) If $\dim A = 1$ then A is noetherian. Indeed, let I be an ideal. If $I \neq (0)$ pick $a \in I$, $a \neq 0$. It suffices to prove that I/aA is a finite module. Writing aA as in II), we can embed A/aA in $A/p_1^{(n_1)} \oplus \cdots \oplus A/p_r^{(n_r)}$. But if $p \in P$ then p is maximal and $A/p^{(n)}$ is a module of finite length. This proves our assertion. An integral domain in which every non-zero ideal is uniquely represented as the product of a finite number of prime ideals is called a <u>Dedekind domain</u>. It is well known that an integral domain is Dedekind iff it is normal, noetherian and of dimension $\leqslant 1$. Therefore Krull domains of dimension $\leqslant 1$ are nothing but Dedekind domains.

V) Suppose we are given $p_1, \ldots, p_r \in P$ and $e_1, \ldots, e_r \in Z$. Then there exists $x \in K$ satisfying

$$v_{p_i}(x) = e_i \quad (1 \leqslant i \leqslant r), \qquad v_p(x) \geqslant 0 \text{ for all other } p \in P.$$

<u>Proof</u>. Take $y_1 \in p_1 - (p_1^{(2)} \cup p_2 \cup \cdots \cup p_r)$. Then $v_i(y_1) = \delta_{i1}$ $(1 \leqslant i \leqslant r)$. Similarly, take $y_j \in A$ such that $v_i(y_j) = \delta_{ij}$ $(1 \leqslant i \leqslant r)$ and put $y = \Pi y_i^{e_i}$. Put $P' = P - \{p_1, \ldots, p_r\}$. There exists at most a finite number of $p \in P'$ such that $v_p(y) < 0$; denote them by $p'_1, \ldots, p'_s$. Take $t_j \in p'_j - (p_1 \cup \cdots \cup p_r)$ for $1 \leqslant j \leqslant s$, and put $x = y(t_1 \cdots t_s)^n$ with n sufficiently large. Then x satisfies our requirement.

(41.B) THEOREM 104 (Y.Mori - J.Nishimura). Let A be a Krull ring and P be as before. If A/p is noetherian for every $p \in P$, then A is noetherian.

<u>Proof</u>. We will prove that $A/p^{(n)}$ is noetherian (as a ring, or what is the same, as an A-module) for every $p \in P$ and for every $n > 0$. Since a finite sum of noetherian modules is again noetherian, and since any submodule of a noetherian module is noetherian by definition, it then follows that A is noetherian as in the proof of IV).

Using V) for $e_1 = -1$ we can find $x \in \Phi A$ such that $v_p(x) = 1$, $v_q(x) \leqslant 0$ for all $q \in P - \{p\}$. Put $B = A[x]$. If $y \in p$ then $y/x \in A$, hence $p \subseteq xB \cap A$. Conversely, since

$B \subseteq A_p$ and $xB \subseteq pA_p$ we have $p \supseteq xB \cap A$. Therefore $p = xB \cap A$, and $B = A + xB$, hence $B/xB \simeq A/p$. Since $x^nB/x^{n+1}B \simeq B/xB$ for all n, it is clear that B/x^nB is noetherian for all n. But $x^nB \cap A \subseteq x^nA_p \cap A = p^{(n)}$ and B/x^nB is generated by the images of $1, x, \ldots, x^{n-1}$ over $A/(x^nB \cap A)$. By Eakin's theorem $A/(x^nB \cap A)$ is a noetherian ring, of which $A/p^{(n)}$ is a homomorphic image. Therefore $A/p^{(n)}$ is noetherian, as wanted.

MORI-NAGATA INTEGRAL CLOSURE THEOREM. Let A be a noetherian domain with quotient field K, and L be a finite algebraic extension of K. Then the integral closure A' of A in L is a Krull ring. If $P' \in \operatorname{Spec} A'$ and $P = P' \cap A$, then $[\kappa(P'):\kappa(P)] < \infty$. If $P \in \operatorname{Spec} A$, there exists only a finite number of prime ideals of A' lying over P.

For the proof we refer to Nagata, Local Rings or to Fossum, The Divisor Class Group of a Krull Domain. (In fact they consider the case L = K, but the general case is easily reduced to this case by enlarging A a little.) They use the structure theorem of complete local rings. Recently, J. Nishimura (J. Math. Kyoto Univ. 16(1976)) and J. Querré (C.R. Acad. Sci. Paris 285(1977)) gave different proofs of the first assertion which do not use the structure theorem.

(41.C) THEOREM OF KRULL-AKIZUKI. If dim A = 1 in the preceding theorem, every ring between L and A is noetherian.

For the proof see Bourbaki, Algèbre Commutative, Ch.7 or Matijevic, Maximal ideal transforms of noetherian rings, Proc. AMS 54 (1976).

THEOREM 105. If dim A = 2 in the Mori-Nagata theorem, then A' is noetherian.

Proof. Let P' be a prime ideal of height 1 in A'. Then A'/P' is integral over A/P, where $P = P' \cap A$, $[\kappa(P'):\kappa(P)]$ is finite and dim A/P = 1. Therefore A'/P' is noetherian by the Krull-Akizuki theorem, hence A' is noetherian by Th.104.

(41.D) THEOREM 106 (J. Marot). Let A be a noetherian ring and I an ideal of A. Suppose that A is complete and separated in the I-adic topology and that A/I is a Nagata ring. Then A is a Nagata ring.

Proof. We have to prove that A/p is N-2 for all $p \in \operatorname{Spec}(A)$. Assume the contrary. Then there exists a maximal element p_0 in $\{p \mid A/p \text{ is not N-2}\}$. The hypotheses on A are inherited by all homomorphic images of A (note that $I \subseteq \operatorname{rad}(A)$). Replacing A by A/p_0, we may therefore assume that A is a noetherian domain, that A/p is N-2 if $(0) \neq p \in \operatorname{Spec}(A)$ and that A is not N-2 (hence $I \neq (0)$). Let K be the quotient field of A,

L be a finite algebraic extension of K and B be the integral closure of A in L. If $(0) \neq P \in \mathrm{Spec}(B)$ and $P \cap A = \mathfrak{p}$, then $\mathfrak{p} \neq (0)$ and $[\kappa(P):\kappa(\mathfrak{p})] < \infty$. Therefore B/P is finite over $A/\mathfrak{p}$ by the N-2 property of $A/\mathfrak{p}$, and so B/P is noetherian. Therefore B is noetherian by Th.104. Let R be the radical of IB and let $R = P_1 \cap \ldots \cap P_r$ be its prime decomposition. Put $\mathfrak{p}_i = P_i \cap A$. Then $\mathfrak{p}_i \supseteq I \neq (0)$, hence $A/\mathfrak{p}_i$ is N-2 and B/P_i is finite over $A/\mathfrak{p}_i$ for all i. Since B/R can be embedded in $B/P_1 \oplus \ldots \oplus B/P_r$ and since A is noetherian, B/R is a finite A-module. Since B is noetherian, R^n/R^{n+1} is a finite module over B/R, hence also over A, for all n. Using the exact sequence $0 \to R^n/R^{n+1} \to B/R^{n+1} \to B/R^n \to 0$ we see inductively that B/R^n is finite over A for all n. Since $R^n \subseteq IB$ for n sufficiently large, B/IB is also finite over A. Since B is noetherian and $IB \subseteq \mathrm{rad}(B)$, B is separated in the I-adic topology. Therefore B is finite over A by Lemma of p.212. This proves that A is N-2, contrary to our assumption.

42. Kunz' Theorems

(42.A) Let A be a ring, $x_1, \ldots, x_n \in A$ and $I = \Sigma x_i A$. The elements x_i are said to be <u>independent</u> if $\Sigma a_i x_i = 0$ implies all $a_i \in I$, or equivalently, if I/I^2 is a free A/I-module of rank n.

This definition is due to C.Lech, Inequalities related to certain couples of local rings, Acta Math. 112 (1964). If $x_1, \ldots, x_n$ form an A-regular sequence then they are independent. When A is a regular local ring the converse is also true. More precisely, we have the following theorem of Vasconcelos:

> Let R be a noetherian local ring and I be a proper ideal with finite projective dimension. If I/I^2 is free over R/I, then I is generated by an R-sequence.

For the proof, see W. Vasconcelos, Ideals generated by R-sequences, J. Algebra 6 (1967) or I.Kaplansky, Commutative Rings, Th.199.

The following two lemmas are due to Lech.

LEMMA 1. If $yz, x_2, \ldots, x_n$ are independent, then $y, x_2, \ldots, x_n$ are also independent.

<u>Proof</u>. Let $a_1 y + a_2 x_2 + \ldots + a_n x_n = 0$, $a_i \in A$. Then $a_1 yz + a_2 y x_2 + \ldots + a_n y x_n = 0$, therefore $a_1 \in (yz, x_2, \ldots, x_n)$. Write $a_1 = byz + c_2 x_2 + \ldots + c_n x_n$. Then $by^2 z + (c_2 y + a_2) x_2 + \ldots + (c_n y + a_n) x_n = 0$, hence $c_i y + a_i \in (yz, x_2, \ldots, x_n)$ and so $a_i \in (y, x_2, \ldots, x_n)$.

LEMMA 2. If $f_1,\dots,f_n$ are independent, if $\ell(A/(f_1,\dots,f_n))$ is finite and if $f_1 = gh$, then

$$\ell(A/(f_1,\dots,f_n)) = \ell(A/(g,f_2,\dots,f_n)) + \ell(A/(h,f_2,\dots,f_n)).$$

Proof. If $ag = b_1f_1 + \dots + b_nf_n$, then $a - b_1h \in (f_1,\dots,f_n)$ and so $a \in (h,f_2,\dots,f_n)$. Hence

$$(g,f_2,\dots,f_n)/(f_1,f_2,\dots,f_n) \simeq A/(h,f_2,\dots,f_n).$$

LEMMA 3. Let $(A,\mathfrak{m},k)$ be a local ring and $\nu_i > 0$ be integers. If $\mathfrak{m}= (x_1,\dots,x_n)$ and if $x_1^{\nu_1},\dots,x_n^{\nu_n}$ are independent, then

$$\ell(A/(x_1^{\nu_1}, \dots, x_n^{\nu_n})) = \nu_1\cdots\nu_n.$$

Proof. This is a corollary of the preceding lemmas.

(42.B) Let p be a prime number and $q = p^s$, $s > 0$. If A is a ring of characteristic p, then the map $F: A \to A$ defined by $F(x) = x^q$ is a homomorphism called the (q-th) Frobenius map. Its image F(A) is written A^q. (Do not confuse it with the free module of rank q, which will not appear in this section.) If A is reduced then $A \to A^q$, and F can be identified with the inclusion map $A^q \hookrightarrow A$.

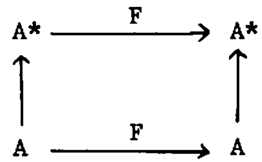
THEOREM 107 (E. Kunz). Let A be a noetherian local ring of characteristic p. Then the following are equivalent:

(1) A is regular,

(2) A is reduced, and A is flat over A^q for $q = p^s$ for every $s > 0$,

(3) A is reduced, and A is flat over A^q for $q = p^s$ for at least one $s > 0$.

Proof. (1) $\Rightarrow$ (2): Let A* be the completion of A. Then



is commutative, where F is $x \mapsto x^q$. The map $F: A \to A$ is flat if its completion $F: A^* \to A^*$ is flat. So we may assume that A is complete. Then A has a coefficient field k and we may assume that $A = k[[X_1,\dots,X_n]]$. In general if $k' \subset k$ is a field extension then the natural map $k'[Y_1,\dots,Y_n] \to k[Y_1,\dots,Y_n]$ is flat, and by localization and completion (Th.49 guarantees that flatness of a local homomorphism of noetherian local rings is preserved by completion) we see that $k'[[Y_1,\dots,Y_n]] \to k[[Y_1,\dots,Y_n]]$ is flat. Therefore $A^p = k^p[[X_1^p,\dots,X_n^p]] \to k[[X_1^p,\dots,X_n^p]]$ is flat, and A is free over $k[[X_1^p,\dots,X_n^p]]$. Hence A is flat over A^p.

(3) $\Rightarrow$ (1): Put $A^q = B$ and let $\mathfrak{m}, \mathfrak{n}$ denote the maximal ideals of A, B. Let $\{x_1,\dots,x_r\}$ be a minimal basis of $\mathfrak{m}$. Since $A \simeq B$ by F, $\{x_1^q,\dots,x_r^q\}$ is a minimal basis of $\mathfrak{n}$.

Put $\mathfrak{m}A = I$. Since A is flat over B we have

$$(\mathfrak{m}/\mathfrak{m}^2)\otimes_B A = (\mathfrak{m}\otimes_B A)/(\mathfrak{m}^2\otimes_B A) = \mathfrak{m}A/\mathfrak{m}^2A = I/I^2,$$

and $(\mathfrak{m}/\mathfrak{m}^2)\otimes_B A$ is a free module of rank r over A/I. Therefore $x_1^q,\dots,x_r^q$ are independent in A in the sense of Lech. By Lemma 3 we have

$$\ell_A(A/(x_1^q,\dots,x_r^q)) = \ell_{A^*}(A^*/(x_1^q,\dots,x_r^q)) = q^r.$$

The completion A* has a coefficient field k, and we can write $A^* = k[[x_1,\dots,x_r]] = k[[X_1,\dots,X_r]]/\mathfrak{a}$. Putting $R = k[[X_1,\dots,X_r]]$ we have $\ell_R(R/(X_1^q,\dots,X_r^q)) = q^r$, which means $\mathfrak{a} \subseteq (X_1^q,\dots,X_r^q)$. Since $F : A^q \to A$ is flat, and

$$\begin{array}{ccc} A^q & \xrightarrow{F} & A \\ {\scriptstyle F}\downarrow\wr & & {\scriptstyle F}\downarrow\wr \\ A^{q^2} & \xrightarrow{F} & A^q \end{array}$$

is commutative, $A^{q^2} \to A^q$ is also flat and $F^2 : A^{q^2} \to A$ is flat. Similarly, $F^\nu : A^{q^\nu} \to A$ is flat for all $\nu > 0$. Then $\mathfrak{a} \subseteq \bigcap_\nu (X_1^{q^\nu},\dots,X_r^{q^\nu}) = (0)$, hence A* is regular and so A is regular.

THEOREM 108 (E. Kunz). Let A be a noetherian ring of characteristic p. If A is finite over A^p then A is excellent.

Proof. First we note that the finiteness of A over A^p is preserved by localization, by taking homomorphic image and

by ring extension of finite type.

To prove that A is J-2, it therefore suffices to show that Reg(A) is open in Spec(A) under the additional assumption that A is an integral domain. Let $B = A^p$, $P \in \mathrm{Spec}(A)$. Then $P \in \mathrm{Reg}(A)$ iff $A_P = A\otimes_B B_{\mathfrak{p}}$ is flat over $(A_P)^p = B_{\mathfrak{p}}$, where $\mathfrak{p} = P\cap B$. Since A is finite over B, $P \in \mathrm{Reg}(A)$ is equivalent to $P\cap B \in \{\mathfrak{p} \in \mathrm{Spec}(B) \mid A_{\mathfrak{p}} = A\otimes_B B_{\mathfrak{p}}$ is free over $B_{\mathfrak{p}}\}$. Since the latter set is open in Spec(B) and since the map $P \to P\cap B$ is a homeomorphism from Spec(A) onto Spec(B), Reg(A) is open in Spec(A).

To prove that A is a G-ring we use the criterion of (33.E). We may assume that A is a local domain, and we have to show that if Q is a prime ideal of the completion A* such that $Q\cap A = (0)$, then $(A^*)_Q$ is regular. Let K be the quotient field of A, $B = A^p$ and $q = Q\cap B$. Then $A^* = A\otimes_B B^*$, and $(A^*)_Q$ is a local ring of $K\otimes_A A^* = K\otimes_B B^* = K\otimes_{K^p} B^*$. Since K^p is a field it is easy to see that $(A^*)_Q$ is free over its p-th power $(B^*)_q$. Hence $(A^*)_Q$ is regular.

Lastly we will show that A is universally catenary. Again it is enough to show that A is catenary under the additional assumption that A is a local domain. This will be done in a series of lemmas.

LEMMA 4. Let A be a noetherian local ring of characteristic p such that A is finite over A^p, and let A* denote its completion. Then A* is finite over $(A^*)^p$, and we have $(A^*)^p = (A^p)^*$. Moreover, $\Omega_{A^*} = \Omega_A \otimes_A A^*$.

Proof. Put $B = A^p$. Since A is finite over B, B is a subspace of A and B* is a subring of A*. The topology of A is equal to the topology as a B-module, hence $A^* = A \otimes_B B^*$ and so A* is finite over B*. The Frobenius map $F: A \to B$ is a surjective homomorphism, hence its completion $F^*: A^* \to B^*$ is also surjective. It coincides with the p-th power map on A, hence on the whole A* by continuity. Thus $(A^*)^p = B^*$. Since $\Omega_A = \Omega_{A/B}$, we have $\Omega_{A/B} \otimes_A A^* = \Omega_{A/B} \otimes_B B^* = \Omega_{A \otimes_B B^*/B^*} = \Omega_{A^*/B^*} = \Omega_{A^*}$.

LEMMA 5. Let A be as above and assume that A is an integral domain. Then A* is reduced.

Proof. Let $F: A \to A$ be the Frobenius map. Since A is reduced, F is injective. The completion map $F^*: A^* \to A^*$ is also injective, but F* is the Frobenius map of A*. Hence A* is reduced.

LEMMA 6. Let A be as in Lemma 5, and let K, k denote the quotient field and the residue field of A, respectively.

Then $\operatorname{rank} \Omega_K = \operatorname{rank} \Omega_k + \dim A$.

Proof. Let P be a minimal prime of A*, and put $L = (A^*)_P$. Then L is a field by the preceding lemma. We have

$$\Omega_L = \Omega_{A^*} \otimes_{A^*} L = \Omega_A \otimes_A L = (\Omega_A \otimes_A K) \otimes_K L ,$$

hence $\operatorname{rank} \Omega_L = \operatorname{rank} \Omega_K$. Therefore we may replace A by A*/P and assume that A is a complete local domain. Then A contains a coefficient field k. Let $x_1, \ldots, x_n$ ($n = \dim A$) be a system of parameters of A, and put $A' = k[[x_1, \ldots, x_n]]$. Then A is finite over A' and if K' is the quotient field of A' we have $\operatorname{rank} \Omega_K = \operatorname{rank} \Omega_{K'}$, by Cartier's equality (or directly: $[K:K'^p] = [K:K^p][K^p:K'^p] = [K:K'][K':K'^p]$, and $[K:K'] = [K^p:K'^p]$ by the Frobenius isomorphism, hence $[K:K^p] = [K':K'^p]$.) Therefore we may replace A by the formal power series ring $A' = k[[x_1, \ldots, x_n]]$. If $\{a_1, \ldots, a_s\}$ is a p-basis of k then $\{a_1, \ldots, a_s, x_1, \ldots, x_n\}$ is a p-basis of A'. Hence $\operatorname{rank} \Omega_K = s + n = \operatorname{rank} \Omega_k + \dim A$.

LEMMA 7. Let A be as in Lemma 4, and let P, Q ε Spec(A), $P \supseteq Q$. Put $\operatorname{rank} \Omega_{\kappa(P)} = \delta(P)$. Then $ht(P/Q) = \delta(P) - \delta(Q)$. Consequently, A is catenary.

Proof. Put $R = A_P/QA_P$. Then $\delta(Q)$ and $\delta(P)$ are the quotient field and the residue field of R, respectively, and $\dim R = ht(P/Q)$. Thus the desired equality is nothing but the preceding lemma (applied to R). If $P \supset P' \supset Q$, $P' \in \mathrm{Spec}(A)$, then the result just obtained shows $\mathrm{ht}(P/P') + \mathrm{ht}(P'/Q) = \mathrm{ht}(P/Q)$. Hence A is catenary.

43. Complement

Grothendieck (EGA 0_{IV} 19.7.1) proved the following important theorem:

(*) Let $(A, \mathfrak{m}, k)$ and $(B, \mathfrak{n}, k')$ be noetherian local rings and $\phi: A \to B$ be a local homomorphism. Then

$$\phi \text{ is formally smooth } \Leftrightarrow B \otimes k \text{ is formally smooth over } k, \text{ and } \phi \text{ is flat.}$$

The most difficult part is the proof of flatness from formal smoothness. His proof is quite interesting but too long to include in this book.

Let A be a ring, B an A-algebra and L a B-module. The set of isomorphism classes of extensions of B by L (§25) has a natural structure of A-module, which was denoted by $\mathrm{Exalcom}_A(B, L)$ in EGA. The algebra B is smooth over A iff this module is zero for all B-modules L. When A and B are topological rings Grothendieck defined a variant of the above module, called $\mathrm{Exalcomtop}_A(B,L)$; B is formally smooth over A iff this last module vanishes for all L.

The functor $\mathrm{Exalcom}_A(B,L)$ has certain formal properties, which make it a 1-dimensional cohomology functor in some

sense. So several poeple tried to construct the higher cohomologies that should follow it. After the partial success of Gerstenhaber, Harrison and others, Michel André succeeded in constructing a satisfactory theory (Méthode simpliciale ..., Springer LN 32 (1967); Homologie des algèbres commutatives, Springer, 1974). Let A, B and L be as above. He defines homology modules $H_n(A,B,L)$ and cohomology modules $H^n(A,B,L)$ for all $n \geqslant 0$. We have $H_0(A,B,L) = \Omega_{B/A} \otimes_B L$, $H^0(A,B,L) = \mathrm{Der}_A(B,L)$ and $H^1(A,B,L) = \mathrm{Exalcom}_A(B,L)$. When $A \to B \to C$ is a sequence of ring homomorphisms and M is a C-module, we have the following long exact sequences called Jacobi-Zariski sequences:

$$\cdots \to H_n(A,B,M) \to H_n(A,C,M) \to H_n(B,C,M) \to H_{n-1}(A,B,M) \to \cdots \to H_0(B,C,M) \to 0,$$

and

$$0 \to H^0(B,C,M) \to \cdots \to H^{n-1}(A,B,M) \to H^n(B,C,M) \to H^n(A,C,M) \to H^n(A,B,M) \to \cdots .$$

Let J be an ideal of B. The A-module B with J-adic topology is formally smooth iff $H^1(A,B,W) = 0$ for all B/J-module W. A noetherian local ring A is excellent iff $H^n(A,A^*,W) = 0$ for all $n > 0$ and for every A^*-module W.

André's homology and cohomology are connected with formal smoothness at $n = 1$, with regularity at $n = 2$ and with complete intersection at $n = 3$ (and up). The theorem (*) cited above is proved rather naturally in André's theory.

A noetherian local ring A is called a complete intersection (CI for short) if its completion A* is of the form R/I, where R is a regular local ring and I is an ideal generated by an R-sequence. This is characterized by $H_3(A,K,K) = 0$, where K is the residue field. Using this criterion it is easy to see that if A is CI and $P \in \mathrm{Spec}(A)$, then A_P is CI also. L.L.Avramov (Dokl. Akad. Nauk SSSR 225(1975); Soviet Math. Dokl. 16(1975), 1413-1417) proved the following theorem using Andre's theory: Let $(A, \mathfrak{m})$ and B be noetherian local rings and f: A → B be a flat local homomorphism. Then

(†) B is CI ⟹ A is CI,

A and $B/\mathfrak{m}B$ are CI ⟹ B is CI.

André (Localisation de la lissité formelle, Manuscripta Math. 13 (1974), 297-307) proved the following useful theorem:

(*) Let f: A → B be a local homomorphism of noetherian local rings. If f is formally smooth and A is excellent, then f is regular.

The question (B) on p.260 was recently solved by C. Rotthaus in the case A is semi-local (to appear in Nagoya Math. J.). André's theorem (*) plays an important role in her proof. In the general case even the problem (A) is open, but when A is an algebra of finite type over a field Problem (A') was solved by P. Valabrega (J. Math. Kyoto Univ. 15(1975), 387-395). Later he generalized his result to the case where k is a

1-dimensional excellent domain of characteristic 0. (Nagoya Math. J. 61 (1976)).

L.J.Ratliff (Catenary rings and the altitude formula, Amer. J. Math. 94(1972)) proved the following beautiful theorem: A noetherian local domain A is catenary iff ht P + dim R/P = dim R holds for every $P \in \mathrm{Spec}(R)$.
He has also characterized universally catenary rings in many different ways. (Cf. his Springer LN 647 for references and for the definitions of his terminology.)

For excellent rings and Nagata rings, see also S. Greco, Two theorems on excellent rings, Nagoya Math. J.60 (1976), and many articles by K. Langmann (in German Journals) and by H. Seydi (mostly in C.R. Acad. Sci. Paris). We also note that R.Y. Sharp defined acceptable rings by replacing "regular" by "Gorenstein" throughout the definition of excellent rings. (Acceptable rings and homomorphic images of Gorenstein rings, J. Algebra 44(1977), 246-261).

Finally, in connection with our Ch.6 we list a few important recent works:

Northcott, Finite Free Resolutions, Cambridge Tracts 71, Cambridge Univ. Press, 1976.
Peskine-Szpiro, Dimension projective finie et cohomologie locale, Publ. IHES 42 (1973), 47-119.
Hochster, Topics in the homological theory of modules over commutative rings, Regional conference series 24, AMS 1975.

INDEX

INDEX OF SYMBOLS

INDEX OF SYMBOLS