Lectures On
Unique Factorization Domains

By

P. Samuel

Tata Institute Of Fundamental Research, Bombay
1964

Lectures On
Unique Factorization Domains

By

P. Samuel

Notes by

M. Pavman Murthy

Tata Institute of Fundamental Research
Bombay
1964

Contents

1 Krull rings and factorial rings **1**

1 Divisorial ideals 1
2 Divisors 2
3 Krull rings 4
4 Stability properties 8
5 Two classes of Krull rings 11
6 Divisor class groups 14
7 Applications of the theorem of Nagata 19
8 Examples of factorial rings 25
9 Power series over factorial rings 32

2 Regular rings **37**

1 Regular local rings 37
2 Regular factorial rings 41
3 The ring of restricted power series 42

3 Descent methods **45**

1 Galoisian descent 45
2 The Purely inseparable case 50
3 Formulae concerning derivations 51
4 Examples: Polynomial rings 53
5 Examples: Power series rings 56

Chapter 1

Krull rings and factorial rings

In this chapter we shall study some elementary properties of Krull rings **1**
and factorial rings.

1 Divisorial ideals

Let A be an integral domain (or a domain) and K its quotient field. A *fractionary ideal* $\mathscr{U}$ is an A-sub-module of K for which there exists an element $d \in A(d \neq 0)$ such that $d\mathscr{U} \subset A$ i.e. $\mathscr{U}$ has "common denominator" d). A fractionary ideal is called a *principal ideal* if it is generated by one element. $\mathscr{U}$ is said to be *integral* if $\mathscr{U} \subset A$. We say that $\mathscr{U}$ is *divisorial* if $\mathscr{U} \neq (0)$ and if $\mathscr{U}$ is an intersection of principal ideals. Let $\mathscr{U}$ be a fractionary ideal and $\mathscr{V}$ non-zero A-submodule of K. Then the set $\mathscr{U} : \mathscr{V} = \{x \in K \big| x\mathscr{V} \subset \mathscr{U}\}$ is a fractionary ideal. The following formulae are easy to verify.

(1) $(\bigcap\limits_i \mathscr{U}_i : (\sum\limits_j \mathscr{V}_j) = \bigcap\limits_{i,j}(\mathscr{U}_i : \mathscr{V}_j)$.

(2) $\mathscr{U} : \mathscr{V}\mathscr{V}' = (\mathscr{U} : \mathscr{V}) : \mathscr{V}'$.

(3) If $x \in K$, $x \neq 0$, then $\mathscr{V} : Ax = x^{-1}\mathscr{V}$.

Lemma 1.1. *Let $\mathscr{U}$ be a fractionary ideal $\neq (0)$ and $\mathscr{V}$ a divisorial ideal. Then $\mathscr{V} : \mathscr{U}$ is divisorial.*

Proof. Let $\mathscr{V} = \bigcap_i Ax_i$. Then $\mathscr{V} : \mathscr{U} = \bigcap_i (Ax_i : \mathscr{U}) = \bigcap_i (\bigcap_{a \in \mathscr{U}} \frac{Ax_i}{a})$ □

2 **Lemma 1.2.** *(1) Let $\mathscr{U} \neq (0)$ be a fractionary ideal. Then the smallest divisorial ideal containing $\mathscr{U}$, denoted by $\overline{\mathscr{U}}$, is $A : (A : \mathscr{U})$.*

(2) If $\mathscr{U}, \mathscr{V} \neq (0)$, then $\overline{\mathscr{U}} = \overline{\mathscr{V}} \Leftrightarrow A : \mathscr{U} = A : \mathscr{V}$.

Proof. (1) By Lemma 1.1, $A : (A : \mathscr{U})$ is divisorial. Obviously $\mathscr{U} \subset A : (A : \mathscr{U})$. Suppose now that $\mathscr{U} \subset Ax$, $x \neq 0$, $x \in K$. Then $A : \mathscr{U} \supset A : Ax = Ax^{-1}$. Thus $A : (A : \mathscr{U}) \subset A : Ax^{-1} = Ax$ and (1) is proved.

(2) is a trivial consequence of (1) and the proof of Lemma 1.2 is complete.

□

2 Divisors

Let $I(A)$ denote the set of non-zero fractionary ideals of the integral domain A. In $I(A)$, we introduce an equivalence relation $\sim$, called *Artin equivalence* (or *quasi Gleichheit*) as follows:
$\mathscr{U} \sim \mathscr{V} \Leftrightarrow \overline{\mathscr{U}} = \overline{\mathscr{V}} \Leftrightarrow A : \mathscr{U} = A : \mathscr{V}$. The quotient set $I(A)/\sim$ of $I(A)$ by the equivalence relation $\sim$ is called the set of *divisors of A*. Thus there is an l-1 correspondence between the set $D(A)$ of divisors and the set of divisorial ideals. Let d denote the canonical mapping $d : I(A) \to I(A)/\sim$. Now, $I(A)$ is partially ordered by inclusion and we have $\mathscr{U} \subset \mathscr{V} \Rightarrow \overline{\mathscr{U}} \subset \overline{\mathscr{V}}$. Thus this partial order goes down to the quotient set $I(A)/\sim$ by d. If $\mathscr{U} \subset \mathscr{V}$, we write $d(\mathscr{V}) \leq d(\mathscr{U})$. On $I(A)$ we have the structure of an ordered commutative monoid given by the composition law $(\mathscr{U}, \mathscr{V}) \rightsquigarrow \mathscr{U}\mathscr{V}$-with A acting as the unit element. Let $\mathscr{U}, \mathscr{U}', \mathscr{V} \in I(A)$ and $\mathscr{U} \sim \mathscr{U}'$ *i.e.* $A : \mathscr{U} = A : \mathscr{U}'$. We have $A : \mathscr{U}\mathscr{V} = (A : \mathscr{U}) : \mathscr{V} = (A : \mathscr{U}') : \mathscr{V} = A : \mathscr{U}'\mathscr{V}$. Hence $\mathscr{U}\mathscr{V} \sim$
3 $\mathscr{U}'\mathscr{V}$. Thus $D(A)$ acquires the structure of a commutative monoid, with

the composition law $(\bar{\mathscr{U}}, \bar{\mathscr{V}}) \to \overline{\mathscr{U}\mathscr{V}}$. We write the composition law in $D(A)$ additively. Thus $d(\mathscr{U}\mathscr{V}) = d(\mathscr{U}) + d(\mathscr{V})$ for $\mathscr{U}, \mathscr{V} \in I(A)$. Since the order in $D(A)$ is compatible with the compositional law in $D(A)$, $D(A)$ is a commutative ordered monoid with unit. We note that

$$d(\mathscr{U} \cap \mathscr{V}) \geq \sup(d(\mathscr{U}), d(\mathscr{V})$$

and

$$d(\mathscr{U} + \mathscr{V}) = \inf(d(\mathscr{U}), d(\mathscr{V}).$$

Let K^* be the set of non-zero elements of K. For $x \in K^*$, we write $d(x) = d(Ax); d(x)$ is called a *principal* divisor.

Theorem 2.1. *For $D(A)$ to be a group it is necessary and sufficient that A be completely integrally closed.*

We recall that A is said to be *completely integrally* closed if whenever, for $x \in K$ there exist an $a \neq 0$, $a \in A s.t. ax^n \in A$ for every n, then $x \in A$.

We remark that if A is completely integrally closed, then it is integrally closed. The converse also holds if A is noetherian. A valuation ring of height > 1 is an example of an integrally closed ring which is not completely integrally closed.

Proof. Suppose $D(A)$ is a group. Let $x \in K$ and a be a non-zero element of A such that $ax^n \in A$, for every $n \geq 0$. Then
$a \in \bigcap_{n=0} Ax^{-n} = \mathscr{V}$ which is divisorial. Set $d(\mathscr{V}) = \beta$ and $\alpha = d(x^{-1})$. □

Now $\beta = \sup_{n\geq 0}(n\alpha)$. But $\beta + \alpha = \mathrm{Sup}_{n\geq 0}((n+1)\alpha)$
$= \sup_{q\geq 1}(q\alpha)$. Thus $\beta + \alpha \leq \beta$. Since $D(A)$ is a group $-\beta$ exists, **4**
and therefore

$$\alpha = (\beta + \alpha) - \beta \leq \beta - \beta = 0 \text{ i.e. } d(x) \geq 0.$$

Hence $Ax \subset A$ i.e. $x \in A$.
Conversely suppose that A is completely integrally closed. Let $\mathscr{U}$ be a divisorial ideal. Then $\mathscr{U} = x\mathscr{U}', \mathscr{U}' \subset A$. Since we already know

that principal divisors are invertible, we have only to prove that integral divisorial ideals are invertible. Let $\mathscr{V}$ be a divisorial ideal $\subset A$. Then $\mathscr{V}.(A:\mathscr{V}) \subset A$. Let $\mathscr{V}(A:\mathscr{V}) \subset Ax$, for some $x \in K$. Then $x^{-1}\mathscr{V}(A:\mathscr{V}) \subset A$. Thus $x^{-1}\mathscr{V} \subset A:(A:\mathscr{V}) = \mathscr{V}$, since $\mathscr{V}$ is divisorial. Thus $\mathscr{V} \subset \mathscr{V}x$. By induction $\mathscr{V} \subset \mathscr{V}x^n$, for every $n \geq 0$. Consider an element $b \neq 0$, $b \in \mathscr{V}$. Then $b(x^{-1})^n \subset \mathscr{V} \subset A$ for every $n \geq 0$. Hence $x^{-1} \in A$ i.e. $Ax \supset A$. Thus $\mathscr{V}(A:\mathscr{V}) \sim A$. Theorem 2.1 is completely proved. Notice that we have $d(\mathscr{U}) + d(A:\mathscr{U}) = 0$.

Let us denote by $F(A)$ the subgroup generated by the principal divisors. If $D(A)$ is a group, the quotient group $D(A)/F(A)$ is called the *divisor class group* of A and is denoted by $C(A)$.

In this chapter we shall study certain properties of the group $C(A)$.

3 Krull rings

Let $\mathbb{Z}$ denote the ring of integers. Let I be a set. Consider the abelian group $\mathbb{Z}^{(I)}$. We order $\mathbb{Z}^{(I)}$ by means of the following relation:
for $(\alpha_i), (\beta_i) \in \mathbb{Z}^{(I)}$, $(\alpha_i) \geq (\beta_i)$ if $\alpha_i \geq \beta_i$, for all $i \in I$.

5 The ordered group $\mathbb{Z}^{(I)}$ has the following properties: (a) any two elements of $\mathbb{Z}^{(I)}$ have a least upper bound and a greatest lower bound i.e. $\mathbb{Z}^{(I)}$ is an ordered lattice. (b) The positive elements of $\mathbb{Z}^{(I)}$ satisfy the minimum condition i.e. given a nonempty subset of positive elements of $\mathbb{Z}^{(I)}$, there exists a minimal element in that set. Conversely any ordered abelian group satisfying conditions (a) and (b) is of the form $\mathbb{Z}^{(I)}$ for some indexing set I (for proof see Bourbaki, Algebre, Chapter VI).

Let A be an integral domain. We call A a *Krull ring* if $D(A) \approx \mathbb{Z}^{(I)}$, the isomorphism being order preserving.

Theorem 3.1. *Let A be an integral domain. Then A is Krull if and only if the following two conditions are satisfied.*

(a) A is completely integrally closed.

(b) The divisorial ideals contained in A satisfy the maximum condition.

In fact the above theorem is an immediate consequence of Theorem 2.1 and the characterization of the ordered group $\mathbb{Z}^{(I)}$ mentioned above. An immediate consequence of Theorem 3.1 is:

Theorem 3.2. *A noetherian integrally closed domain is a Krull ring.*

We remark that the converse of Theorem 3.2 is false. For example the ring of polynomials in an infinite number of variables over a field K is a Krull ring, but is not noetherian. In fact this ring is known to be factorial and we shall show later that any factorial ring is a Krull ring.

Let $e_i = (\delta_{ij})_{j\in I} \in \mathbb{Z}^{(I)}$, where δ_{ij} is the usual
Kronecker delta. The e_i are minimal among the strictly positive ele- 6
ments. Let A be a Krull ring and let φ be the order preserving isomorphism $\varphi : D(A) \to \mathbb{Z}^{(I)}$. Let $\underline{P}_i = \varphi^{-1}(e_i)$. We call the divisors $\underline{P}_i$ the *prime divisors*. Let $P(A)$ denote the set of prime divisors. Then any $\underline{d} \in D(A)$ can be written uniquely in the form

$$\underline{d} = \sum_{\underline{P}\in P(A)} n_{\underline{P}}\underline{P}$$

where $n_{\underline{P}} \in \mathbb{Z}$ and $n_{\underline{P}} = 0$ for almost all $\underline{P}$. Now let $x \in K^*$. Consider the representation

$$d(x) = \sum_{\underline{P}\in P(A)} v_{\underline{P}}(x)\underline{P}, v_{\underline{P}}(x) \in \mathbb{Z}, v_{\underline{P}}(x) = 0$$

for almost all $\underline{P} \in P(A)$. Since $d(xy) = d(x) + d(y)$ we have, $v_{\underline{P}}(xy) = v_{\underline{P}}(x) + v_{\underline{P}}(y)$ for all $\underline{P}$. Further $d(x + y) \geq d(Ax + Ay) = \inf(d(x), d(y))$. This, in terms of $v_{\underline{P}}$, means that $v_{\underline{P}}(x + y) \geq \inf(v_{\underline{P}}(x), v_{\underline{P}}(y))$. We set $v_{\underline{P}}(0) = +\infty$. Thus the $v_{\underline{P}}$ are all discrete valuations of K. These are called the *essential valuations* of A.

Let $\underline{P}$ be a prime divisor. Let $\mathscr{Y}$ be the divisorial ideal corresponding to $\underline{P}$. As $\underline{P}$ is positive, $\mathscr{Y}$ is an integral ideal. We claim that $\mathscr{Y}$ is a *prime* ideal. For let $x, y \in A$, $xy \in \mathscr{Y}$. Then $d(xy) \geq \underline{P}$ i.e. $d(x) + d(y) \geq \underline{P}$ i.e. $v_{\underline{P}}(x) + v_{\underline{P}}(y) \geq 1$. As $v_{\underline{P}}(x) \geq 0$, $v_p(y) \geq 0$, we have $v_{\underline{P}}(x) \geq 1$ or $v_{\underline{P}}(y) \geq 1$; i.e. $x \in \mathscr{Y}$ or $y \in \mathscr{Y}$. Further the divisorial ideal
corresponding to $n\underline{P}$ is $\{x \in A | v_{\underline{P}}(x) \geq n\}$, $n \geq 0$. The prime ideal 7
$\mathscr{Y}$ is the centre of the valuation $v_{\underline{P}}$ on A (i.e. the set of all elements $x \in A$ s.t. $v_{\underline{P}}(x) \geq 0$). Since the prime divisors are minimal among the set of positive divisors, the corresponding divisorial ideals, which we call *prime divisorial ideals*, are maximal among the integral divisorial

ideals. The following lemma shows that the divisorial ideals which are prime divisorial and this justifies the terminology 'prime divisorial'.

Lemma 3.3. *Let $\mathscr{G}$ be a prime ideal $\neq (0)$. Then $\mathscr{G}$ contains some prime divisorial ideal.*

Proof. Take an $x \in \mathscr{G}$, $x \neq 0$. Let $d(x) = \sum_i n_i P_i$, (finite sum), $n_i > 0$, $\underline{P}_i \in P(A)$. Let $\mathscr{Y}_i$ be the prime ideal corresponding to $\underline{P}_i$. Let $y \in \prod \mathscr{Y}_i^{n_i}$, $y \neq 0$. Then $v_{P_i}(y) \geq n_i$. Hence $d(y) \geq d(x)$ i.e. $Ay \subset Ax$. Thus $\prod \mathscr{Y}_i^{n_i} \subset Ax \subset \mathscr{G}$. As $\mathscr{G}$ is prime, $\mathscr{Y}_i \subset \mathscr{G}$ for some i. □

Corollary. *A prime ideal is prime divisorial if and only if it is height 1.*

(We recall that a prime ideal is of *height one* if it is minimal among the non-zero prime ideals of A).

Proof. Let $\mathscr{Y}$ be a prime divisorial ideal. If $\mathscr{Y}$ is not of height 1, then $\mathscr{Y} \underset{\neq}{\supset} \mathscr{G}$, where $\mathscr{G}$ is a non-zero prime ideal. By the above lemma $\mathscr{G}$ contains a prime divisorial ideal $\mathscr{Y}'$. Thus $\mathscr{Y} \underset{\neq}{\supset} \mathscr{Y}'$. This contradicts the maximality of $\mathscr{Y}'$ among integral divisorial ideals. Conversely let $\mathscr{Y}$ be a prime ideal of height 1. Then, by the above lemma, $\mathscr{Y}$ contains a prime divisorial ideal $\mathscr{Y}'$. Hence $\mathscr{Y} = \mathscr{Y}'$ and the proof of the Corollary is complete. □

8 **Lemma 3.4.** *Let $\mathscr{Y}$ be a divisorial ideal corresponding to a prime divisor $\underline{P}$. Then the ring of quotients $A_{\mathscr{Y}}$ is the ring of $v_{\underline{P}}$.*

Proof. Let $\dfrac{a}{s} \in A_{\mathscr{Y}}$, $a \in A$, $s \in A - \mathscr{Y}$. Then $v_{\underline{P}}(s) = 0$, $v_{\underline{P}}(a) \geq 0$, $v_P\left(\dfrac{a}{s}\right) \geq 0$. Conversely let $x \in K^*$ with $v_{\underline{P}}(x) \geq 0$. Set $d(x) = \sum_{\underline{Q}} n(\underline{Q})\underline{Q}$, and let $\mathscr{G}$ be the prime divisorial ideal corresponding to $\underline{Q}$. Let $\mathscr{V} = \prod_{n(\underline{Q})<0} \mathscr{G}^{-n(\underline{Q})}$. As the prime divisor $\underline{Q}$, with $n(\underline{Q}) < 0$ are different from $\underline{P}$, we have $\mathscr{V} \not\subset \mathscr{Y}$. Take $s \in \mathscr{V}$, $s \notin \mathscr{Y}$. Then $v_{\underline{Q}}(sx) \geq 0$ for all $\underline{Q}$ i.e. $d(sx) \geq 0$ i.e. $sx \in A$. Hence $x \in A_{\mathscr{Y}}$. This proves the lemma. □

Corollary. *$A = \bigcap_{\mathscr{Y}} A_{\mathscr{Y}}$, $\mathscr{Y}$ running through all prime ideals of height one. We shall now give a characterization of Krull rings in terms of discrete valuation rings.*

Theorem 3.5 ("valuation Criterion"). *Let A be a domain. Then the following conditions are equivalent:*

(a) A is a Krull ring.

(b) There exists a family $(v_i)_{i \in I}$ of discrete valuations of K such that

(1) $A = \bigcap_i R_{v_i}$ (i.e. $x \in A$ if and only if $v_i(x) \geq 0$), where R_{v_i} denotes the ring of v_i,

(2) For every $x \in A$, $v_i(x) = 0$, for almost all $i \in I$.

Proof. (a) $\Rightarrow$ (b). In fact $A = \bigcap_{\underline{P} \in P(A)} R_{v_{\underline{P}}}$ and condition (2) of (b) is obvious from the very definition of $v_{\underline{P}}$.

(b) $\Rightarrow$ (a). Since a discrete valuation ring is completely integrally closed and any intersection of completely integrally closed domains is completely integrally closed, we conclude that A is completely integrally closed. Now let $x \in K^*$. Then **9**

$$Ax = \left\{ y \in K \middle| v_i(y) \geq v_i(x), \text{ for } i \in I \right\}.$$

Thus, because of condition (2), any divisorial ideal is of the form $\left\{ x \in K \middle| v_i(x) \geq n_i, i \in I, (n_i) \in \mathbb{Z}^{(I)} \right\}$, and conversely. Any integral divisorial ideal $\mathscr{V}$ is defined by the conditions $v_i(x) \geq n_i$, $n_i \geq 0$, $n_i = 0$ for almost all $i \in I$. There are only finitely many divisorial ideals $\mathscr{V}'$ containing $\mathscr{V}$ (in fact the number of such ideals is $\prod_i (1 + n_i)$). Hence A satisfies the maximum condition for integral divisorial ideals therefore by Theorem 3.1, A is a Krull ring.

□

Remark. Let $\mathscr{G}$ be a prime divisorial ideal of A defined by $v_i(x) \geq n_i$, $n_i \geq 0$, $n_i = 0$ for almost all i. Let $\mathscr{Y}_i$ be the centre of v_i on A. Then

$\prod_i \mathscr{Y}_i^{n_i} \subset \mathscr{G}$. Hence $\mathscr{Y}_i \subset \mathscr{G}$ for some i. But height $\mathscr{G} = 1$. Hence $\mathscr{Y}_i = \mathscr{G}$. Thus every prime divisorial ideal is the centre of some v_i. Now $A_{\mathscr{G}} \subset R_{v_i}$. But $A_{\mathscr{G}}$, being a discrete valuation ring, is a maximal subring of K. Hence $A_{\mathscr{G}} = R_{v_i}$ = ring of $v_{\underline{Q}}$, where $\underline{Q}$ is the prime divisor corresponding to $\mathscr{G}$. Thus every essential valuation of A is equivalent to some v_i. The family $(v_i)_{i\in I}$ may be 'bigger', but contains all essential valuations.

4 Stability properties

In this section we shall see that Krull rings behave well under localisations polynomial extensions etc.

10 **Proposition 4.1.** *Let K be a field and A_α a family of Krull rings. Assume that any $x \in B = \bigcap_\alpha A_\alpha$, $x \neq 0$ is a unit in almost all A_α. Then B is a Krull ring.*

Proof. By theorem 3.5, $A_\alpha = \bigcap_{i\in I_\alpha} R(v_{\alpha,i})$, where $R(v_{\alpha,i})$ are discrete valuation rings and every $x \in A_\alpha$ is a unit in almost all $R(v_{\alpha,i})$, $i \in I$. Now $B = \bigcap_{\alpha,i} R(v_{\alpha,i})$. Let $x \neq 0$, $x \in B$. Then by assumption, x is a unit in almost all A_α, i.e. $v_{\alpha,i}(x) = 0$, for all $i \in I_\alpha$, and almost all α. Then x is not a unit in at most a finite number of the A_β, say $A_{\beta_1}, \ldots A_{\beta_t}$. Now $v_{\beta_{ji}}(x) = 0$ for almost all i, $j = 1, \ldots, t$. Thus $v_{\alpha,i}(x) = 0$ for almost all α and i. The proposition follows immediately from Theorem 3.5. □

Corollary. *(a) A finite intersection of Krull rings is a Krull ring.*

(b) Let A be a Krull ring, K its quotient field. Let L be a subfield of K. Then $A \cap L$ is a Krull ring.

Proposition 4.2. *Let A be a Krull ring. Let S be any multiplicatively closed set with $0 \notin S$. Then the ring of quotients $S^{-1}A$ is again a Krull ring. Further the essential valuations of $S^{-1}A$ are those valuation v_P for which $\mathscr{Y} \cap S = \phi$, $\mathscr{Y}$ being the prime divisorial ideal corresponding to P.*

Proof. By Theorem 3.5 we have only to prove that $S^{-1}A = \bigcap_{\mathscr{Y}\in I} A_{\mathscr{Y}}$, I, being the set of prime ideals of height one which do not intersect S. Trivially, $S^{-1}A \subset \bigcup_{\mathscr{Y}\in I} A_{\mathscr{Y}}$. Conversely let $x \in \bigcup_{\mathscr{Y}\in \mathscr{I}} A_{\mathscr{Y}}$. We have $v_P(x) \geq 0$, for any prime divisor corresponding to $\mathscr{Y} \in I$. For a 11
prime divisorial ideal $\mathscr{G}$ with $\mathscr{G} \cap S \neq \emptyset$, choose $s_{\mathscr{G}} \in \mathscr{G} \cap S$. Set $s = \prod_{v_Q(x)<0} s_{\mathscr{G}}^{-v_Q(x)}$, where Q is the prime divisor corresponding to $\mathscr{G}$. Then $sx \in A$ i.e. $x \in S_A^{-1}$ and the proposition is proved. □

Proposition 4.3. *Let A be a Krull ring. Then the ring $A[X]$ of polynomials is again a Krull ring.*

Proof. Let A be defined by the discrete valuation rings $\{v_i\}_{i\in I}$. If v is a discrete valuation of A, then v can be extended to $A[X]$, by putting $\overline{v}(a_o + a_1 x + \cdots + a_q x^q) = \min_j(v(a_j))$ and then to the quotient field $K(X)$ of $A[X]$ (K is the quotient field of A) by putting $\overline{v}(f/g) = \overline{v}(f) - \overline{v}(g)$. Let $\Phi = \{\overline{v}_i\}_{i\in I}$. On the other hand, let Ψ denote the set $p(X)$-adic valuation of $K(X)$, where $p(X)$, runs through all irreducible polynomials $K[X]$. We now prove that $A[X]$ is a Krull ring with $\Phi \bigcup \Psi$ as a set of valuations defining it. Let $f \in K(X)$. If $\omega(f) \geq 0$ for all $\omega' \in \Psi$, then $f \in K[X]$, say $f = a_o + a_1 X + \cdots + a_q X^q : a_i \in K$. If further $v(f) \geq 0$, for all $v \in \Phi$, then $v(a_i) \geq 0$, $v \in \Phi$, $i = 1, \ldots, q$. Since A is a Krull ring, $a_i \in A$, $i = 1, \ldots, q$. Hence $f \in A[X]$. To prove that $A[X]$ is a Krull ring, it only remains to verify that for $f \in A[X]$, $v(f) = 0 = \omega(f)$ for almost all $v \in \Phi$, $\omega \in \Psi$. Since KX is a principal ideal domain, $\omega(f) = 0$, for almost all $\omega \in \Psi$. Further $\overline{v}_i(f) = \min_j(v_i(a_j)) = 0$ for almost all $i \in I$, since A is a Krull ring. □

Corollary. *Let A be a Krull ring. Then $A[X_1, \ldots, X_n]$ is a Krull ring.* 12

Remark. Since, in a polynomial ring in a an infinite number of variables, a given polynomial depends only on a finite number of variables the above proof shows that a polynomial ring in an infinite number of variables over A is also a Krull ring,

Proposition 4.4. *Let A be a Krull ring. Then the ring of formal power series $A[[X]]$ is again a Krull ring.*

Proof. We note that $A[[X]] = \bigcap V_\alpha[[X]]_S \bigcap K[[X]]$, where S is the multiplicatively closed set $\{1, x, x^2, \dots\}$, K, the quotient field of A and V_α the essential valuation rings of A. Now $V_\alpha[[X]]_S$ and $K[[X]]$, being noetherian and integrally closed, are Krull rings, Now the proposition is an immediate consequence of Proposition 4.1. □

Proposition 4.5. *Let A be a Krull ring and K its quotient field. Let K' be a finite algebraic extension of K and A', the integral closure of A in K'. Then A' is also a Krull ring.*

Proof. Let K'' be the least normal extension of K containing K' and let A'' be the integral closure of A in K''. Since $A' = A'' \bigcap K'$, by Corollary (b), Prop. 4.1, it is sufficient to prove that A'' is a Krull ring. Let Φ be the family of essential valuations of A. Let Φ'' be the family of all discrete valuations of K'' whose restriction to K are in Φ. It is well known (see Zariski-Samuel. Commutative algebra Vol. 2) that every discrete valuation v of K extends to a discrete valuation of K'' and
13 that such extensions are finitely many in number. We shall show that A'' is a Krull ring by using the valuation criterion with Φ'' as family of valuations. We prove (i) $x \in A''$ if and only if $\omega'(x) \geq 0$, for all $\omega \in \Phi''$ □

Proof. Let $x \in A''$. Then x satisfies a monic polynomial, say $x^n + a_{n-1}x^{n-1} + \cdots + a_o = 0$, $a_i \in A$. If possible let $\omega(x) < 0$, for some $\omega \in \Phi$. Then $\omega(-a_{n-1}x^{n-1} - \cdots - a_o) \geq \inf(\omega(a_{n-1}x^{n-1}), \dots, \omega(a_o) > \omega(x^n)$, since $\omega(a_i) \geq 0$. Contradiction. Conversely let $x \neq 0$, $x \in K''$ with $\omega(x) \geq 0$, for all $\omega \in \Phi''$. Let σ be any K-automorphism of K''. Then $\omega o \sigma \in \Phi''$. Hence $\omega(\sigma(x)) \geq 0$ for all K-automorphisms σ of K''. Let us now consider the minimal polynomial $f(X)$ of x over K; say $f(X) = X^r + \alpha_{r-1}X^{r-1} + \cdots + \alpha_o$, $\alpha_i \in K$. Since the α_i are symmetric polynomials in the $\sigma(x)$, we have $v(\alpha_i) \geq 0$, for all $v \in \Phi$. Since A is a Krull ring, $\alpha_i \in A$ and (i) is proved. (ii) For $x \neq 0$, $x \in A''$, $\omega(x) = 0$, for almost all $\omega \in \Phi''$. □

Proof. Let $x^n + a_{n-1}x^{n-1} + \cdots + a_o = 0$ be an equation satisfied by x (which expresses the integral dependence of x). We may assume $a_o \neq 0$. If $\omega(x) > 0$, then $\omega(a_o) = \omega(x^n + a_{n-1}x^{n-1} + \cdots + a_1 x) \geq \omega(x) > 0$. Since

A is a Krull ring there are only a finitely many $v \in \Phi$ such that $v(a_o) > 0$ and since every $v \in \Phi$ admits only a finite number of extensions, (*ii*) is proved and with it, the proposition. □

5 Two classes of Krull rings

Theorem 5.1. *Let A be a domain. The following conditions are equivalent.*

(a) *Every fractionary ideal* $\mathscr{V} \neq (0)$ *of A is invertible. (i.e. there exists a fractionary ideal* $\mathscr{V}^{-1}$ *such that* $\mathscr{V}\mathscr{V}^{-1} = A$). 14

(b) *A is a Krull ring and every non-zero ideal is divisorial.*

(c) *A is a Krull ring and every prime ideal* $\neq (0)$ *is maximal (minimal).*

(d) *A is a noetherian, integrally closed domain such that every prime ideal* $\neq (0)$ *is maximal.*

Proof. $(a) \Rightarrow (b)$. Let $\mathscr{V}^{-1}$ exist. Then $\mathscr{V}^{-1} = A : \mathscr{V}$. For $\mathscr{V}\mathscr{V}^{-1} \subset A \Rightarrow \mathscr{V}^{-1} \subset A : \mathscr{V}$ and $\mathscr{V}\mathscr{V}^{-1} = A$ and $\mathscr{V}(A : \mathscr{V}) \subset A$ together imply $A : \mathscr{V} \subset \mathscr{V}^{-1}$. Further $\mathscr{V} = A : (A : \mathscr{V})$; the condition that $\mathscr{U}$ and $\mathscr{V}$ are Artin equivalent becomes "$\mathscr{U} = \mathscr{V}$". Thus $D(A)$ is a group. The following lemma now proves the assertion $(a) \Rightarrow (b)$ because of Theorem 2.1. □

Lemma . $\mathscr{V} \subset A$ *invertible* $\Rightarrow \mathscr{V}$ *is finitely generated. (and thus (a) implies that A is noetherian).*

Proof. Since $\mathscr{V}\mathscr{V}^{-1} = A$, we have $1 = \sum_{1} x_i y_i$, $x_i \in \mathscr{V}$, $y_i \in \mathscr{V}^{-1}$. For $x \in \mathscr{V}$, we have $x = \sum_i x_i(y_i x)$ i.o. $\mathscr{V} = \sum_i Ax_i$. □

$(b) \Rightarrow (c)$, Since A is a Krull ring and every non-zero ideal is divisorial, every non-zero prime ideals is of height 1.
$(c) \Rightarrow (a)$. Let $\mathscr{V}$ be any fractionary ideal. Then $\mathscr{V}(A : \mathscr{V}) \subset A$ and since $D(A)$ is a group, $\mathscr{V}(A : \mathscr{V})$ is Artin-equivalent to A. Hence $\mathscr{V}(A : \mathscr{V})$ is not contained in any prime divisorial ideal. But by (c). Since every

prime ideal $\neq (0)$ is prime divisorial, $\mathscr{V}(A : \mathscr{V})$ is not contained in any maximal ideal, and hence $\mathscr{V}(A : \mathscr{V}) = A$.

15 $(a) \Rightarrow (d)$. That A is noetherian is a consequence of the lemma used in the proof of the implication $(a) \Rightarrow (b)$. That A is integrally closed and every prime ideal $\neq (0)$ is maximal is a consequence of the fact that $(a) \Rightarrow (c)$.

$(d) \Rightarrow (c)$. This is an immediate consequence of the fact that a noetherian integrally closed domain is a Krull ring. The proof of Theorem 5.1 is now complete.

Definition 5.2. *A ring A is called a Dedekind ring if A is a domain satisfying any one of the equivalent conditions of Theorem 5.1.*

Remark. (1) The condition (c) can be restated as: A is a Dedekind ring if A is a Krull ring and its Krull dimension is atmost 1.

(2) Let A be a Dedekind ring and K its quotient field. Let K' be a finite algebraic extension of K and A', the integral closure of A in K'. Then A' is again a Dedekind ring.

Proof. By Proposition 4.5 it follows that A' is a Krull ring. For a non-zero prime ideal $\mathscr{Y}'$ of A', we have, by the Cohen-Seidenberg theorem, height $(\mathscr{Y}')$ = height $(\mathscr{Y}' \cap A) \leq 1$. Now (2) is a consequence of Remark (1).

(3) Let A be a domain and $\mathscr{U}$, a fractionary ideal. Then $\mathscr{U}$ is invertible if and only if $\mathscr{U}$ is a projective A-module. If further, A is noetherian, then $\mathscr{U}$ is projective if and only if $\mathscr{U}$ is locally principal (i.e $\mathscr{U}_{\mathscr{M}}$ is principal for all maximal ideals $\mathscr{M}$ of $\triangle$).

□

We shall say that a ring A satisfies the *condition* (M) if A satisfies the maximum condition for principal ideals. For instance Krull rings satisfy (M).

16 **Theorem 5.3.** *For a domain A, the following conditions are equivalent.*

a) A is a Krull ring and every prime divisorial ideal is principal.

b) *A is a Krull ring and every divisorial ideal is principal.*

c) *A is a Krull ring and the intersection of any two principal ideals is principal.*

d) *A satisfies* (M) *and any elements of A have a least common multiple (1.c.m.) (i.e.* $Aa \cap Ab$ *is principal for* $a, b \in A$*).*

e) *A satisfies* (M) *and any two elements of A have greatest common divisor* $(g.c.d.)$*.*

f) *A satisfies* (M) *and every irreducible element of A is prime.*

(We recall that $a \in A$ *is* irreducible if Aa is maximal among principal ideals, an element $p \in A$ is *prime if* $A\,p$ *is a prime ideal).*

g) *A has the unique factorization property. More precisely, there exists a subset* $P \subset A$, $0 \notin P$ *such that every* $x \neq 0$, $x \in A$ *can be written in on and only way as* $x = u. \prod\limits_{p \in P} p^{n(p)}$, $n(p) \geq 0$, $n(p) = 0$ *for almost all* p, u *being a unit.*

Proof. (a) $\Rightarrow (b)$. Since prime divisors generate $D(A)$, we have $D(A) = F(A)$.

(b) $\Rightarrow (c)$. Trivial.

(c) $\Rightarrow (b)$. Let $\mathscr{V}$ be any divisorial ideal $\neq (0)$.

□

We shall show that $\mathscr{V}$ is principal. We may assume that $\mathscr{V}$ is integral. Let $\mathscr{V} = \bigcap\limits_{\lambda \in I} Ac_\lambda$, $c_\lambda \in K$. Consider the set of all divisorial ideals $\mathscr{V}_J =$ 17
$\bigcap\limits_{\lambda \in J} Ac_\lambda \bigcap A$, where J runs over all finite subsets I. We have $\mathscr{V} \subset \mathscr{V}_J \subset A$, for all finite subsets $J \subset I$. Since A is a Krull ring, any integral divisorial ideal is defined by the inequalities $v(x) \geq n_v$, $n_v > 0$, $n_v = 0$ for almost all v, v running through all essential valuations of A. Hence there are only finitely many divisorial ideals between $\mathscr{V}$ and A. Hence $\mathscr{V} = \bigcap_{\lambda \in J} Ac$, for some finite set $J \subset I$. By choosing a suitable common denominator for c_λ, $\lambda \in J$, we may assume that $c_\lambda \in A$. Now $(c) \Rightarrow (b)$ is immediate.

(b) $\Rightarrow (a)$. Trivial.

(c) $\Rightarrow (d)$. Trivial.

(d) $\Rightarrow$ (e). This is an immediate consequence of the following elementary property of ordered abelian groups, namely: in an ordered abelian group G, the existence of sup (a, b) is equivalent to the existence of $\inf(a, b)$, for $a, b \in G$. (Apply this, for instance to $F(A)$) $(e) \Leftrightarrow (f) \Leftrightarrow (g)$. This follows from divisibility arguments used in elementary number theory.

(g) $\Rightarrow (c)$. For $K \in A$, $x \neq 0$, we write $x = u_x \prod_{p \in P} p^{v_p(x)}$, u being a unit. The set of all $\{v_p\}_{p \in P}$, defines a set Φ of discrete valuations of the quotient field X of A. It is clear that A satisfies the valuation criterion for Krull rings with Φ as the set of valuations. Further, for a, $b \in A$, $Aa \cap Ab = Ac$, where $c = u_x u_y \prod_{p \in P} p^{\max(v_P(x) v_P(g))}$. Hence $(g) \Rightarrow (c)$ and the proof of Theorem 5.3 is complete.

Definition 5.4. *A is said to be factorial if A is a domain satisfying any one of the conditions of Theorem 5.3.*

18 **Remark 5.5.** Let A be a noetherian domain with the property that every prime ideal of height 1 is principal. Then A is factorial.

Proof. We shall prove the condition (f). Set $b \in A$ be an irreducible element. By Krull's Principal Ideal Theorem, $Ab \subset \mathscr{Y}$, $\mathscr{Y}$, a prime ideal of height 1. By hypothesis, $\mathscr{Y}$ is principal. Since Ab is maximal among principal ideals, $Ab = \mathscr{Y}$. Of course A satisfies (M). □

6 Divisor class groups

Let A be a Krull ring. We recall that the divisor class group $c(A)$ of A is $\dfrac{D(A)}{F(A)}$, where $D(A)$ is the group of divisors of A and $F(A)$ the subgroup of $D(A)$ consisting of principal divisors of A. If A is a Dedekind ring, $C(A)$ is called the *group of ideal classes*. By Theorem 5.3, it is clear that a Krull ring A is factorial if and only if $C(A) = 0$.

Let A and B be Krull rings, with $A \subset B$. From now on we shall use the same notation for a prime divisor and the prime divisorial ideal corresponding to it. Let $\underline{P}$, $\underline{p}$ be prime divisors of B and A respectively. We write $\underline{P}\big|\underline{p}$ if $\underline{P}$ lies above $\underline{p}$ i.e. $\underline{P} \cap A = \underline{p}$. If $\underline{P}\big|\underline{p}$, the restriction of $v_{\underline{P}}$ to the quotient field of A is equivalent to $v_{\underline{p}}$, and we denote by $e(\underline{P}, \underline{p})$, the ramification index of $v_{\underline{p}}$ in $v_{\underline{P}}$. For a $\underline{p} \in P(A)$, we define

$$j(\underline{p}) = \sum_{\underline{P}\big|\underline{p}} e(\underline{P}, \underline{p})\underline{P}, \underline{P} \in \underline{P}(B).$$

The above sum is finite since $x \in \underline{p}$, $x \neq 0$ is contained in only finite many $\underline{P}, \underline{P} \in \underline{P}(B)$. Extending j by linearity we get a homomorphism of $D(A)$ into $D(B)$ which we also denote by j. We are interested in 19
the case in which j induces a homomorphism of $\bar{j} : C(A) \to C(B)$ i.e. $j(F(A)) \subset F(B)$. For $x \in A$, we write $d_A(x) = d(Ax) \in D(A)$ and $d_B(x) = d(Bx) \in D(B)$.

Theorem 6.1. *Let A and B be Krull rings with $A \subset B$. Then we have $j(d_A(x)) = d_B(x)$ if and only if the following condition is satisfied.* (NBU). *For every prime divisor P of B, height* $(P \cap A) \leq 1$.

Proof.

$$\begin{aligned} j(d_A(x)) &= j\Big(\sum_{\underline{p} \in P(A)} v_{\underline{p}}(x)\underline{p}\Big) \\ &= \sum_{\underline{p} \in P(A)} v_{\underline{p}}(x) \sum_{\underline{P}|\underline{p}} e(\underline{P}, \underline{p})\underline{P} = \sum_{\underline{p}, \underline{P}|\underline{p}} v_{\underline{P}}(x)\underline{P} \\ &= \sum_{\underline{P}, \underline{P} \cap A \in P(A)} v_{\underline{P}}(x)\underline{P}. \end{aligned}$$

□

If $\underline{P} \cap A = (0)$, then $v_{\underline{P}}(x) = 0$. Therefore,

$$j(d_A(x)) = \sum_{\text{height}(\underline{P} \cap A) \leq 1} v_{\underline{P}}(x)\underline{P}. \tag{1}$$

Now, if (NBU) is true, then $j(d_A(x)) = \sum\limits_{\underline{P}\in P(B)} v_{\underline{P}}(x)\underline{P} = d_B(x)$. On the other hand let $j(d_A(x)) = d_B(x)$ for every $x \in A$. Let $\underline{P} \in P(B)$ with $\underline{P} \cap A \neq (0)$. Choose $x \in \underline{P} \cap A$, $x \neq 0$. We have by (1) above

$$j(d_A(x)) = \sum_{\text{height } (\underline{P}\cap A)\leq 1} v_{\underline{P}}(x)\underline{P} = d_B(x) = \sum_{\underline{P}\in P(B)} v_{\underline{P}}(x)\underline{P}.$$

Since $v_{\underline{P}}(x) > 0$, we have height $(\underline{P} \cap A) = 1$ and the theorem is proved.

When (NBU) is true we have $\underline{j}(F(A)) \subset F(B)$ and therefore j induces a canonical homomorphism $\bar{j} : C(A) \to C(B)$.

20 We now give two sufficient conditions in order that (NBU) be true.

Theorem 6.2. *Let A and B be as in Theorem 6.1. Then* (NBU) *is satisfied if any one of the following two conditions are satisfied.*

(1) B is integral over A.

(2) B is a flat A-module (i.e the functor $\underset{A}{\otimes} B$ *is exact).*

Further, if (2) is satisfied we have $j(\mathscr{U}) = \mathscr{U}B$*, for every divisorial ideal* $\mathscr{U}$ *of A.*

Proof. If (1) is satisfied, (NBU) is an immediate consequence of the Cohen-Seidenberg theorem. □

Suppose now that (2) is satisfied. Let $\underline{P} \in P(B)$ with $\mathscr{U} = \underline{P} \cap A \neq (0)$. Suppose $\mathscr{U}$ is not divisorial. Choose a non-zero element $x \in \mathscr{U}$. Let $d(x) = \sum\limits_{i=1}^{n} v_{p_i}(x)\underline{p}_i \underline{p}_i \in P(A)$. Since height $\sigma > 1$ we have $\mathscr{U} \not\subset \underline{p}_i$ for $i = 1, \ldots, n$. By an easy reasoning on prime ideals there exists a $y \in \mathscr{U}$, $y \notin \bigcup\limits_{f=1}^{n} \underline{p}_i$. Then $d_A(x)$ and $d_A(y)$ do not have any component in common and therefore

$$d_A(xy) = d_A(x) + d_A(y) = \operatorname{Sup}(d_A(x), d_A(y)).$$

This, in terms of divisorial ideals, means that $Ax \cap Ay = Axy$. Since B is A-flat, we have $Bxy = Bx \cap By$; that is $d_B(x)$ and $d_B(y)$ do not have any component in common. But $x, y \in \underline{P} \cap A$. Contradiction.

We shall now prove that for any divisorial ideal $\mathscr{U} \subset A$, $j(\mathscr{U}) = \mathscr{U}B$. Since A is a Krull ring $\mathscr{U}$ is the intersection of finitely many principal ideals, say $\mathscr{U} = \bigcap_{i=1}^{n} Ax_i$, so that $d_A(\mathscr{U}) = \sup(d_A(x_i))$. Since 21
B is A-flat, we have $B\mathscr{U} = \bigcap_{i=1}^{n} Bx_i$. Thus $B\mathscr{U}$ is again divisorial. On the other hand, $d_B(B\mathscr{U}) = \sup_i(d_B(x_i)) = \sup_i(j(d_A(x))$. Noting that j is order preserving and that any order preserving homomorphism of $\mathbb{Z}^{(I)}$ into $\mathbb{Z}^{(J)}$ is compatible with the formation of sup and inf (to prove this we have only to check it component - wise), we have

$$B\mathscr{U} = \sup_i(j(d_A(x_i)) = j(\sup_i(d_A(x_i))) = j(d_A(\mathscr{U})).$$

Theorem 6.3 (Nagata)**.** *Let A be a Krull ring and S, a multiplicatively closed set in $A(0 \notin S)$. Consider the ring of quotients $S^{-1}A$ (which is A-flat). We have*

(a) $\bar{j} : C(A) \to C(S^{-1}A)$ *is surjective.*

(b) If S is generated by prime elements then $\bar{j}$ is bijective.

Proof. (a) Since $P(S^{-1}A) = \{\underline{p}S^{-1}A \mid \underline{p} \in P(A), \underline{p} \cap S = \phi\}$, $\bar{j}$ is surjective by Theorem 6.2, (2). □

Let us look at the kernel of $\bar{j}$. Let H be the subgroup of $D(A)$ generated by prime divisors $\underline{p}$ with $\underline{p} \cap S \neq \phi$. Then it is clear that

$$\operatorname{Ker}(\bar{j}) = \frac{(H + F(A))}{F(A)} \approx \frac{H}{(H \cap F(A))} \tag{6.4}$$

Suppose that S is generated by prime elements. Let $\underline{p} \in P(A)$, with $\underline{p} \cap S \neq \phi$, say $s_1 \cdots s_n \in \underline{p}$, where s_i are prime elements. Then since $\underline{p}$ is minimal $\underline{p} = As_i$ for some s_i. Thus $H \subset F(A)$ and hence $\bar{j}$ is a bijection.

'Theorem 6.3 (Nagata)**.** *Let A be a noetherian domain and S a multiplicatively closed set of A generated by prime elements $\{\underline{p}_i\}_{i \in I}$. If $S^{-1}A$ is a Krull ring then A is a Krull ring and $\bar{j}$ is bijective.* 22

Proof. By virtue of Theorem 6.3, we have only to prove that A is integrally closed (then it will be a Krull ring, since it is noetherian). Now A_{Ap_i} is a local noetherian domain whose maximal ideal is principal and hence A_{Ap_i} is a discrete valuation ring. It suffices to show that $A = S^{-1}A \cap (\bigcap_{i \in I} A_{Ap_i})$. We may assume $Ap_i \neq Ap_j$ for $i \neq j$. Let $a/s \in S^{-1}A \cap (\bigcap_i A_{Ap_i})$, $a \in A$, $s \in S$, $s = \prod_i p_i^{n(i)}$. We have $v_{p_i}(a/s) \geq 0$, where v_{p_i} is the valuation corresponding to $A_{A_{p_i}}$. By our assumption, $v_{p_i}(p_j) = 0$ for $j \neq i$. Hence $v_{p_i}(a) \geq v_{p_i}(s) = n(i)$. Hence S divides a i.e. $a/s \in A$. □

Corollary. *Let A be a domain and S a multiplicatively closed set generated by a set of prime elements. Let $S^{-1}A$ be factorial. If A is noetherian or a Krull ring, then A is factorial.*

Proof. By Theorems 6.3 and 6.3, $\bar{j} : C(A) \to C(S^{-1}A)$ is bijective. □

Theorem 6.4 (Gauss)**.** *Let R be a Krull ring. Then $\bar{j} : C(R) \to C(R[X])$ is bijective. In particular, R is factorial if and only if $R[X]$ is factorial.*

(Since $R[X]$ is R-flat, $\bar{j}$ is defined).

Proof. Set $A = R[X]$, $S = R^*$, the set of non-zero elements of R. Then $S^{-1}A = K[X]$, where K is the quotient field of R. Thus $C(S^{-1}A) = 0$ i.e.

$$C(A) = \operatorname{Ker}(\bar{j} : C(A) \to C(S^{-1}A)) = \frac{(H + F(A))}{F(A)}$$

23 where H is the subgroup of $D(A)$ generated by $P \in P(A)$, with $P \cap R \neq (0)$ (see formula 6.4). Hence $D(A) = H + F(A)$. Since $R[X]$ is R-flat, by Theorem 6.2, (2) we have

$$j(P \cap R) = (P \cap R)R[X] = P, \text{ for } P \in P(A), P \cap R \neq (0).$$

Hence $j(D(R)) = H$ and therefore $\bar{j}$ is surjective, since $D(A) = H + F(A)$. Now an ideal $\mathscr{U}$ of R is principal if and only if $\mathscr{U}R[X]$ is principal. Therefore $\bar{j}$ is injective. Thus $\bar{j}$ is bijective.

Let A be a noetherian ring and $\mathscr{M}$ an ideal contained in the radical of A (i.e. the intersection of all maximal ideals of A). If we put on A the

$\mathscr{M}$-adic topology, then $(A, \mathscr{M})$ is called a *Zariski ring*. The completion $\hat{A}$ of A is again a Zariski ring and it is well known that $\hat{A}$ is A-flat and $A \subset \hat{A}$. □

Theorem 6.5 (Mori)**.** *Let $(A, \mathscr{M})$ be a Zariski ring. Then if $\hat{A}$ is a Krull ring, then so is A. Further $j : C(A) \to C(\hat{A})$ is injective. In particular if $\hat{A}$ is factorial, so is A.*

Proof. Let K and L be the quotient fields of A and $\hat{A}$ respectively; $K \subset L$. To prove that A is a Krull ring we observe that $A = \hat{A} \cap K$. For if $\frac{a}{b} \in \hat{A} \cap K$, $a, b \in A$, then $a \in \hat{A}b \cap A = Ab$, i.e. $\frac{a}{b} \in A$. Hence A is a Krull ring. By virtue of Theorem 6.2 (2), to prove that $\bar{j}$ is an injection it is enough to show that an ideal $\mathscr{U}$ of A, is principal if $\hat{A}\mathscr{U}$ is principal. Let $\hat{A}\mathscr{U} = \hat{A}\alpha$, $\alpha \in \hat{A}$. Now $\frac{\mathscr{U}}{\mathscr{M}\mathscr{U}} \approx \frac{\hat{A}\mathscr{U}}{\hat{A}\mathscr{M}\mathscr{U}}$ is generated by a single element as an $\frac{A}{\mathscr{M}}$-module say by $x(\mod \mathscr{M}\mathscr{U})$, $x \in \mathscr{U}$. Then $\mathscr{U} = Ax + \mathscr{M}\mathscr{U}$. By Nakayama's-lemma $\mathscr{U} = Ax$ and the theorem is 24
proved. □

7 Applications of the theorem of Nagata

We recall that a ring A is called *graded* if $A = \sum_{n \in \mathbb{Z}} A_n$, A_n being abelian groups such that $A_p\, A_q \subset A_{p+q}$, for $p, q \in \mathbb{Z}$, and the sum being direct. An ideal of A is *graded* if it generated by homogeneous elements.

Proposition 7.1. *Let Λ be a graded Krull ring. Let $DH(A)$ denote the subgroup of $D(A)$ generated by graded prime divisorial ideals and let $FH(A)$ denote the subgroup of $DH(A)$ generated by principal ideals. Then the canonical mapping $\frac{DH(A)}{FH(A)} \to C(A)$, induced by the inclusion $i : DH(A) \to D(A)$, is an isomorphism.*

Proof. If $A = A_o$, there is nothing to prove. Hence we may assume $A \neq A_o$. Let S be the set of non-zero homogeneous elements of A. Then $S^{-1}A$ is again a graded ring; infact $S^{-1}A = \sum_{j \in \mathbb{Z}} (S^{-1}A)_j$, where $(S^{-1}A)_j = \{\frac{a}{b} \big| a, b \in A, a, b \text{ homogeneous}, d^o a - d^o b = j\}$. □

Here $d^o x$ denotes the degree of a homogeneous element $x \in A$. We note that $(S^{-1}A)_o = K$ is a field and that $S^{-1}A \approx K[t, t^{-1}]$, where t is a homogeneous element of smallest strictly positive degree. Now t is transcendental over K and therefore $S^{-1}A$ is factorial. Hence $C(A) \approx Ker(\overline{j})$, where $\overline{j}$ is the canonical homomorphism $\overline{j} : C(A) \to C(S^{-1}A)$, and $C(S^{-1}A) = 0$.

Hence $C(A) \approx \dfrac{H}{(H \cap F(A))}$, where H is the subgroup of $D(A)$, gen-
25 erated by prime ideals $\mathscr{Y}$ of height 1 with $\mathscr{Y} \cap S \neq \phi$. Since $DH(A) \cap F(A) = FH(A)$, and since prime divisorial ideals are of height 1, the proposition is a consequence of the following

Lemma 7.2. *Let $A = \sum\limits_{n \in \mathbb{Z}} A_n$ be a graded ring and $\mathscr{Y}$ a prime ideal in A and let $\mathscr{U}$ be the ideal generated by homogeneous elements of $\mathscr{Y}$. Then $\mathscr{U}$ is a prime ideal.*

Proof. Let $xy \in \mathscr{U}$, $x = \sum x_i$, $y = \sum y_i$, $x \notin \mathscr{U}$, $y \notin \mathscr{U}$. Let $x_{i_o} y_{j_o}$ be the lowest components of x, y such that $x_{i_o} \notin \mathscr{U}$, $y_{j_o} \notin \mathscr{U}$. Then $x_{i_o} y_{j_o} \in \mathscr{U} \subset \mathscr{Y}$. Since $\mathscr{Y}$ is prime, x_{i_o} or $y_{j_o} \in \mathscr{Y}$, say $x_{i_o} \in \mathscr{Y}$. Then $x_{i_o} \in \mathscr{U}$, a contradiction. □

Corollary. *Let $A = \sum\limits_{n \in \mathbb{Z}} A_n$ be a graded ring and $\mathscr{Y}$ a prime ideal of height 1. Then $\mathscr{Y}$ is graded if and only if $\mathscr{Y} \cap S \neq \phi$.*

Remark. If $\mathscr{U}$ is a graded ideal of A, then the least divisorial ideal $A : (A : \mathscr{U})$ containing $\mathscr{U}$ is also graded (straight forward proof). Thus the divisors corresponding to graded divisorial ideals of A form a subgroup of $D(A)$; this subgroup obviously contains $DH(A)$; furthermore, since, given a graded integral divisorial ideal $\mathscr{U}$, all the prime divisorial ideals containing $\mathscr{U}$ are graded (by the corollary), we see that this subgroup is in fact $DH(A)$.

The above proposition can be applied for instance to the homogeneous coordinate ring of a projective variety. The following proposition connects the divisor class group of a projective variety V with the divisor class group of a suitable affine open subset of V.

26 **Proposition 7.3.** *Let A be a graded Krull ring and p a prime homogeneous element $\neq 0$ with $d^o p = 1$. Let A' be the subring of K (quotient field of A) generated by A_o and $\dfrac{a}{p^{d^o a}}$, where a runs over the non-zero homogeneous elements of A. Then $C(A') \approx C(A)$.*

Proof. We note that $A' = (S^{-1}A)_o$ and that p is transcendental over A'. The inclusions $A' \to A'[p] \to A'[p, p^{-1}]$ induce isomorphisms $C(A') \approx C(A'[p]), C(A'[p]) \approx C(A'[p, p^{-1}])$, the first isomorphism follows from Theorem 6.4 and the second from Theorem 6.3. Now $A[p^{-1}] = A'[p, p^{-1}]$. But again by Theorem 6.3, $C(A) \approx C(A[p^{-1}])$ and the proof of the proposition is complete. □

Let V be an arithmetically normal projective variety. We prove that the homogeneous coordinate ring of V is factorial if and only if the local ring of the vertex of the projecting cone is factorial; in fact we have the following

Proposition 7.4. *Let $A = A_o + A_1 + A_2 + \cdots$ be a graded Krull ring and suppose that A_o is a field. Let $\mathscr{M}$ be the maximal ideal $A_1 + A_2 + \cdots$. Then $C(A) \approx C(A_{\mathscr{M}})$.*

Proof. We have only to prove that $\bar{j} : C(A) \to C(A_{\mathscr{M}})$ is injective. Because of Proposition 7.1 and of the remark following it is sufficient to prove that if $\mathscr{V}$ is a graded divisorial ideal such that $\mathscr{V} A_{\mathscr{M}}$ is principal, then so is $\mathscr{V}$. Suppose that $\mathscr{V}$ is a graded divisorial ideal with $\mathscr{V} A_{\mathscr{M}}$ principal. Since $A_{\mathscr{M}}$ is a local ring, there is a homogeneous element $u \in \mathscr{V}$ such that $\mathscr{V} A_{\mathscr{M}} = uA_{\mathscr{M}}$. Let $x \in \mathscr{V}$ be any homogeneous element. Then $x = \dfrac{y}{z}u$, $y \in A$, $z \in A - \mathscr{M}$. Let

$$y = y_q + y_{q+1} + \cdots, z = z_o + z_1 + z_2 + \cdots, y_i \in A_i, i \geq q, y_q \neq 0,$$
$$z_j \in A_j, z_o \neq 0. \text{ Thus } x(z_o + z_1 + z_2 + \cdots) = (y_q + y_{q+1} + \cdots)u.$$

27

Hence $xz_o = y_q u$. Since z_o is invertible, we conclude that $\mathscr{V} = An$ and the proposition is proved. □

Adjunction of indeterminates.

Let A be a local ring and $\mathscr{M}$ its maximal ideal. We set $A(X)_{\text{loc}} = A[X]_{\mathscr{M}A[X]}$ and by induction $A(X_1, \ldots, X_n)_{\text{loc}} = A(X_1, \ldots, X_{n-1})_{\text{loc}} (X_n)_{\text{loc}}$. We remark that $A(X)_{\text{loc}}$ is a local ring and that if A is noetherian, properties of A like its dimension, multiplicity, regularity and so on are preserved in passing from A to $A(X)_{\text{loc}}$. Further $A(X)_{\text{loc}}$ is A-flat (in fact it is faithfully flat).

Proposition 7.5. *Let A be a local Krull ring. Then*

$$\bar{j} : C(A) \to C(A(X_1, \ldots, X_n)_{\text{loc}})$$

is an isomorphism.

Proof. It is sufficient to prove this when $n = 1$. Since by Theorem 6.5 $C(A) \approx C(A[X])$, we see that $\bar{j}$ is surjective. Let $\mathscr{V}$ be a divisorial ideal of A for which $\mathscr{V} A(X)_{\text{loc}}$ is principal. Since $A(X)_{\text{loc}}$ is a local ring, we may assume that $\mathscr{V} A(X)_{\text{loc}} = A(X)_{\text{loc}}\alpha$, $\alpha \in \mathscr{V}$. Let $y \in \mathscr{V}$. Then $y = \dfrac{f(X)}{g(X)}.\alpha$, where $f(X)$, $g(X) \in A[X]$ and atleast one of the coefficients of $g(X)$ is invertible in A. Looking at a suitable power of X in $y.g(X) = \alpha f(X)$ we see that $y \in A\alpha$ i.e. $\mathscr{V} = A\alpha$. Hence $\bar{j}$ is injective. This proves the proposition. ◻

28 **Proposition 7.6.** *Let A be a domain and a, b ∈ A with $Aa \cap Ab = Aab$.*

The following results hold.

(a) The element $aX - b$ is prime in $A[X]$.

(b) If further, we assume that A is a noetherian integrally closed domain and that Aa and $Aa + Ab$ are prime ideals, then the ring $A' = \dfrac{A[X]}{(aX - b)}$ is again integrally closed and the groups $C(A)$ and $C(A')$ are canonically isomorphic.

Proof. (a) Consider the A-homomorphism $\varphi : A[X] \to A[\frac{b}{a}]$ given by $\varphi(X) = \frac{b}{a}$. It is clear that the ideal $(aX - b) \subset \text{Ker}(\varphi)$. Conversely we show by induction on the degree that if a polynomial $P(X) \in \text{Ker}(\varphi)$, then $P(X) \in (aX - b)$. This is evident if

$d^o(P) = 0$. If $P(X) = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_o (n > 0)$, the relation $P(\frac{b}{a}) = 0$, shows that $b^n c_n \in Aa$. Since $Aa \cap Ab = Aab$, it follows that $c_n \in Aa$, say $c_n = d_n a$, $d_n \in A$. Then the polynomial $P_1(X) = P(X) - d_n(aX - b)X^{n-1} \in \operatorname{Ker}(\varphi)$ and has degree $\leq n - 1$. By induction we have $P_1(X) \in (aX - b)$ and hence $P(X) \in (aX - b)$. Thus $(aX - b) = \operatorname{Ker}(\varphi)$ and (a) is proved.

1. We note that $A' \approx A[\frac{b}{a}] \subset A[\frac{1}{a}]$ and $A[\frac{1}{a}] \approx A'[\frac{1}{a}]$. By Theorem 6.3, the proof of (b) will be complete if we show that a is a prime element in A'. But

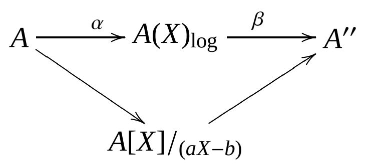
$$\frac{A'}{A'a} \approx \frac{A[X]}{(a, aX - b)} = \frac{A[X]}{(a, b)} \approx \frac{A}{(a, b)}[X].$$

□

By assumption (a, b) is a prime ideal and therefore a is a prime element in A'. 29

Remark 1. In (b), if a, b are contained in the radical of A, and if the ideal $Aa + Ab$ is prime, then a and b are prime elements (for proof see *P*. Samuel: Sur les anneaux factoriels, Bull. Soc. math. France, 89 (1961), 155-173).

Remark 2. Let A be a noetherian integrally closed local domain and let the elements a, $b \in A$ satisfy the hypothesis of the above proposition. Set $A'' =^{A(X)}$ loc $/(aX - b)$. Then it follows from (a) that A'' is a Krull ring. We have a commutative diagram



Since A'' is a ring of quotients of $A[X]/_{(aX-b)}$, it follows from (b) that $\beta o \alpha$ induces a surjective mapping $\varphi : C(A) \to C(A'')$. We do not know if φ is an isomorphism. If φ is an isomorphism we can get another proof of the fact that a regular local ring is factorial (see P. Samuel : Sur les anneaux factoriels, Bull. Soc. math. France, t.89, 1961).

Proposition 7.7 (C.P. Ramanujam)**.** *Let A be a noetherian analytically normal local ring and let $\mathscr{M}$ be its maximal ideal. Let $B = A\big[[X_1, \ldots, X_n]\big]$. Then the canonical mapping $j : C(B) \to C(M_{\mathscr{M}B})$ is an isomorphism.*

Proof. By Theorem 6.3 (a), $\overline{j}$ is surjective and $\mathrm{Ker}(j) = (H + F(B))/F(B)$, where H is the subgroup of $D(B)$ generated by prime ideals $\mathscr{Y}$ of height one in B with $\mathscr{Y} \not\subset \mathscr{M}B$ and $F(B)$ is the group of principal
30 ideals. Thus we have only to prove that if $\mathscr{Y}$ is a prime ideal of height one of B with $\mathscr{Y} \not\subset \mathscr{M}B$, the then $\mathscr{Y}$ is principal. This, we prove in two steps.

(i) Assume that A is complete. Let $\mathscr{Y}$ be a prime ideal of height one with $\mathscr{Y} \not\subset \mathscr{M}B$. It is clear that $\mathscr{Y}$ is generated by a finite number of elements $f_j \in \mathscr{Y}$ such that $f_j \notin \mathscr{M}B$. Set $R = A\big[[X_1, \ldots, X_{n-1}]\big]$ and let $\mathscr{M}(R)$ denote the maximal ideal of R. We claim that any $f \in B - \mathscr{M}B$ is an associate of a polynomial $g(X_n) = X_n^q + a_{q-1}X_n^{q-1} + \cdots + a_o$, $a_i \in \mathscr{M}(R)$. To prove this we first remark that by applying an A-automorphism of B given by $X_i \rightsquigarrow X_i + X_n^{t(i)}, t = 1, \ldots, n-1, X_n \rightsquigarrow X_n$ with $t(i)$ suitably chosen, we may assume that the series f_j are regular in X_n, (for details apply Zariski and P.Samuel : Commutative algebra p.147, Lemma 3 to the product of the $f_j's$). Now since the Weierstrass Preparation Theorem is valid for the ring of formal power series over a complete local ring, it follows that $f = u(X_n^q + a_{q-1}X_n^{q-1} + \cdots + a_o)$, u invertible in $B = R\big[[X_n]\big]$, $a_i \in \mathscr{M}(R)$ and q being the order of $f \mod \mathscr{M}(R)$. Thus $\mathscr{Y}$ is generated by $\sigma = \mathscr{Y} \cap R[X_n]$. Now, since B is $R[X_n]$ - flat it follows by Theorem 6.2, (2), that σ is divisorial. Now by Proposition 7.5 $C(R[X_n]) \to C(R(X_n)_{\mathrm{loc}})$ is an isomorphism. Since $\sigma \not\subset \mathscr{M}(R)\, R[X_n]$, it follows that σ is principal. Hence $\mathscr{Y}$ is principal.

(ii) Now we shall deal with the case in which A is not complete. The completion $\hat{B}$ of B is the ring $\hat{A}\big[[Y_1, \ldots, Y_n]\big]$. Let $\mathscr{Y}$ be a minimal prime ideal of B, with $\mathscr{Y} \not\subset \mathscr{M}_B$. Since $\hat{B}$ is B-flat, the ideal $\mathscr{Y}\hat{B}$ is divisorial. Furthermore, since $\mathscr{Y} \not\subset \mathscr{M}B$, all the components k of $\mathscr{Y}\hat{B}$ are such that $k \not\subset \mathscr{M}\hat{B}$, and therefore principal by (i). Thus $\mathscr{Y}\hat{B}$ is principal. Hence $\mathscr{Y}$ is principal by Theorem 6.6. **31**

□

8 Examples of factorial rings

Theorem 8.1. *Let A be a factorial ring. Let $A[X_1, \dots, X_n]$ be graded by assigning weights ω_i to x_i ($\omega_i > 0$). Let $F(X_1, \dots, X_n)$ be an irreducible isobaric polynomial. Let c be a positive integer prime to ω, the weight of F. Set $B = A[X_1, \dots X_n, Z]/(Z^c - F(X_1, \dots, X_n)) = A[x_1, \dots, x_n, z]$, $z^c = F(x_1, \dots, x_n)$. Then B is factorial in the following two cases.*

(a) $c \equiv 1 (\mod \omega)$

(b) Every finitely generated projective A-module is free.

Proof. (a) Since $B_{/zB} \approx A[X_1, \dots, X_n, Z]/(Z^c - F, Z) \approx A[X_1, \dots, X_n]/(F)$, it follows that z is prime in B. Now, set $x_i = z^{d\omega_i} x_i'$, where $c = 1 + d\omega$. Then $z^c = F(x_1, \dots, x_n) = z^{c-1} F(x_1', \dots, x_n')$, i.e. $z = F(x_1', \dots, x_n')$ so that $B[z^{-1}] = A[x_1', \dots, x_n', F(x_1', \dots, x_n')^{-1}]$. Since $x_1', \dots, x_n'$ are algebraically independent over A, we see that $B[z^{-1}]$ is factorial. Now $B = B[z^{-1}] \cap K[x_1, \dots, x_n, z]$, where K is the quotient field of Aj for, let $\dfrac{y}{z^r} \in K[x_1, \dots, x_n, z]$ with $y \in B$. Then since (z^r) is a primary ideal not intersecting A, we have $y \in Bz^r = B \cap K[x_1, \dots, x_n, z]z^r$. Hence B is a Krull ring and therefore factorial by Theorem 6.3.

(b) Since c is prime to ω, there exists a positive integer e such that $c\, e \equiv 1 (\mod \omega)$. Now by ($a$) $B' = A[x_1, \dots, x_n, u]$, with $u^{ce} = F(x_1, \dots, x_n)$ is factorial. Further $B' = B[u]$, $u^e = z$ and B' is a free B-module with $1, u, u^2, \dots, u^{e-1}$ as a basis. It follows that B is the intersection of B' and of the quotient field of B, and is therefore a **32** Krull ring. Now B can be graded by attaching a suitable weight to Z. Let $\mathscr{U}$ be a graded divisorial ideal. Since B' is factorial, $\mathscr{U}B'$ is principal. As B' is free over B, $\mathscr{U}$ is a projective B-module. Now by Nakayama's lemma for graded rings it follows that $\mathscr{U}$ is free and therefore principal. The proof of (b) is complete.

□

Examples. (1) Let a, b, c be positive integers which are pairwise relatively prime. Let A be a factorial ring. Then the ring $B = A[x, y, z]$, with $z^c = x^a + y^b$, is factorial.

(2) Let $\mathbb{R}$ denote the field of real numbers. Then the ring $B = \mathbb{R}[x, y, z]$ with $z^3 = x^2 + y^2$ is factorial.

Theorem 8.2 (Klein-Nagata)**.** *Let K be a field of characteristic $\neq 2$ and $A = K[x_1, \ldots, x_n]$ with $F(x_1, \ldots, x_n) = 0$, where F is a non-degenerate quadratic form and $n \geq 5$. Then A is factorial.*

Proof. Extending the ground field K to a suitable quadratic extension K' if necessary, the quadratic form $F(X_1, \ldots, X_n)$ can be transformed into $X_1\ X_2 - G(X_3, \ldots, X_n)$. Let $A' = K' \underset{K}{\otimes} A = K'[x_1, \ldots, x_n]$, $x_1 x_2 = G(x_3, \ldots, x_n)$. Since F is non-degenerate and $n \geq 5$, $G(X_3, \ldots, X_n)$ is irreducible and therefore x_l is a prime element in A'. Now $A'[\frac{1}{x_1}] = K'[x_1, x_3, \ldots, x_n, \frac{1}{x_1}]$. □

Since $x_1, x_3, \ldots, x_n$ are algebraically independent, it follows from Theorem 6.3 that A' is factorial. Now as A' is A-free, for any graded divisorial ideal $\mathscr{U}$ of A, $\mathscr{U}A'$ is divisorial and hence principal. Therefore $\mathscr{U}$ is a projective ideal. Since a finitely generated graded projective module is
33 free over A, we conclude that $\mathscr{U}$ is principal. Thus A is factorial.

Remark 1. The above theorem is not true for $n \leq 4$. For instance, $A = K[x_1, x_2, x_3, x_4]$ with $x_1 x_2 = x_3 x_4$ is evidently not factorial.

Remark 2. We have proved that if A is a homogeneous coordinate ring over a field K such that $K' \bigotimes_K A$ is factorial for some ground field extension K' of K, then A is factorial. This is not true for affine coordinate rings (see the study of plane conics later in this section).

Remark 3. The above theorem is a particular case of theorems of Severi, Lefshetz and Andreotti, which in turn are particular cases of the following general theorem proved by Grothendieck.

Theorem. (Grothendieck). *Let R be a local domain which is a complete intersection such that* $R_{\mathscr{Y}}$ *is factorial for every prime ideal* $\mathscr{Y}$ *with height* $\mathscr{Y} \leq 3$. *Then R is factorial.*

(We recall that R is a complete intersection if $R = A/\mathscr{U}$, where A is a regular local ring and $\mathscr{U}$ an ideal generated by an A-sequence). (For proof of the above theorem see Grothendieck: Seminaire de Geometric algebrique, exposé XI, IHES (Paris), 1961-62).

Study of plane conics. Let C be a projective non singular curve over a ground field K. Let A be the homogeneous coordinate ring of C. The geometric divisors of C can be identified with elements of $D\,H(A)$. Then $FH(A) = G_1(C) + \mathbb{Z}h$, where $G_l(C)$ denotes set of divisors of C linearly equivalent to zero and h denotes a hyper plane section. Let now C be a conic in the projective plane P^2. Since the genus of C is zero we have $G_l(C) = G_o(C)$ where $G_o(C)$ is the set of divisors of degree zero of C. 34 (i.e. its Jacobian variety is zero). Let d denote the homomorphism of $DH(A)$ into $\mathbb{Z}$ given by $d(\mathscr{U}) =$ degree of $\mathscr{U}$, for $\mathscr{U} \in DH(A)$. Then $d^{-1}(2\mathbb{Z}) = G_o(C) + \mathbb{Z}h = G_l(C) + \mathbb{Z}h = FH(A)$. Hence $C(A) \approx Imd_{/2\mathbb{Z}}$. Thus A is factorial if and only if $Imd = 2\mathbb{Z}$.

Suppose C does not carry any K-rational points. Then A is factorial. For if not, $C(A) \approx \mathbb{Z}/(2)$ and there exists a divisor $\mathscr{U} \in DH(A)$ with $d(\mathscr{U}) = 1$. By the Riemann-Roch Theorem, we have $l(\mathscr{U}) \geq d(\mathscr{U}) - g + 1 = 2$, where $l(\mathscr{U})$ denotes the dimension of the vector space of functions f on C with $(f) + \mathscr{U} \geq 0$. Thus there exists a function f on C with $(f) + \mathscr{U} \geq 0$ and thus we obtain a positive divisor of degree 1, i.e. C carries a rational point: Contradiction. Conversely if C carries a rational point P, then P is a divisor of degree 1 and $C(A) \approx Z/(2)$ i.e. A is not factorial. Thus we have proved (a) The homogeneous coordinate ring A of C is factorial if and only if C does not have rational points over K.

Let now C' be a conic in the affine place over K. Let A' be its coordinate ring. Let C be its projective closure in P^2. Let I be the subgroup of $DH(A)$ generated by the divisors at infinity (A is the homogeneous coordinate ring of C). Then $C(A') \approx DH(A)/(FH(A) + I)$. Thus

(i) if C has no rational points over K, then by $(a)DH(A) = FH(A)$ and therefore $C(A') = 0$, so that A' is factorial;

(ii) if C has rational points over K at infinity, then $DH(A) = FH(A) + I$ and A' is factorial;

35 (iii) if C has rational points, but not at infinity, then $I \subset FH(A)$ and $C(A') \approx C(A) \approx \mathbb{Z}_{/(2)}$; in this case A is not factorial.

Examples. (i) $C' \equiv x^2 + 2y^2 + 1 = 0$ over the rationals. Then A' is factorial. However the coordinate ring of C' over $\mathbb{Q}(i)$ is not factorial.

(ii) $C' \equiv x^2 + y^2 - 1 = 0$. The coordinate ring of C' over $\mathbb{Q}$ is not factorial. But the coordinate ring of C' over $\mathbb{Q}(i)$ is factorial.

The above examples show that unique factorization is preserved neither by ground field extension nor by ground field restriction.

Study of the real sphere. Let $\mathbb{R}$ denote the field of real numbers and $\mathbb{C}$, the field of complex numbers. We shall consider the coordinate ring of the sphere $X^2 + Y^2 + Z^2 = 1$ over $\mathbb{R}$ and $\mathbb{C}$.

Proposition 8.3. *(a) The ring $A = \mathbb{R}[x, y, z]$, $x^2 + y^2 + z^2 = 1$ is factorial*

(b) The ring $A = \mathbb{C}[x, y, z]$, $x^2 + y^2 + z^2 = 1$ is not factorial.

Proof. (a) We have $A/(z - 1) \approx \mathbb{R}[X, Y, Z]/(Z - 1, X^2 + Y^2 + Z^2 - 1)$

$$\mathbb{R}[X, Y, Z]/(X^3 + Y^2, Z - 1) \approx \mathbb{R}[X, Y]/(X^2 + Y^2).$$

Hence $Z - 1$ is prime in A. Set $t = \dfrac{1}{z - 1}$, so that $z = 1 + \dfrac{1}{t}$. Now, since $x^2 + y^2 + z^2 - 1 = 0$, we have $x^2 + y^2 + 1 + \dfrac{1}{t^2} + \dfrac{2}{t} - 1 = 0$ i.e. $(tx)^2 + (ty)^2 = -2t - 1$ i.e. $t \in \mathbb{R}[tx, ty]$. Now $A[t] = \mathbb{R}[tx, ty, \dfrac{1}{t}]$ is factorial. Hence by Theorem 6.3, A is factorial.

(b) Since $(x+iy)(x-iy) = (z+1)(z-1)$, we conclude that $A = \mathbb{C}[x,y,z]$, $x^2+y^2+z^2 = 1$ is not factorial.

□

Let K denote the field of complex numbers or the field of reals, and 36
$A = K\ x,y,z,\ x^2+y^2+z^2 = 1$. Let M be the module $M = Adx+Ady+Adz$, with the relation $xdx+ydy+zdz = 0$.

Proposition 8.4. *The A-module M is projective*

(a) If $K = \mathbb{R}$, then M is not free

(b) If $K = \mathbb{C}$, then M is free.

Proof. Since the elements $v_1 = (0,z,-y)$, $v_2 = (-z,0,x)$, $v_3 = (y,-x,0)$ of A^3 satisfy the relation $xv_1+yv_2+zv_3 = 0$, we have a homomorphism $u : M \to A^3$, given by $u(dx) = v_1$, $u(dy) = v_2$, $u(dz) = v_3$. Let v be the homomorphism $v : A^3 \to M$ given by $v(a,b,c) = a(ydz-zdy) + b(zdx-xdz) + c(xdy-ydx)$. It is easy to verify that vou is the identity on M. Hence M can be identified with a direct summand of A^3. Hence M is projective. Now the linear form $\varphi : A^3 \to A$ given by $\varphi(a,b,c) = ax+by+cz$ is zero on M. But A^3/M is a tossion-free module of rank 1. Hence $M = \ker\varphi$. On the other hand we have $\varphi(A^3) = A$, since $x^2+y^2+z^2 = 1$. Hence $M \oplus A \approx A^3$. Thus M is equivalent to a free module. □

(a) If $K = \mathbb{R}$, then M is not free. We remark that M is the A-module of sections of the dual bundle of the targent bundle to the sphere S_2. Since there are no non-degenerate continuous vector fields on S_2, the tangent bundle is not trivial, nor is its dual.

(b) If $K = \mathbb{C}$, then M is free. For, the tangent bundle to the complexification of S_2 is trivial (this complexification being the product of two complex projective lines).

Remark. R.Swan (Trans, Amer. Math. Soc. 105(1962), 264-277(1962) 37
has proved the following. The ring $A = \mathbb{R}[x_1,x_2,\ldots,x_5]$, $\sum\limits_{i=0}^{5} x_i^2 = 1$ is

factorial. Now S_7 can be fibred by S_3, the base being S_4. Let V be the bundle of tangent vectors along the fibres for this fibration and M, the corresponding module. Then M is not free, where as $M \bigotimes_{\mathbb{R}} \mathbb{C}$ is free over $A \bigotimes_{\mathbb{R}} \mathbb{C}$. Further $A \bigotimes_{\mathbb{R}} \mathbb{C}$ is factorial. Moreover M is not equivalent to a free-module.

Grassmann varieties. Let E be a vector space of dimension n over a field K. Let $G = G_{n,q}$ be the set of all q dimensional subspaces of $E (q \leq n)$. Then set G can be provided with a structure of a projective variety as given below.

We call an element $x \in \overset{q}{\wedge} E$ a decomposed multi-vector if x is of the form $x_1 \wedge \cdots \wedge x_q$, $x_i \in E$. We have $x_1 \wedge \cdots \wedge x_q = 0$ if and only if $x_1, \ldots, x_q$ are linearly dependent. Further $x_1 \wedge \cdots \wedge x_q = \lambda y_1 \wedge \cdots \wedge y_q$, $\lambda \in K^*$ if and only if $x_1, \ldots, x_q$ and $y_1, \ldots, y_q$ generate the same subspace. In the set of all decomposed multivectors we introduce the equivalence relation $x_1 \wedge \cdots x_q \sim y_1 \wedge \cdots \wedge y_q$ if $x_1 \wedge \cdots \wedge x_q = \lambda y_1 \cdots y_q$ for some $\lambda \in K^*$. Then the set $G_{n,q}$ can be identified with the quotient set which is a subset of $P(\overset{q}{\wedge} E)$ the $\binom{n}{q} - 1$ dimensional projective space defined by the vector space $\overset{q}{\wedge} E$. It can be shown that with this identification, $G_{n,q}$ is a closed subset of $P(\overset{q}{\wedge} E)$ in the Zariski topology). The projective variety $G_{n,q}$ is known as the Grassmann variety. As $GL(n, K)$ acts transitively on $G_{n,q}$, it is non-singular.

38 Let L be a generic q-dimensional subspace of E with a basis $x_1, \ldots x_q$, say $x_i = \sum\limits_{j=1}^{n} \lambda_{ij} e_j$, $1 \leq i \leq q$, $\lambda_{ij} \in K$. Then

$$x_1 \wedge \cdots \wedge x_q = \sum_{i_1 \cdots i_q} d_{i_1, \ldots, i_q}(\lambda) e_{i_1} \wedge \cdots \wedge e_{i_q},$$

where $d_{i_1, \ldots, i_q} = \det(\lambda_{k i_j})$. Let x_{ij}, $1 \leq i \leq q$, $1 \leq j \leq n$ be algebraically independent elements over K. Let $B = K[x_{ij}]_{\substack{1 \leq i \leq q \\ 1 \leq j \leq n}}$ the polynomial ring in nq variables. For any subset $H = \{i_1, \ldots, i_q\}$, $i_1 < i_2 < \cdots < i_q$ of cardinality q, we denote by $d_H(x)$ the q by q determinant $\det(x_{k i_j})$. It is clear that $A = K[d_H(x)]'_{H\in J}$ where J is the set of all subsets of cardinality q of $\{i, \ldots, n\}$, is the homogeneous coordinate ring of $G_{n,q}$.

Proposition 8.5. *The ring A is factorial.*

Proof. It is known that the ring A is normal (See J. Igusa: On the arithmetic normality of Grassmann variety, Proc. Nat. Acad. Sci. U.S.A. Vol. 40, 309 - 313). Consider the element $d = d_{\{1,\ldots,q\}}(x) \in A$. We first prove that d is prime in A. Consider the subvariety S of $G_{n,q}$ defined by $d = 0$. Let E' be the subspace generated by $e_1, \ldots, e_q$ and E'' the subspace generated by $e_{q+1}, \ldots, e_n$. (We recall that $e_1, \ldots, e_n$ is a basis of E). Now $\alpha \in S$ if and only if $\dim(pr_{E'}(\alpha)) < q$, i.e. if and only if $\alpha \cap E'' \neq (0)$. Let $Z = (0, \ldots, 0, Z_{q+1}, \ldots, Z_n)$, where the Z_i are algebraically independent. Let $x_1, \ldots, x_{q-1}$ be independent generic points of E, independent over $k(z)$. Then $Z \wedge x_1 \wedge \cdots \wedge x_{q-1}$ is a generic 39
point of S, and therefore S is irreducible. Let $\mathscr{Y}$ be the prime ideal defining S. Then $A.d = \mathscr{Y}^{(s)}$ for some s. We now look at the zeros of $A.d$ which are singular points. These zeros are given by the equations $\dfrac{\partial}{x_{it}}(d) = 0$, $1 \leq i \leq q$, $1 \leq t \leq n$, or equivalently, by equating to 0 the sub-determinants of d of order $q - 1$. Hence α is a singular zero of $A.d$ if and only if $pr'_E(\alpha)$ has codimension ≥ 2 i.e. if and only if $\dim(\alpha \cap E'') \geq 2$. Hence $A.d$ has at least one simple zero. That is, $s = 1$ and $A.d$ is a prime. □

The co-ordinate ring of the affine open set U defined by $d \neq 0$ is the ring $A' = \left\{ \dfrac{a}{d^{d^o(a)/q}} \middle| a \in A, \text{ a homogeneous} \right\} = A_{/(1-d)}$. We shall describe the ring A' in another way. Let $\alpha \in G_{n,q}$. Then $\alpha \in U \Leftrightarrow \alpha \cap E'' = (0)$. Let $y_1 = (1, 0, \ldots, 0, y_{1q+1}, \ldots y_{1n}), \ldots, y_q = (0, \ldots, 1, y_{q,q+1}, \ldots, y_{qn})$, where the y_{ij} are algebraically independent over K. Then $y_1 \wedge \cdots \wedge y_q$ is a generic point of U. Set $y = (y_{ij})_{\substack{1\leq i\leq q\\ 1\leq j\leq n}}$ where $y_{ij} = \delta_{ij}$, $i \leq q$, $j \leq q$. Then $A' = K[d_H(y)]_{H\in J}$. But $d_{1,\ldots,i,\ldots,q,j}(y) = \pm y_{ij}$, $1 \leq i \leq q$, $q + 1 \leq j \leq n$. Hence $A' = K[y_{ij}]_{\substack{1\leq i\leq q,\\ q+1\leq j\leq n}}$. Hence A' is factorial. Hence, by Proposition 7.3, the ring A is factorial.

Remark 1. The ring A provides an example of a factorial ring which is not a complete intersection.

40 **Remark 2.** We do not know any example of a factorial ring which is not a Cohen-Macaulay ring.

Remark 3. We do not know any example of a factorial ring which is not a Gorenstein ring.

A local ring A is said to be a *Gorenstein ring* if A is Cohen-macaulay and every ideal generated by a system of parameters is irreducible.

9 Power series over factorial rings

Theorem 9.1. *Let A be a noetherian domain containing elements x, y, z satisfying*

(i) y is prime, $Ax \cap Ay = Axy$;

(ii) $z^{i-1} \notin Ax + Ay$, $z^i \in Ax^j + Ay^k$, where i, j, k are integers such $ijk - ij - jk - ki \geq 0$.

Then $A[[T]]$ *is not factorial*.

We first list here certain interesting corollaries of the above theorem.

Corollary 1. *There exist factorial rings A (also local factorial ones) such that $A[[T]]$ is not factorial. Let k be a field and let $A' = k[x, y, z]$ with $z^i = x^j + y^k$, $(i, j, k) = 1$, $ijk - ij - jk - ki \geq 0$ (for instance $i = 2$, $j = 5$, $k = 7$). Then by Theorem 8.1 the ring A' is factorial, and so is the local ring $A = A'_{(x,y,z)}$. But x, y, z satisfy the hypothesis of the above theorem. Therefore $A'[[T]]$ and $A[[T]]$ are not factorial.*

41 **Corollary 2.** *There exists a local factorial ring B such that its completion $\hat{B}$ is not factorial. Set $A = A'_{(x,y,z)}$, $B = A[T]_{(\mathscr{M},T)}$, where A' is as in the proof of Corollary 1 and $\mathscr{M}$ is the maximal ideal of A. Then $\hat{B}$ is factorial. Now $\hat{B} = \hat{A}[[T]]$. Further $\hat{B}$ is also the completion of the local ring $A[[T]]$. Thus if $\hat{B}$ is factorial, so is $A[[T]]$ by Mori's Theorem*

(see for instance, Sur les anneaux factorials, Bull. Soc. Math. France, 89, (1961), 155 - 173). Contradiction.

Corollary 3. *There exists a local non-factorial ring B such that its associated graded ring $G(B)$ is factorial.*

We set $A_1 = k[u, v, x, y, z]$, $z^7 = u^5 x^2 + v^4 y^3$. We observe that z is prime in A_1 and that $A_1[\frac{1}{z}] = k[x', y', u, v, \frac{1}{z}]$, $x = z^3 x'$, $y = z^2 y'$, $z = u^5 x'^2 + v^4 y^3$. Hence $A_1[\frac{1}{z}]$ is factorial and therefore is A_1. Take $A = A_{1_{(u,v,x,y,z)}}$, $B = A[[T]]$. Since x, y, z A satisfy the hypothesis of the above theorem with $i = 7$, $j = 2$, $k = 3$, the ring $B = A[[T]]$ is not factorial. But $G(B) = G(A)[T] = A_1[T]$ is factorial.

Remark. 1. If A is a regular factorial ring, then so is $A[[T]]$. (see Chapter 2, Theorem 2.1).

2. If A is a noetherian factorial ring such that $A_{\mathscr{M}}[[T]]$ is factorial for every maximal ideal $\mathscr{M}$ of A, then $A[[T]]$ is factorial.

3. Suppose that A is a factorial Macaulay ring such that $A_{\mathscr{Y}}[[T]]$ is factorial for all prime ideals $\mathscr{Y}$ with height $\mathscr{Y} = 2$. Then $A[[T]]$ is factorial (for proofs of (2) and (3), see P. Samuol, on unique factorization domains, Illinois J.Math. 5(1961) 1-17).

4. **Open question**. Let A be a *complete* local ring which is factorial. **42**
   Then is $A[[T]]$ factorial?

In Chapter 3 we shall see that at least in characteristic 2, the completion $\hat{A}$ of A of Corrolary 2 is not factorial. We shall also give examples to show that $C(A) \to C(A[[T]])$ is not surjective. Finally it may be of interest to note that J. Geiser has proved that there do not exist *complete* factorial rings satisfying the hypothesis of Theorem 9.1.

Proof of Theorem 9.1. Let S denote the multiplicatively closed set $1, x, x^2, \ldots$. Set $A' = S^{-1}A$, $B = A[[T]]$. Then $S^{-1}B \subset A'[[T]]$; in fact $A'[[T]]$ is the T-adic completion of $S^{-1}B$. But, however, $S^{-1}B$ is not a Zariski ring with the T-adic topology. Let S' denote the set of elements of B, whose constant coefficients are in S. Then $S'^{-1}B$ is a Zariski ring with the T-adic topology and its completion is $A'[[T]]$. Consider the element $v = xy - z^{i-1}T \in B$.

(a) No power series $y + a_1T + a_2T^2 + \cdots B$ is an associate of $v = xy - z^{i-1}T$ in $A'\ T$ (nor, a fortiori in $S'^{-1}B$).

Proof. If possible, suppose that $(xy - z^{i-1}T)\ (\dfrac{1}{x} + \dfrac{c}{x^{\alpha}}T + \cdots) \in B$, with $\dfrac{1}{x} + \dfrac{c}{x^{\alpha}}T + \cdots \in A'[[T]]$. Then $\dfrac{cy}{x^{\alpha-1}} - \dfrac{z^{i-1}}{x} \in A$ i.e $cy - z^{i-1}x^{\alpha-2} \in Ax^{\alpha-1}$. Since $z^{i-1} \notin Ax + Ay$ we have $\alpha \geq 2$. Further since $Ax \cap Ay = Axy$ we have $c \in Ax^{\alpha-2}$, say $c = c'x^{\alpha-2}$. Then $z^{i-1} - c'y \in Ax$. Contradiction

(b) There exists an integer t and an element $v' = \dfrac{y^t}{x} + \dfrac{b_1}{x^2}T + \cdots + \dfrac{b_n}{x^{n+1}}T^{n+1} + \cdots$ such that $u = vv' \in B$, where $v = xy - z^{i-1}T$.

□

Proof. Take $t \geq ij$. We have to find elements $b_1,\ b_2, \ldots b_n, \ldots$ of A such that

$$\frac{b_n}{x^{n+1}}xy - \frac{b_{n-1}}{x^n}z^{i-1} \in A \text{ i.e. } b_ny - b_{n-1}z^{i-1} \in Ax^n$$

43 for $n \geq 1$. We set $b_0 = y^t$. Assume that the b_l for $l \leq nij$ have been determined and that $b_{nij} = y^{t(n)}F_n(x^j, y^k)$, where $t(n) \geq ij$ and $F_n(X, Y)$ is a form of degree ni. This is trivially verified for $n = 0$. □

The congruence $b_{nij+1}y - b_{nij}z^{i-1} \in Ax^{nij+1}$ may be solved by taking $b_{nij+1} = y^{t(n)-1}F_n(x^j, y^k)z^{i-1}$. Similarly
$b_{nij+r} = y^{t(n)-r}F_n(x^j, y^k)z^{r(i-1)}$, $0 \leq r < ij$. Further the relation

$$b_{(n+1)ij}y - b_{nij+ij-1}z^{i-1} \in Ax^{(n+1)ij}$$

implies that

$$b_{(n+1)ij}y - y^{t(n)-ij+1}F_n(x^j, y^k)Z^{ij(i-1)} \in Ax^{(n+1)ij}.$$

But $z^i \in Ax^j + Ay^k$, say $z^i = cx^j + dy^k$. Now we have to solve the congruence, $b_{(n+1)ij} \equiv y^{t(n)-ij+1}G(\mod Ax^{(n+1)ij})$ where $G = (cx^j + dy^k)^{j(i-1)}F_n(x^j, y^k)$. The form $G(X, Y) = (cX + dY)^{j(i-1)}F_n(X, Y)$ is of degree $ni + (i-1)j$. The monomials in $G(x^j, y^k)$ are of the form $x^{j\alpha}y^{k\beta}$, $\alpha + \beta = ni + (i-1)j$. By reading modulo $Ax^{(n+1)ij}$ we can 'neglect' the terms for which $j\alpha \geq (n+1)ij$ i.e. $\alpha \geq (n+1)i$. For the remaining terms we have $\beta > ni + (i-1)j - (n+1)i = ij - j - i$. Thus $G(x^j, y^k) \equiv y^{(ij-j-i)k}F_{n+1}(x^j, y^k)(\mod Ax^{(n+1)ij})$, where F_{n+1} is a form of degree $ni + (i-1)j - (ij - j - i) = (n+1)i$. Now $b_{(n+1)ij}y \equiv y^{t(n)+(ijk-jk-ki-ij)+1}F_{n+1}(x^j, y^k)\ (\mod Ax^{(n+1)ij})$. We may solve this by taking $b_{(n+1)ij} = y^{t(n)+ijk-jk-ki-ij}F_{n+1}(x^j, y^k)$, i.e. we may take $t(n+1) = t(n) + ijk - jk - ki - ij$ and (b) is proved.

(c) B is not factorial. Suppose that, in fact, B were factorial. **44**

Set $u = vv'$, with v, v' as in (b). Let $u = u_1, \ldots u_s$ be the decomposition of u into prime factors in B; since the constant term of u is a power of y and since y is prime, the constant term of each u_l is a power of y. Consider $R = S'^{-1}B; R$ is factorial. Now $v' \in \hat{R}$ and therefore $u\ R\ Rv = Rv$. Further v is prime in R (since the constant term of v is y times an invertible element in $S^{-1}A$). Now unique factorization in R implies that v is an associate of some u_j in R. This contradicts (a).

Chapter 2

Regular rings

Let A be a noetherian local ring and $\mathscr{M}$ its maximal ideal. We say 45
that A is *regular* if $\mathscr{M}$ is generated by an A-sequence. We recall that $x_1, \ldots, x_r \in A$ is an A-sequence if, for $i = 0, \ldots, r-1$, x_{i+1} is not a zero divisor in $A/(x_1, \ldots, x_i)$. It can be proved that a regular local ring is a normal domain. Let A be a noetherian domain. We say that A is regular if $A_{\mathscr{M}}$ is regular for every maximal ideal $\mathscr{M}$ of A.

1 Regular local rings

Let A be a noetherian local ring and $\mathscr{M}$ its maximal ideal. Let E be a finitely generated module over A. Let $x_1, \ldots, x_n \in E$ be such that the elements $x_i \mod \mathscr{M}E$ form a basis for $E/\mathscr{M}E$; then the x_i generate E (by Nakayama's lemma). Such a system of generators is called a *minimal* system of generators. Let $x_1, \ldots, x_n$ be a minimal system of generators of E. Let $F = \sum\limits_{i=1}^{n} Ae_i$ be a free module of rank n. Then the sequence $0 \to E_1 \to F_o \xrightarrow{\varphi} E \to 0$ is exact where $\varphi(e_i) = x_i$. Now E_1 is finitely generated. Choosing a minimal set of generators for E_1, we can express E_1 as a quotient of a free module F_2. Continuing in this fashion we get an exact sequence of modules.

$$\cdots \to F_n \to F_{n-1} \to \cdots \to F_o \to E \to 0;$$

we call this a *minimal resolution* of E. We say that the homological dimension of E (notation hd E) is $< n$ if $F_{n+1} = 0$ in a minimal resolution of E. If $F_i \neq 0$ for every i, then we put $hdE = \infty$. It can be proved that
46 $hd\ E$ does not depend upon the minimal resolution (since two minimal systems of generators of E differ by an automorphism of E). We recall that

E is free $\Leftrightarrow$ the canonical mapping $\mathscr{M} \otimes E \to E$ is injective $\Leftrightarrow$ Tor $^A_1(E, A/_{\mathscr{M}}) = 0$.

From this it easily follows that for a finitely generated A-module E we have $hdE < n$ if and only if Tor $^A_{n+1}(E, A/_{\mathscr{M}}) = 0$.

Theorem 1.1 (Syzygies). *Let A be a regular local ring and d the number of elements in an A-sequence generating the maximal ideal $\mathscr{M}$ of A. Then for any finitely generated module E. We have $hdE \leq d$.*

We state a lemma which is not difficult to prove.

Lemma 1.2. *Let A be a noetherian local ring and G a finitely generated A-module with $hdG < \infty$. Let a be a non-zero divisor for G. Then $hd\ \dfrac{G}{aG} = hd\ G + 1$.*

Now if $\mathscr{M} = (x_1, \ldots, x_d)$, where $x_1, \ldots, x_d$ is an A-sequence, then by means of an immediate induction and a use of the above lemma we get $hd(A/_{\mathscr{M}}) = d$. Hence $\mathrm{Tor}^A_{d+1}\ (E, A/_{\mathscr{M}}) = 0$ for any module E'. Hence $hdE \leq d$.

Theorem 1.3 (Serre). *Let A be a local ring with maximal ideal $\mathscr{M}$ such that $hd\mathscr{M} < \infty$. Then A is regular.*

We first observe that the hypothesis of the theorem implies that for an A-module E, we have $hdE \leq hd(A/\mathscr{M}) = hd\ m + 1$.

We prove the theorem by induction on the dimension d of the $A/_m$ vector space $\mathscr{M}/_{\mathscr{M}^2}$. If $d = 0$, then $\mathscr{M} = 0; A$ is a field and therefore
47 regular. Suppose $d > 0$. Then we claim that under the hypothesis of the theorem there exist an element $b \in \mathscr{M} - \mathscr{M}^2$ which is not a zero divisor. This follows from the following lemma.

Lemma 1.4. *Let A be local ring. Suppose that every $x \in \mathscr{M} - \mathscr{M}^2$ is a zero divisor. Then any finitely generated module of finite homological dimension is free.*

Proof. Let G be a module with $hdG < \infty$. If $hdG > 0$, we find, by resolving G, an A-module E such that $hdE = 1$. Let $0 \to F_1 \to F_o \to E \to 0$ be a minimal resolution of E. Then F_1 is free and $F_1 \subset \mathscr{M} F_o$. Now, since every element of $\mathscr{M} - \mathscr{M}^2$ is a zero divisor, it follows that every element of $\mathscr{M}$ is a zero divisor and $\mathscr{M}$ is associated to (0). Hence there exists an $a \neq 0$, such that $a\mathscr{M} = 0$. Hence a $F_1 = 0$. This contradicts the fact that F_1 is free. Hence $hdG = 0$, and G is free. □

Applying this lemma to 'our' A we see that if every element of $\mathscr{M} - \mathscr{M}^2$ is a zero divisor, then $\mathscr{M}$ is free. Since $\mathscr{M}$ consists of zero divisors we have $\mathscr{M} = 0$ i.e. A is a field. Thus if $d > 0$ there is a $b \in \mathscr{M} - \mathscr{M}^2$ such that b is not a zero divisor. Set $A' = A/_{Ab}$, $\mathscr{M}' = \mathscr{M}/Ab$. We claim that $\mathscr{M}/Ab$ is a direct summand of $\mathscr{M}/\mathscr{M}b$. Let ψ denote the canonical surjection $\mathscr{M}/_{\mathscr{M}^b} \to \mathscr{M}/_{Ab}$. Let $b, q_1, \ldots, q_{d-1}$ be a minimal set of generators of $\mathscr{M}$. Set $\sigma = \sum\limits_{i=1}^{d-1} Aq_i$. Let φ be the canonical mapping $\sigma \to \mathscr{M}/_{\mathscr{M}^b}$. Then $\mathrm{Ker}(\varphi) = \sigma \cap \mathscr{M}^b \subset \sigma \cap Ab$. On the other hand if $\lambda b \in \sigma$, then $\lambda b = \sum\limits_{i=1}^{d-1} \lambda_i q_i$, $\lambda_i \in A$. But $b, q_1, \ldots, q_d$ is a minimal set of generators of $\mathscr{M}$. Hence $\lambda, \lambda_i \in \mathscr{M}$. Thus $\sigma \cap \mathscr{M}b = \sigma \cap Ab$.

Thus we have a canonical injection $\mathscr{M}/_{Ab} = \dfrac{\sigma + Ab}{Ab} \xrightarrow{\theta} \dfrac{\mathscr{M}}{\mathscr{M}^b}$, since 48
$\sigma + Ab/_{Ab} \approx \sigma/_{\sigma \cap Ab} = \sigma/_{\sigma \cap \mathscr{M}b}$. It is easy to see that $\psi o \theta = I_{\mathscr{M}}$. Hence $\mathscr{M}/_{Ab}$ is a direct summand of $\mathscr{M}/_{\mathscr{M}^b}$. We now have the following lemma easily proved by induction on $hd(E)$).

Lemma 1.5. *Let A be a commutative ring and E an A-module with $hdE < \infty$. Let $b \in A$ be a non-zero divisor for A and E. Then $hd_{A/Ab} E/bE < \infty$.*

From the above lemma, it follows that $hd_{A/bA} \mathscr{M}/_{\mathscr{M}^b} < \infty$. Since $\mathscr{M}/_{Ab}$ is a direct summand of $\mathscr{M}/_{\mathscr{M}^b}$ we have $hd_{A/Ab}\ \mathscr{M}/Ab < \infty$. Since $\dim_{A/\mathscr{M}}\ \mathscr{M}/Ab/_{\mathscr{M}^2 Ab/Ab} = \dim_{A/\mathscr{M}}\ \mathscr{M}/_{\mathscr{M}^2 + Ab} = d - 1$, A/Ab is regular by induction hypothesis. Hence $\mathscr{M}/Ab$ is generated by an

A/Ab-sequence, say $x_1, \dots x_{d-1}$ modulo Ab. Then $b, x_1, \dots, x_{d-1}$ is an A-sequence and generates $\mathscr{M}$. Thus A is regular.

For any local ring A we define the global dimension of A to be $hdA/\mathscr{M}$, where $\mathscr{M}$ is the maximal ideal; notation : $gl\dim A = \delta(A)$. For any A-module E we have $hd_A E \leq \delta(A)$.

Corollary. *Let A be a regular local ring and $\underline{p}$ a prime ideal with $\underline{p} \neq \mathscr{M}$, where $\mathscr{M}$ is the maximal ideal of A. Then $A_{\underline{p}}$ is regular and $\delta(A_{\underline{p}}) < \delta(A)$.*

Proof. We have $\delta(A_{\underline{p}}) = hd_{A_{\underline{p}}} A_{\underline{p}}/_{\underline{p}A_{\underline{p}}} = hd_{A_{\underline{p}}} A/_{\underline{p}} \otimes A_{\underline{p}} \leq hd_A A/_{\underline{p}}$, the last inequality, being a consequence of the fact that $A_{\underline{p}}$ is A-flat.
49 Choose $x \in \mathscr{M} - \underline{p}$. Since x is not a zero divisor for $A/_{\underline{p}}$ we have by Lemma 1.2, $hd_A A/_{\underline{p}}/_x(A/_{\underline{p}}) = hd_A \dfrac{\underline{p} + x}{\underline{p}} = 1 + hd_A A/_{\underline{p}} \leq \delta(A)$ i.e. $hd_A A/_{\underline{p}} \leq \delta(A) - 1$. Hence $\delta(A_{\underline{p}}) < \delta(A)$. □

Theorem 1.6 (Auslander-Buchsbaum)**.** *Any regular local ring is factorial.*

Proof. Let A be a regular local ring. We prove the theorem by induction on the global dimension $\delta(A)$ of A. If $\delta(A) = 0$, then A is a field and therefore factorial. Suppose $\delta(A) > 0$. Let x be an element of an A-sequence generating $\mathscr{M}$. Then x is a prime element. By Nagata's theorem, we have only to prove that $B = A[\frac{1}{x}]$ is factorial. For any maximal ideal $\mathscr{M}$ of B, we have $B_{\mathscr{M}} = A_{\underline{p}}$, where $\underline{p}$ is a prime ideal with $x \notin \underline{p}$. By the corollary to Theorem 1.3, we see that $A_{\underline{p}}$ is regular and $\delta(A_{\underline{p}}) < \delta(A)$. Hence by the induction hypothesis, $A_{\underline{p}}$ is factorial. Thus $B_{\mathscr{M}}$ is factorial for every maximal ideal $\mathscr{M}$ of B (i.e. B is locally factorial). Let σ be a prime ideal of height 1 in B. Then σ is locally principal i.e. σ is a projective ideal. Now B being a ring of quotients of the regular local ring A, the ideal admits a finite free resolution. By making an induction on the length of the free resolution of σ we conclude that there exist free modules F, L such that $\sigma \oplus L \approx F$. By comparing the ranks we see that $L \approx B^n$, $F \approx B^{n+1}$ for some n. Taking the $(n+1)^{th}$ exterior power we have $\bigoplus_{j=1}^{n} \overset{j}{\wedge}(\sigma) \otimes \overset{n+1-j}{\wedge}(L) \approx B$. Since σ is a modulo of rank 1 $\overset{j}{\wedge}(\sigma)$, $j \geq 2$ is a torsion-module. Hence $\sigma \approx B$ that is, σ is principal and therefore B is factorial. Hence A is factorial. ◻

2 Regular factorial rings

We recall that a regular ring A is a noetherian domain such that $A_{\mathscr{M}}$ is 50
regular for any maximal ideal $\mathscr{M}$ of A. We say that domain A is locally *factorial* if $A_{\mathscr{M}}$ is factorial for every maximal ideal $\mathscr{M}$ of A.

Theorem 2.1. *If A is a regular factorial ring then the rings $A[X]$ and $A[[X]]$ are regular factorial rings.*

Proof. We first prove that $A[X]$ and $A[[X]]$ are regular. Let $B = A[X]$. Let $\mathscr{M}$ be a maximal ideal of B. Set $\underline{p} = A \cap \mathscr{M}$. Then $B_{\mathscr{M}} = (A_{\underline{p}}[X])_{\mathscr{M} A_{\underline{p}}[X]}$. Since a localisation of a regular ring is again regular, we see that $A_{\underline{p}}$ is regular. Thus to prove that B is regular we may assume that A is a local ring with maximal ideal $m(A)$ and that $\mathscr{M} \cap A = m(A)$. Since A is regular, $m(A)$ is generated by an A-sequence, say $a_1, \ldots, a_r$. Now $B/_{m(A)B} \approx A/_{m(A)}[X]$. Thus $\mathscr{M}/_{m(A)B} = (\overline{F}(X))$, where $F(X) \in \mathscr{M}$ is such that the class $\overline{F}(X)$ of $F(X)$ ($\mod m(A)$) is irreducible in $\dfrac{A}{m(A)}[X]$. Now $a_1, \ldots, a_r, F(X)$ is $B_{\mathscr{M}}$-sequence and generates $\mathscr{M}/B_{\mathscr{M}}$ (in fact $\mathscr{M} = (a_1, \ldots, a_r F(X))$). Hence $B_{\mathscr{M}}$ is regular for every maximal ideal $\mathscr{M}$ i.e. B is regular. We shall now prove that $C = A[[X]]$ is regular. Let $\mathscr{M}$ be a maximal ideal of C. Since $X \in Rad(C)$, $\mathfrak{M} = \mathscr{M} + XC$, where $\mathscr{M}$ is a maximal ideal of A. Now $A_{\mathscr{M}} \subset C_{\mathfrak{M}}$. Since $A_{\mathscr{M}}$ is regular, $\mathscr{M} A_{\mathscr{M}}$ is generated by an $A_{\mathscr{M}}$- sequence, say $m_1, \ldots, m_d$. Then $m_1, \ldots, m_d$, X is a $C_{\mathfrak{M}}$-sequence which generates $\mathfrak{M} C_{\mathfrak{M}}$. Thus $C_{\mathfrak{M}}$ is regular i.e. C is regular. ◻

We now prove that $B = A[X]$, $C = A[[X]]$ are factorial. That B 51
is factorial has already been proved (see Chapter I, Theorem 6.5). To prove that C is factorial, we note that K is in the radical Rad (C) of C and $\dfrac{C}{XC} \approx A$ is factorial. Now the following lemma completes the proof of the theorem.

Lemma 2.2. *Let B be a locally factorial noetherian ring (for instance a regular domain). Let $x \in Rad\ (B)$. Assume that B/xB is factorial. Then B is factorial.*

Proof. Let σ be a prime ideal of height 1 in B. Then σ is locally principal i.e. σ is projective. If $x \in \sigma$, then $\sigma = Bx$. If $x \notin \sigma$, then $\sigma \cap Bx = \sigma x$. Thus $\sigma/\sigma x = \sigma/_{(\sigma \cap Bx)} \approx (\sigma + Bx)/_{Bx}$ i.e. $\sigma/_{\sigma x}$ is a projective ideal in $B/_{Bx}$. Since $B/_{Bx}$ is factorial and $\sigma/_{\sigma x}$ divisorial, we see that $\sigma/_{\sigma x}$ is principal in $B/_{Bx}$. Hence, by Nakayama's lemma, σ is principal. ◻

Corollary. *Let A be a principal ideal domain. Then $A[[X_1, \ldots, X_n]]$ is factorial.*

In particular if K is a field, then $K[[X_1, \ldots, X_n]]$ is factorial.

3 The ring of restricted power series

Let A be a commutative ring and let $\mathscr{M}$ be an ideal of A. We provide A with the $\mathscr{M}$ - adic topology. Let $f = \sum a_\alpha X^\alpha \in A[[X_1, \ldots, X_d]]$, $\alpha = (\alpha_1, \ldots, \alpha_d)$, $X^\alpha = X_1^{\alpha_1} \cdots X_d^{\alpha_d}$. We say that f is a *restricted power series* if $a_\alpha \to 0$ as $|\alpha| \to \infty$, $|\alpha| = \alpha_1 + \cdots + \alpha_d$. It is clear that the set of all restricted power series is a subring of $A[[X_1, \ldots, X_d]]$ which
52 we denote by $A\{x_1, \ldots, X_d\}$; we have the inclusions $A[X_1, \ldots, X_d] \subset A\{X_1, \ldots X_d\} A[[X_1, \ldots, X_d]]$. In fact $A\{X_1, \ldots, X_d\}$ is the $\mathscr{M}(X_1, \ldots, X_d)$- adic completion of $A[X_1, \ldots, X_d]$. In particular, if A is noetherian so is $A\{X_1, \ldots, X_d\}$. Further $A[[X_1, \ldots, X_d]]$ is the completion of $A\{X_1, \ldots, X_d\}$ for the $(X_1, \ldots, X_d)$-adic topology. But this is not of interest, since $A\{X_1, \ldots, X_d\}$ is not a Zariski ring with respect to the $(X_1, \ldots, X_d)$-adic topology.

Lemma 3.1. *Let A be a commutative ring and $\mathscr{M}$ an ideal of A with $\mathscr{M} \subset Rad\ (A)$. Let $A\{X_1, \ldots, X_d\}$ denote the ring of restricted power series, A being provided with the $\mathscr{M}$-adic topology. Then $\mathscr{M} \subset Rad\ (A\{X_1, \ldots, X_d\})$.*

Proof. Let $m \in \mathscr{M}$. Consider $1 + ms(X)$, where $s(X) \in A\{X_1, \ldots, X_d\}$. Set $s(X) = a_o + t(X)$, $t(X)$ being without constant term. Since $1 + ma_o$ is invertible, we have $1 + ms(X) = \dfrac{1}{1 + ma_o}(1 - mu(X))$, where $u(X)$ is a restricted series without constant term. Now, $\dfrac{1}{1 - mu(X)} = 1 + mu(X) + m^2u(X)^2 + \cdots$ is clearly a restricted power series. Thus $1 + ms(X)$ is invertible in $A\{X_1, \ldots, X_d\}$ i.e. $m \in \text{Rad}\ (A\{X_1, \ldots, X_d\})$. □

Theorem 3.2. *[P. Salmon]Let A be a regular local ring and let $\mathscr{M}$ denote its maximal ideal. Then $R = A\{X_1, \ldots, X_d\}$ is regular and factorial, the power series being restricted with respected to the maximal ideal.*

Proof. Let $\underline{p}$ be a maximal ideal of R. By Lemma 3.1, $\mathscr{M}R \subset \text{Rad}\ (R) \subset \underline{p}$. Now $\underline{p}/_{\mathscr{M}R}$ is a maximal ideal of $R/_{\mathscr{M}R} = (A/_{\mathscr{M}})[X_1, \ldots, X_d]$. It is well known that any maximal ideal of $(A/_{\mathscr{M}})[X_1, \ldots, X_d]$ is generated by d elements which form an $(A/_{\mathscr{M}})[X_1, \ldots, X_d]$ -sequence. Thus 53
$\underline{p}/_{\mathscr{M}R}$ is generated by an $R/_{\mathscr{M}R}$-sequence. But, A being regular, $\mathscr{M}R$ is generated by an R-sequence. Therefore $\underline{p}$ is generated by an R-sequence. By passing to the localisation, we see that $\underline{p}R_{\underline{p}}$ is generated by a $R_{\underline{p}}$-sequence. Hence R is regular. □

We now prove that R is factorial. The proof is by induction on $gl.\dim A = \delta(A)$. If $\delta(A) = 0$, then A is a field and $R = A[X_1, \ldots, X_d]$ hence R is factorial. Let $\delta = \delta(A) > 0$ and $m_1, \ldots, m_\delta$ generate $\mathscr{M}$. Now R is regular and therefore locally factorial. By Lemma 3.1 $m_1 \in \text{Rad}\ (R)$. Further $R/_{m_1R} \approx (A/_{mA})\{X_1, \ldots, X_d\}$, $\delta(A/_{m_1A}) = \delta - 1$; hence, by induction hypothesis, $R/_{m_1R}$ is factorial. Using Lemma 2.2 we see that R is factorial.

Remark 1. Let A be a local ring which is factorial. Then it does not imply that $A\{T\}$ is factorial. Take $A = k[x, y, z]_{(x,y,z)}$, $z^2 = x^3 + y^7$. As in the proof of Theorem 9.1, Chapter 1, we can prove that there exist $b_1, b_2, \ldots \in A$ such that $(xy - zT)\ (\frac{y}{x} + \frac{b_1}{x^2}T + \frac{b_2}{x^3}T^2 + \cdots + \frac{b_n}{x^{n+1}}T^{n+1} + \cdots) = u \in B = A\{T\}$. In fact it can be checked that we can take the elements b_i such that $u = y^2 - xT^2 - xyT^8 - 3xy^2T^{14} \cdots, -\alpha_n xy^n T^{2+6n} \ldots$, where α_n is an integer such that $0 \leq \alpha_n \leq 2^{3n}$. By providing A with the (x, y, z)-adic topology, we see that the power series u is restricted. Now the proof of Theorem 9.1 verbatum carries over and we conclude that the restricted power series ring $A\{T\}$ is not factorial.

Remark 2. In the above example, if we take $k = \mathbb{R}$ or $\mathbb{C}$, the real number
54 field or the complex number field respectively, then we can speak of the convergent power series ring over A. Now the above power series u is convergent since $0 \leq \alpha_n \leq 2^{3n}$. Hence the convergent power series ring over A is also not factorial.

Chapter 3

Descent methods

1 Galoisian descent

Let A be a Krull ring and let K be its quotient field. Let G be a finite group of automorphisms of A. Let A' denote the ring of invariants of A with respect to G and let K' be the quotient field of A'. Then $A' = A \cap K'$, so that A' is a Krull ring. Since $\prod_{s \in G} (x - s(x)) = 0$, $x \in A$, we see that A is integral over A'. Thus we have the homomorphism $j : D(A') \to D(A)$ and $\overline{j} : C(A') \to C(A)$ (see Chapter 1 §6). We are interested in computing Ker $(\overline{j})$. Let $D_1 = j^{-1}(F(A))$. Then Ker $(\overline{j}) = D_1/_{F(A)}$. Let S be a system of generators of G. Let $\underline{d} \in D_1$, with $j(\underline{d}) = (a)$, $a \in K$. 55
The divisor $j(\underline{d})$ is invariant under G, i.e. $(s(a)) = (a)$, $s \in G$. Hence $s(a)/a \in U$, the group of units of A. Let h denote the homomorphism $h : K^* \to (K^*)^S$ given by $x \rightsquigarrow (s(x)/_x)_{s \in S}$. Then $h(a) \in h(K^*) \cap U^S$, Now if $a = a'u$, $a' \in K$, $u \in U$, then $s(a)/a = s(a')/a' \cdot s(u)/u'$. Thus $h(a)$ is determined uniquely modulo $h(U)$, and we therefore have a homomorphism $\varphi : D_1 \to (h(K^*) \cap U^S)_{h(U)}$ with $\underline{d} \rightsquigarrow h(a) \pmod{h(U)}$, where $a(\underline{d}) = (a)$, $a \in K$.

Theorem 1.1. *The mapping φ induces a monomorphism θ : Ker $(\overline{j}) \to \dfrac{(h(K^*) \cap U^S)}{h(U)}$. Furthermore, if no prime divisor of A is ramified over A', then θ is an isomorphism.*

56 *Proof.* Let $\underline{d} \in D_1$. Then $\varphi(\underline{d}) = 0 \Leftrightarrow h(a) = h(u)$, $u \in U \Leftrightarrow s(a)/a = s(u)/_u$, for all $s \in S$.

$$\Leftrightarrow s(\frac{a}{u}) = \frac{a}{u} \quad \text{for all} \quad s \in G \Leftrightarrow \frac{a}{u} = a' \in K'$$
$$\Leftrightarrow j(d) = (a)_A = (\frac{a}{u})_A = (a')_A = j((a')_{A'}).$$

□

But, since j is injective, we have $\underline{d} = (a')_{A'}$ i.e. $\mathrm{Ker}(\varphi) = F(A')$. Hence θ is a monomorphism.

Now assume that no prime divisor of A is ramified over A'. Let $\alpha \in (h(K^*) \cap U^S)\Big/_{h(U)}$, $\alpha = h(a)$ (mod $h(U)$). Since $h(K^*) = h(A^*)$, we may assume that $a \in A$. Since $s(a)/a \in U$, for $s \in S$, the divisor

(a) is invariant under G. Now, by hypothesis for any prime divisor $\mathscr{Y}' \in D(A')$, we have $j(\mathscr{Y}') = \mathscr{Y}_1 + \cdots + \mathscr{Y}_g$, where the $\mathscr{Y}_i$ form a complete set of prime divisor lying over $\mathscr{Y}'$. Further the $\mathscr{Y}_i$ are conjugate to each other. Since the divisor (a) is invariant under G, the prime divisors which are conjugate to each other occur with the same coefficient in (a) so that (a) is the sum of divisors of form $j(\mathscr{Y}')$, $\mathscr{Y}' \in P(A')$. Hence θ is surjective and therefore an isomorphism.

Remark 1. For $S = G$ the group $(h(K^*) \cap (U)^G)/h(U)$ is the *cohomology group $H^1(G, U)$: in fact a system $(\frac{s(x)}{x})_{s \in G}$ for $x \in K^*$ is the most general cocycle of G in K^* (since $H^1(G_1 K^*) = 0$, as is well known), whence $h(K^*) \cap (U)^G = Z^1(G, U)$; on the other hand $h(U)$ is obviously the group $B^1(G, U)$ of coboundaries. The preceding theorem may also be proved by the following cohomological argument. As usual, if G operates on a*
57 *set E, we denote by E^G the set of invariant elements of E; we recall that $E^G = H^o(G, E)$. Now, since $H^1(G, K^*) = 0$, the exact sequence*

$$0 \to U \to K^* \to F(A) \to 0$$

gives the exact cohomology sequence

$$0 \to U^G \to (K^*)^G \to F(A)^G \to H^1(G, U) \to 0.$$

On the other hand, since U^G is the group of units in $A' = A^G$, we have

$$0 \to U^G \to (K^*)^G \to F(A') \to 0$$

and therefore,

$$0 \to F(A') \to F(A)^G \to H^1(G, U) \to 0$$

In other words, $H^1(G, U) =$ (invariant principal divisors of A) / (divisors of A induced by principal divisors of A'). This gives immediately a monomorphism $\theta : \ker(\bar{j}) \to H^1(G, U)$. If A is divisorially unramified over A', one sees, as in the theorem, that every invariant divisor of A comes from A', thus θ is surjective in this case.

Remark 2. Suppose G is a finite cyclic group generated by an element say s. Then we may take $S = \{s\}$. By Hilbert's Theorem 90, the group $h(K^*)$ is precisely the group of elements of norm 1. Thus $(h(K^*) \cap U)/h(U)$ is the group of units of norm 1 modulo $h(U)$.

Remark 3. The hypothesis of ramification is essential in the above theorem. For instance let $A = \mathbb{Z}[i]$, $i^2 = -1$, $G = \{1, \sigma\}$, $\sigma(i) = -i$. Then $A' = \mathbb{Z}$, $C(A') = C(A) = 0$. Hence $\mathrm{Ker}(\bar{j}) = 0$. However, $U \cap h(K^*) = \{1, -1, i, -i\}$, $h(U) = \{1, -1\}$. Thus $(h(K^*) \cap U)/h(U) \approx \mathbb{Z}/_{(2)}$.

We note that the prime number 2 is ramified in A. **58**

Examples: Polynomial rings.

1. Let k be a fied and $A = k[x_1, \ldots, x_d]$, the ring of polynomials in d variables, $d \geq 2$. Let n be an integer with $(n, p) = 1$, p being the characteristic of k and let k contain a primitive n^{th} root of unity w. Consider the automorphism $s : A \to A$ with $x_i \rightsquigarrow wx_i$, $1 \leq i \leq d$ and let G be the cyclic group of order n generated by s. Then the ring of invariants A' is generated by the monomials of degree n in the x_i; geometrically this is the n-tuple model of the projective space. Set $F_i(X) = X^n - x_i^n$. Now any ramified prime divisor of A must contain $F_i'(x_i) = nx_i^{n-1}$. Thus there is no divisorial ramification in A. Here $U = k^*$ and the group of units of norm 1 is the group of n^{th} roots of

unity. Further $h(U) = \{1\}$, $(h(K^*) \cap U)/h(U) \approx \dfrac{\mathbb{Z}}{(n)}$, by Remark 2. Since A is factorial, by Theorem 3.1, we have $C(A') \approx \mathbb{Z}/(n)$.

2. Let k, w, n, be as in (1) and $A = k[x, y]$. Let s be the k-automorphism of A defined by $x \rightsquigarrow wx$, $y \rightsquigarrow w^{-1}y$. The ring of G-invariants $A' = k[x^n, y^n, xy]$, i.e. A' is the affince coordinate ring of the surface $Z^n = XY$. Again as in (1) there is no divisorial ramification, $U = k^*$ and $C(A') \approx \mathbb{Z}/(n)$.

3. Let k be a field and $A = k[X_1, \ldots X_n]$. Let A_n denote the alternating group. Now A_n acts on A. If the characteristic of k is $\neq 2$, then the ring of A_n-invariants is $A' = k[s_1, \ldots, s_n, \triangle]$ where $s_1 \cdots s_n$ denote
59 the elementary symmetric functions and $\triangle = \prod\limits_{1<j)} (x_i - x_j)$. If characteristic $k = 2$, then $\triangle$ is also symmetric and $A' = k[s_1, \ldots, s_n, \alpha]$, where $\alpha = \dfrac{1}{2}(\prod\limits_{i<j}(x_i - x_j) + \prod\limits_{i<j}(x_i + x_j))$.

As the coefficients of $\prod\limits_{i<j}(x_i - x_j) + \prod\limits_{i<j}(x_i + x_j)$ are divisible by 2, the element α has a meaning in characteristic 2. Further there is no divisorial ramification in A over A'. For the only divisorial ramifications of A over $k[s_1, \ldots, s_n]$ are those prime divisors which contain $F'(x_i) = \prod\limits_{j\neq i}(x_j - x_i)$, where $F(X) = \prod(X - x_j)$. Since $\triangle = \prod\limits_{i<j}(x_i - x_j) \in A'$ (in characteristic 2, $\triangle$ is in fact in $k[s_1, \ldots, s_n]$), there is no divisorial ramification in A over A'. Hence $C(A') \approx H^1(A_n, U)$, by the remark following Theorem 1.1. But $U = k^*$ and A_n acts trivially on k^*. Hence $C(A') \approx H^1(A_n, U)$ is the group of homomorphisms of A_n into k^*. Thus if $n \geq 5$, A_n is simple and therefore $C(A') = 0$ i.e. A' is factorial. The only non-trivial cases we have to consider are, $n = 3, 4$. For $n = 3$, A_n is the cyclic group of order 3. Hence $C(A') = 0$ if k does not contain cube roots of unity, otherwise $C(A') \approx \mathbb{Z}/(3)$. We now consider the case $n = 4$. We have $[A_4, A_4] = \{1, (2\ 2)(3\ 4), (1\ 4)(2\ 3), (1\ 3)(2\ 4)\}$ and $A_4/[A_4, A_4] \approx \mathbb{Z}/(3)$. Now the group of homomorphisms of A_4 into k^* is isomorphic to the group of homomorphisms of $A_4/[A_4, A_4]$ into k^*. Hence, is in the case $n = 3$, $C(A') = 0$ if k does not contain cube roots of unity; otherwise

$C(A')_{\approx}\mathbb{Z}/(2)$.

Example. Power series rings. We first prove the following lemma.

Lemma 1.2. *Let A be a local domain, $\mathscr{M}$ its maximal ideal. Let s be an automorphism of A of order n, $(n, \text{char } (A/\mathscr{M})) = 1$. Let U denote the group of units of A and h the mapping $K^* \to K^*$ with $x \rightsquigarrow s(x)/x$, K being the quotient field of A. Then $(1 + \mathscr{M}) \cap h(K^*) \subset h(U)$ (i.e. $\operatorname{im}(H'(G, I + \mathscr{M}) \to H'(G, U)) = 0$, where G is the group generated by s).* 60

Proof. Let $u \in 1 + \mathscr{M}$, $u = s(x)/_x$, $x \in K^*$. Then u has norm 1, i.e. $N(u) = u^{1+s+\cdots+s^{n-1}} = 1$. Set $v = 1 + u + u^{1+s} + \cdots + u^{1+\cdots+s^{n-2}}$. Then $v \equiv n.1(\mod \mathscr{M})$. Since n is prime to the characteristic of $A/\mathscr{M}$, it follows that v is a unit. Further we have $s(v) = 1 + u^s + u^{s+s^2} + \cdots u^{s+1\cdots+s^{n-1}}$ and $us(v) = v$ i.e. $u = s(v^{-1})/v^{-1} \in h(U)$ and the lemma is proved. □

In the examples (1) and (2) of polynomial rings we replace the rings $A = K[x_1, \ldots, x_d]$ and $A = K[x, y]$ respectively by $A = K[[x_1, \ldots, x_d]]$ and $A = K[[x, y]]$. Since in A we have $U/(1 + \mathscr{M}) \approx k^*$, we obtain the same results as in the case of ring of polynomials, in view of the above lemma.

Proposition 1.3. *Let A be a local ring, $\mathscr{M}$ its maximal ideal. Let G be a finite group of automorphisms of A, acting trivially on $k = A/\mathscr{M}$. Further, assume that there are no non-trivial homomorphisms of G into k^* and that $(Card(G),\ Char\ (k)) = 1$. Then $H^1\ (G, U) = 0, U$ being the group of units of A. In particular, if A is factorial, so is A'.*

Proof. Let $(u_s)_{s\in G}$, $u_s \in U$, be a 1-cocycle of G with values in U. Then $u_{ss'} = s(u_{s'}).u_s$. Reducing modulo $\mathscr{M}$, we get $\overline{u}_{ss'} = \overline{u}_{s'} \cdot \overline{u}_s$, since G acts trivially on k. We have made the hypothesis that there are no non-trivial homomorphisms of G into k^*. Hence $u_s \in 1 + \mathscr{M}$, $s \in G$. Set $y = \sum\limits_{t\in G} u_t$. 61
Then $y = \text{Card } (G) \cdot 1 (\mod \mathscr{M})$. Thus $y \in U$. Now $s(y) = \sum\limits_{t\in G} s(u_t) = \sum\limits_t \dfrac{u_{st}}{u_s} = \dfrac{1}{u_s} y$ i.e. $u_s = s(y^{-1})/y^{-1}$. Hence $H^1(G, U) = 0$. □

Corollary . *Let* $A = k[[x_1, \ldots, x_n]]$. *Let* k *be of characteristic* $p > n$ *or 0. Let* A_n *be the alternating group on* n *symbols. Then for* $n \geq 5$, $H^1(G, U) = 0$, *i.e. the ring of invariants* A' *is factorial.*

For further information about the invariants of the alternating group we refer to Appendix 1.

2 The Purely inseparable case

Let A be a Krull ring of characteristic $p \neq 0$, and let K be its quotient field. Let $\triangle$ be a derivation of K such that $\triangle(A) \subset A$. Set $K' = \mathrm{Ker}(\triangle)$ and $A' = A \cap K'$. Then A' is again a Krull ring and $A^p \subset A'$, $K^p \subset K'$. In particular, A is integral over A'. Hence the mapping $j : D(A') \to D(A)$ of the group of divisors goes down to a mapping $\bar{j} : C(A') \to C(A)$ of the corresponding divisor class groups. We are interested in computing $\mathrm{Ker}(\bar{j})$. Set $D_1 = j^{-1}(F(A))$, so that $\mathrm{Ker}(\bar{j}) = D_1/F(A')$. Let $\underline{d} \in D_1$, and $j(\underline{d}) = (a)$, $a \in K^*$. From the definition of j it follows that $e_{\underline{p}}$ divides $v_{\underline{p}}(a)$, where $\underline{p}$ is a prime divisor of A, $v_{\underline{p}}$ the corresponding valuation and $e_{\underline{p}}$ the ramification index of $v_{\underline{p}}$. Hence there exists an $a' \in K'^*$ such that $v_{\underline{p}}(a) = v_{\underline{p}}(a')$, i.e. $a = \overline{a'}.u$, u being a unit in $A_{\underline{p}}$. Thus $\triangle a/a = \triangle a'/a' + \triangle u/u = \dfrac{\triangle u}{u}$. Since $\triangle(A_{\underline{p}}) \subset A_p$, it follows that
62 $\triangle a/a \in A_{\underline{p}}$, for all prime divisors $\underline{p}$ of A, i.e. $\triangle a/a \in A$. We shall call $ax \in K$, a *logarithmic derivative* if $x = \triangle t/t$ for some $t \in K^*$. The set of all logarithmic derivative is an additive subgroup of K. Set $\mathscr{L} = \{\triangle t/t \big| \triangle t/t \in A, t \in K^*\}$. Let U denote, as before, the group of units of A and set $\mathscr{L}' = \{\triangle u/u \big| u \in U\}$. Now $\mathscr{L}' \subset \mathscr{L}$. For $a\underline{d} \in D_i$ with $j(\underline{d}) = (a)$, $a \in K^*$, $\triangle a/a \in \mathscr{L}$ is uniquely determined modulo $\mathscr{L}'$. Let φ denote the homomorphism : $D_1 \to \mathscr{L}/\mathscr{L}'$, $\underline{d} \rightsquigarrow \triangle a/a(\mod \mathscr{L}')$ if $j(\underline{d}) = (a)$. Now $\varphi(\underline{d}) = 0 \Leftrightarrow \triangle a/a = \triangle u/u$, for $u \in U \Leftrightarrow \triangle(a/u) = 0$ i.e. $a/u = a' \in K' \Leftrightarrow (a)_A = (a')_A$. But $j((a')_{A'}) = (a')_{A'}$ and j is injective. Hence $\underline{d} = (a')_{A'}$. Thus $\mathrm{Ker}(\varphi) = F(A')$. We have proved the first assertion of the following theorem.

Theorem 2.1. *(a) We have a canonical monomorphism* $\varphi : \mathrm{Ker}(\bar{j}) \to \mathscr{L}/\mathscr{L}'$.

(b) If $[K : K'] = p$ and if $\triangle(A)$ is not contained in any prime ideal of height 1 of A, then $\bar{\varphi}$ is an isomorphism.

Proof. To complete the proof of the theorem, we have only to show that $\bar{\varphi}$ is surjective under the hypothesis of (b). As K/K' is a purely inseparable extension, every prime divisor of A' uniquely extends to a prime divisor of A. Thus a divisor $\underline{d} = \sum_{\underline{p}\in P(A)} n_{\underline{p}}\underline{p} \in \mathrm{Im}(j)$ if and only if $e_{\underline{p}}/n_{\underline{p}}$ where $e_{\underline{p}}$ denotes the ramification index of $\underline{p}$. Since $A^p \subset A'$, it follows that for any prime division $\underline{p}$ of A, $e_{\underline{p}} = 1$ or p. Let $a \in K^*$ be such that $\triangle a/a \in A$. It is sufficient to prove that for a prime divisor $\underline{p}$ of A, if $n = v_p(a)$ is not a multiple of p, then $e_p = 1$. Let t be a uniformising parameter of v_p. Let $a = ut^n$, u being a unit in $A_{\underline{p}}$. Then $\triangle u/u + n\ \triangle t/t = \triangle a/a \in A_{\underline{p}}$. Hence, $\triangle t/t \in A_{\underline{p}}$, i.e. $\triangle$ induces a derivation $\bar{\triangle}$ on the residue class field $k = A_{\underline{p}}/tA_{\underline{p}}$. By hypothesis, since $\triangle A \not\subset \underline{p}$, we have $\bar{\triangle} \neq 0$. Let k' be the residue class field of $\underline{p} \cap A'$. Then $\bar{k'} \subseteq \mathrm{Ker}(\bar{\triangle}) \underset{\neq}{\subset} k$. Thus $f = [k : k'] \neq 1$. Since $[K : K'] = p$, and $k^p \subset k'$, we have $f = p$. Now the inequality $e_{\underline{p}} f \leq [K : K'] = p$ gives $e_p = 1$. The proof of Theorem 2.1 is complete. □ 63

3 Formulae concerning derivations

Let K be a field of characteristic $p \neq 0$ and let $D : K \to K$ be a derivation. Let tD denote the derivation $x \rightsquigarrow t.\ D(x)$. We note that D^p, the p^{th} iterate of D, is again a derivation.

Proposition 3.1. *Let $D : K \to K$ be a derivation of K(char $K = p \neq 0$). Assume that $[K : K'] = p$. Then*

(a) $D^p = aD$, $a \in K' = \mathrm{Ker}\, D$.

(b) If A is a Krull ring with quotient field K such that $D(A) \subset A$, that $a \in A' = K' \cap A$.

Proof. (a) By hypothesis $K = K'(z)$, $z^p \in K'$. For any K'- derivation $\triangle$ of K, $\triangle = \dfrac{\triangle z}{Dz}D$. In particular $D^p = aD$ for $a \in K$. Hence

$D_a^{p+1} = D(D^p a) = D(a \cdot Da) = (Da)^2 + aD^2 a$. On the other hand, $Da^{p+1} = D^p(Da) = aD^2 a$. Hence $Da = 0$ i.e. $a \in K'$.

(b) Since $A = \bigcap_{p \in P(A)} A_{\underline{p}}$ and $D(A_{\underline{p}}) \subset A_{\underline{p}}$, we have only to deal with the case when A is a discrete valuation ring. Let v denote the corresponding valuation. Let $t \in A$, with $v(t) = 1$. We have $D^p t = a \cdot Dt$. If $v(Dt) = 0$, then $a = \dfrac{1}{Dt}$, $D^p t \in A$. Assume $v(Dt) > 0$. Then for $x \in A$, we have $v(Dx) \geq v(x)$. For is $x = ut^n$ with $v(u) = 0$. In particular, $v(D^p t) \geq v(Dt)$ i.e. $a \in A$.

□

64 **Proposition 3.2.** *Let $D : K \to K$ be a derivation of, K(char $K = p \neq 0$). Let $K' = \operatorname{Ker} D$ and $[K : K'] = p$. An element $t \in K$ is a logarthmic derivative (i.e. there exists an $x \in K$ such that $t = Dx/x$) if and only if*

$$D^{p-1}(t) - \ at \ + t^p = 0,$$

where $D^p = aD$.

Proof. We state first the following formula of Hochschild (Trans. A.M.S. 79(1955), 477-489). □

Let K be a field of characteristic $p \neq 0$ and D a derivation of K. Then

$$(tD)^p = t^p D^p + (tD)^{p-1}(t).D$$

($t \in K$, tD denotes the derivation $x \rightsquigarrow t.Dx$). We have to prove the proposition only in the case when $t \neq 0$.

Let now t be a logarthmic derivative, say $t = Dx/x$. Set $\triangle = \dfrac{1}{t}D$. Then by Hochschild's formula, we have,

$$\begin{aligned} D^p &= (t\triangle)^p = t^p \triangle^p + (t\triangle)^{p-1}(t)\triangle. \\ &= t^p \triangle^p + D^{p-1}(t) \cdot \triangle = aD. \end{aligned}$$

But $\triangle^n x = x$, for $n \geq 1$. Hence $a.Dx = t^p x + D^{p-1}(t)x$, i.e.

$$t^p - \ \text{at} \ + Dt^{p-1}(t) = 0.$$

Conversely assume that t is such that $D^{p-1}t -$ at $+ t^p = 0$. Set $\triangle = \frac{1}{t}.D$. Again by Hoschschild's formula, we have $D^p = (t\triangle)^p = t^p\triangle^p + D^{p-1}(t).\triangle = aD = a.t\triangle$, i.e. $a.t\triangle = t^p\triangle^p + (\text{at} - t^p)\triangle$ i.e. $t^p(\triangle^p - \triangle) = 0$, i.e. $\triangle^p - \triangle = 0$, i.e. $(\triangle - (p-1)I)\cdots(\triangle - 2I)(\triangle - I) = 0$, where I is the identity mapping of K into K. Choose $y \in K$ with $y_1 = \triangle y \neq 0$ and set 65 $y_2 = (\triangle - I)y_1, \ldots, y_p = (\triangle - (p-1)I)y_{p-1}(= 0)$. Then, there exists a j such that $y_{j-1} \neq 0$ and $y_j = (\triangle - jI)y_{j-1} = 0$.
Hence

$$\triangle y_{j-1} = jy_{j-1}, \quad \text{i.e. } \triangle y_{j-1}/y_{j-1} = j \in \mathbb{F}_p^*, \mathbb{F}_p$$

being the prime field of characteristic p. Let n be the inverse of j modulo p. Set $x = y_{j-1}^n$. Then $\frac{\triangle x}{x} = n\frac{y_{j-1}}{y_{j-1}} = nj = 1$, i.e. $\triangle x = x$ i.e. $t = Dx/x$.

4 Examples: Polynomial rings

Let k be a factorial ring of characteristic $p \neq 0$. Set $A = k[x,y]$. Let D be a k-derivation of A and $A' = \text{Ker}(D)$. The group of units U of A is the group of units of k. Hence here $\mathscr{L}' = \underline{0}$. Since A is factorial, we by Theorem 2.1, an injection of $C(A') = \text{Ker}(\bar{j})$ into $\mathscr{L}$. (We recall that $\mathscr{L}$ is the group of logarthmic derivatives contained in A and that $\mathscr{L}'$ is the group of logarthmic derivatives of units.) We shall now consider certain special k-derivations of A.

(a) **The Surface $Z^p = XY$.** Consider the derivation D of A $k[x,y]$ with $Dx = x$ and $Dy = -y$. Then $k[x^p, y^p, xy] \subset A' = \text{Ker}(D)$. Let L, K, K' denote the quotient fields of k, A, A' respectively. Now $L[x^p, y^p, xy]$ is the coordinate ring of the affine surface $Z^p = XY$. Since the surface $Z^p = XY$ has only an isolated singularity (at the origin), it is normal. But $k[x^p, y^p, xy] = L[x^p y^p, xy] \cap k[x,y]$. Hence $k[x^p, y^p, xy]$ is normal. Since A' is integral over $k[x^p, y^p, xy]$ and has the same quotient field as $k[x^p, y^p, xy]$, we have $A' = k[x^p, y^p, xy]$. We note that the hypothesis of Theorem 2.1 (b) is satisfied here. 66 Hence $C(A') = \mathscr{L}$. Now $\mathscr{L} = \{DP/P \big| P \in K, DP/P \in A\}$. For $P \in A$, we have $d^o(DP) \leq d^o(P)$. Hence $DP/P \in \mathscr{L}$ if and only if

$DP/P \in k$. The formula $D(x^a y^b) = (a-b)x^a y^b$ shows that $\mathscr{L} = \mathbb{F}_p$, the prime field of characteristic p. Hence $C(A') \approx \mathbb{Z}/(p)$.

(b) **The surface $Z^p = X^i + Y^j$.** Again we take $A = k[x, y]$, k a factorial ring of characteristic $p \neq 0$. Let D be the k-derivation of A given by $Dx = jy^{j-1}$, $Dy = -ix^{i-1}$, where i, j are positive integers prime to p. Let K, K', L denote the quotient fields of $A, A' = \text{Ker}(D)$ and k respectively. We have $k[x^p, y^p, x^i + y^j] \subset A'$ and $[L(x^p, y^p, x^i + y^j) : K] = p$. Hence $K' = L(x^p, y^p, x^i + y^j)$. Now $L[x^p, y^p, x^i + y^j]$ is the coordinate ring of the affine surface $Z^p = X^i + Y^j$ which is normal since it has only an isolated singularity (at the origin). Hence $L[x^p, y^p, x^i + y^j]$ is integrally closed. But $k[x^p, y^p, x^i + y^j] = L[x^p, y^p, x^i + y^j] \cap k[x, y]$. Hence $k[x^p, y^p, x^i + y^j]$ is integrally closed. Since A' is integral over $k[x^p, y^p, x^i + y^j]$, we have $A' = k[x^p, y^p, x^i + y^j]$. We remark that our D satisfies the hypothesis of Theorem 2.1 (b). Hence $C(A') = \{DP/P \big| P \in K, DP/P \in A\}$. We shall now compute $\mathscr{L}$. We attach weights j and i to x and y respectively. By Proposition 3.1, we have $D^p = aD$ with $a \in A'$. It is easily checked that if G is an isobaric polynomial of weight w, then DG is isobaric weight $w + ij - i - j$ and therefore $D^p G$ is isobaric of weight $w + p(ij - i - j)$. Now $D^p x = aDx$. Comparing the weights we see that a is isobaric of weight $(p-1)(ij - i - j)$.

67 Let F be a polynomial which is a logarthmic derivative. Let F_α of weight α (respectively F_β of weight β) be the component of smallest (respectively largest) weight of F. By Proposition 3.2, F is a logarthmic derivative if anly only if $D^{p-1}F - aF = -F^p$. Comparing the weights of the components with smallest and largest weights on both sides, we get weight $(D^{p-1}F_\alpha - aF_\alpha) \leq$ weight (F_α^p) and weight $(D^{p-1}F_\beta - aF_\beta) \geq$ weight (F_β^p). That is $p\alpha \geq \alpha + (p-1)(ij - i - j)$, $p\beta \leq \beta + (p-1)(ij - i - j)$. Hence $ij - i - j \leq \alpha \leq \beta \leq ij - i - j$ i.e. $\alpha = \beta = ij - i - j$. Hence F must be isobaric of weight $ij - i - j$. Set $d = (i, j)$, $i = dr$, $j = ds$. Thus, the monomials that can occur in F are of the form $x^\lambda y^\mu$, $\lambda j + \mu i = ij - i - j$ i.e. $\lambda s + \mu r = drs - r - s$, i.e. $(\lambda + 1)s = (ds - \mu - 1)r$. Since $(r, s) = 1$, $\lambda + 1$ is a multiple of r. Thus the smallest value of λ admissible is $r - 1$, the corresponding μ being $(d-1)s - 1$. Thus F is necessarily of the form

$F = \sum_{n=1}^{d-1} b_n x^{nr-1} y^{(d-n)s-1}$. If $d = 1$, then $\mathscr{L} = 0$ and A' is factorial. If $d > 1$, the coefficients of $D^{p-1}F - aF$ will be linear forms in $b_1, \ldots, b_{d-1}$ and those of $-F^p$ are p^{th} powers of $b_1, \ldots, b_{d-1}$. Thus F is a logarithmic derivative if and only if $b_n^p = L_n(b)$, $L'_{n'}(b) = 0$, $1 \leq n \leq d-1$, $1 \leq n' \leq t$, where $L_n(b)$, $L'_{n'}(b)$ are linear forms occuring as the coefficient of $D^{p-1}F - aF$.

$L'_{n'}(b)$ indicates the ones which do not occur in $-F^p$. The hypersurfaces $b_n^p = L_n(b)$ intersect at a finite number of points in the profective space P^{d-1} and, by Bezout's theorem, the number of such points in the algebraic closure of L is atmost p^{d-1}. As $\mathscr{L}$ is an additive subgroup of A, $\mathscr{L}$ is a p-group of type $(p, \ldots, p)$ of order p^f, $f \leq d-1$. Hence we have proved the 68

Theorem 4.1. *Let k be a factorial ring of characteristic $p \neq 0$, and let i, j be two positive integers prime to p and $d = (i, j)$. Then the group $C(A')$ of divisor classes of $A' = k[X, Y, Z]$ with $Z^p = X^i + Y^j$ is a finite group of type $(p, \ldots p)$ of order p^f with $f \leq d-1$. In particular A' is factorial if i and j are coprime.*

We can say more about $C(A')$ in the case $p = 2$. Let k be of characteristic 2. Then $D^2 = 0$, i.e. $a = 0$. The equation for the logarithmic derivative then becomes $DF = F^2$. As above F is of the form $F = \sum_{n=1}^{d-1} b_n x^{nr-1} y^{(d-n)s-1}$. Here i, j, r, s, d are all odd integers. If n is odd, then $D(b_n x^{nr-1} y^{(d-n)s-1} = b_n x^{nr-1+dr-1} y^{(d-n)s-2}$. The corresponding term in D^2F is $b_m^2 x^{2mr-2} y^{2(d-m)s-2}$, where $2m = n + d = 2q + 1 + d(n = 2q + 1)$, $b_n = b_m^2$. Set $d = 2c - 1$. Then $m = q + c$. Thus $b_{2q+1} = b_{q+c}^2$. On the other hand let n be even, say $n = 2q$. The $D(b_n x^{nr-1} y^{(d-n)s-1}) = b_n x^{nr-2} y^{(d-n)s-1+ds-1}$. The corresponding term in D^2F is $b_m^2 x^{2mr-2} y^{2(d-m)s-2}$, where $b_n = b_m^2$ and $nr - 2 = 2mr - 2$ i.e. $2m = n = 2q$. Hence $b_{2q} = b_q^2$. Thus F is a logarithmic derivative if and only if the equations $b_{2q+1} = b_{q+c}^2$ and $b_{2q} = b_q^2$, $d + 1 = 2c$, are satisfied.

Consider the permutation $\prod$ of $(1, 2, \ldots, d-1)$ given by, $\prod(2q) = q$, $1 \leq q \leq c-1$, $\prod(2q-1) = q + c$, $0 \leq q \leq c-2$. Now the equations for the logarthmic derivative can be written as $b_q = b_{\Pi(q)}^2$, $1 \leq q \leq 2c-2$. Let $U_1, \ldots, U_l$ be the orbits of the group generated by $\prod$ and let Card

69 $(U_i) = u(i)$. Then $u(1)+\cdots+u(l) = 2c-2$. If $U_e = (q_1, \ldots q_{u(e)})$, then the equations $b_{q_1} = b^2_{\Pi(q_1)}, \ldots, b_{q_{u(e)}} = b^2_{\Pi(q_{u(e)})}$ are equivalent to $b_{q_1}^{2^{u(e)}} = b_{q_1}$. Thus the solutions of $b^{2u(e)} = b$ give rise to solution of $b_m = b^2_{\Pi(m)}$, where $m \in U_l$. But the solutions of $b^{2^{u(e)}} = b$ in k is the group $\mathbb{F}(2^{u(e)}) \cap k$, where $\mathbb{F}(2^{u(e)})$ is the field consisting of $2^{u(e)}$ elements. Hence the group $\mathscr{L}$ of logarithmic derivatives is isomorphic to $\prod_{e=1}^{1} (\mathbb{F}(2^{u(e)}) \cap k)$. Hence we have proved the following

Theorem 4.2. *Let k be a factorial ring of characteristic 2 and let i, j be odd integers and $d = (i, j)$. Let $A' = k[X, Y, Z]$, $Z^2 = X^i + Y^j$. The group $C(A')$ is of the type $(2, \ldots, 2)$ and of order 2^u with $u \leq d - 1$. If k contains the algebraic closure of the prime field, then the order of $C(A')$ is 2^{d-1}.*

Remark. It would be interesting to know if the above theorem is true for arbitrary non-zero characteristics. We remark that for $p = 3$ and for the surfaces $Z^3 = X^2 + Y^4$, $Z^3 = X^4 + Y^8$, the analogue of the above result can be checked.

5 Examples: Power series rings

Let A be a Krull ring and $D : A \to A$, a derivation of A. Let $\mathscr{L}$ denote the group of logarithmic derivatives contained in A and $\mathscr{L}'$ the group of logarithmic derivatives of units of A. Set $\underline{q} = A \cdot D(A)$. We have, $\mathscr{L}' \subset \underline{q} \cap \mathscr{L}$. We prove the other inclusion in a particular case.

70 **Lemma 5.1.** *Let A be a factorial ring of characteristic 2 and $D : A \to A$ be a derivation of A satisfying $D^2 = aD$, with $a \in$ Ker(D). Assume that there exist $x, y \in$ Rad (A) such that $\underline{q} = (Dx, Dy)$. Then $\mathscr{L}' = \mathscr{L} \cap \underline{q}$.*

Proof. Let $t \in \mathscr{L} \cap \underline{q}$, say $t = cDx + dDy$. If $r = (Dx, Dy)$. By considering the derivation $\frac{1}{r}D$, we may assume that Dx and Dy are relatively prime. Since $t \in \mathscr{L}$, by Proposition 3.2, we have $Dt + at + t^2 = 0$. Substituting $t = cDx + dDy$ in this equation, we get

$$Dx(Dc + c^2 Dx) = Dy(Dd + d^2 Dy).$$

□

Since Dx and Dy are relatively prime, there is an $\alpha \in A$ such that

$$Dc + c^2Dx = \alpha Dy, Dd + d^2Dy = \alpha Dx.$$

Set $u = 1 + cx + dy + (cd + \alpha)xy$. The element u is a unit in A. A straight forward computation shows that $Du = tu$. The proof of the lemma is complete.

(a) **The surface $Z^2 = XY$ in characteristic 2.** Let k be a regular factorial ring. Then, by Theorem 2.1, $A = k[[x, y]]$ is factorial. Let D be the k-derivation of A given by $Dx = x, Dy = y$. Then as in §4, $A' = \ker(D) = k[[x^2, y^2, xy]] = k[[X, YZ]], Z^2 = XY$. Here, $\underline{q} = (x, y)$ and $[K : K'] = 2$. Hence, by Theorem 2.1, $C(A') \approx \mathscr{L}/\overline{\mathscr{L}}'$. By Lemma 5.1, we have $\mathscr{L}/\mathscr{L}' = \mathscr{L}/(\mathscr{L} \cap \underline{q} = (\mathscr{L} + \underline{q}/\underline{q}$. This, and the formula $D(x^a y^b) = (a - b)x^a y^b$ show that $(\mathscr{L} + \underline{q})/\underline{q} \approx \mathbb{F}_2 = \mathbb{Z}/(2)$.

(b) **The Surface $Z^2 = X^{2i+1} + Y^{2j+1}$ in characteristic 2.** Let k be a **71**
regular factorial ring and $A = k[[x, y]]$. Let D be the k-derivation defined by $Dx = y^{2j}, Dy = x^{2i}$. Then $A' = k[[x^2, y^2, x^{2i+1} + y^{2j+1}]] = k[[X, Y, Z]], Z^2 = X^{2i+1} + Y^{2j+1}$. We have $\underline{q} = AD(A) = (x^{2i}, y^{2j})$ and $[K : K'] = 2$. Hence $C(A') \approx \mathscr{L}/\overline{\mathscr{L}}'$. Since $D^2 = 0$, an element $F \in A$ is a logarthmic derivative if and only if $DF = F^2$. We assign the weights $2j + 1$ and $2i + 1$ to x and y respectively. For an $F \in A$ with $F = \sum_{l \geq q} F_l$, where F_l is an isobaric polynomial of weight l, $F_q \neq 0$, we call q the order of F, $0(F) = q$. As in Theorem 4.1, D elevates the weight of an isobaric polynomial by $4ij - 1$, Hence, if $F \in \mathscr{L}$ and $0(F) = q$, then $0(F) = 2q = 0(DF) = q + 4ij - 1$. Hence $q \geq 4ij - 1$.

Let $\mathscr{L}_q = \{F \big| F \in \mathscr{L}, 0(F) \geq q\}$. Now $\{\mathscr{L}_q\}_{q \geq 4ij-1}$ filters $\mathscr{L}$ and $\mathscr{L}'_q = \mathscr{L}_q \cap \mathscr{L}'$ filters $\mathscr{L}'$. Hence $C(A') = \mathscr{L}/\mathscr{L}'$ is filtered by $C_q = (\mathscr{L}_q + \mathscr{L}')/_{\mathscr{L}' \approx \mathscr{L}_{q/\mathscr{L}'q}}$. In view of Lemma 5.1, we have $\mathscr{L}_q = \mathscr{L}'_q$ for q large, ie.e $C_q = 0$, for q large. Since the C_q are vector spaces over $\mathbb{F}_2$,

the extension problem here is trivial. Hence $C(A') \approx \sum_{q \geq 4ij-1} C_q/C_{q+1}$. Since $0(x^{2i}) = 2i(2j+1) > 4ij$ and $0(y^{2j}) = 2j(2i+1) > 4ij$, we have $\mathscr{L}' = \mathscr{L} \cap \underline{q} \subset \mathscr{L}_{4ij}$. Therefore $C_{4ij-1}/C_{4ij} = \mathscr{L}_{4ij-1}/\mathscr{L}_{4ij}$. By Theorem 4.2, $\mathscr{L}_{4ij-1}/\mathscr{L}_{4ij}$ is a finite group of type $(2, \ldots, 2)$ of order 2^f, with $f \leq d-1, d = (2i+1, 2j+1)$. We now determine C_q/C_{q+1}, for
72 $q \geq 4ij$. Let $A^{(q)}$ denote the k-free module generated by monomials of weight q. Let $\varphi_q : \mathscr{L}_q \to A^{(q)}$ be the homomorphism given by $\varphi_q(F) =$ component of F of weight $q, F \in \mathscr{L}_q$. Then $\ker(\varphi_q) = \mathscr{L}_{q+1}$. We shall now prove

$$\varphi_q(\mathscr{L}_q) = A^{(q)} \cap A', q \geq 4ij, \tag{*}$$

$$\varphi_q(\mathscr{L}'_q) = A^{(q)} \cap A' \cap \underline{q}, q \geq 4ij. \tag{**}$$

Note that $(**)$ is a consequence of $(*)$ and the fact that

$$\mathscr{L}'_q = \mathscr{L}_q \cap \underline{q}.$$

Proof if (*). *Let $F = F_q + F_{q+1} + \cdots \in \mathscr{L}_q, F_q$ being of weight q. Since $DF = F^2$, and weight $DF_q = q + 4ij - 1 < 2q$, we have $DF = 0$, i.e. $\varphi_q(F) = F_q \in A^{(q)} \cap A'$. Conversely, let $F_q \in A^{(q)} \cap A'$. We have to find $F_n, n \geq q, F_n$ isobaric polynomial weight n, such that $F = \sum_{n \geq q} F_n \in \mathscr{L}_q$, i.e. $DF = F^2$. Hence we have to determine F_n such that $DF_n = 0$, if n is even or $n + 4ij - 1 < 2q$ and $DF_n = F^2 m$, if $2m = n + 4ij - 1 (m < n)$. Thus F_n have to determined by 'integrating' the equation $DF_n = G^2$, where $G = 0$ or an isobaric polynomial of weight q. Because of the additivity of the derivation, we have only to handle the case $G = x^\alpha y^\beta, \alpha(2j+1) + \beta(2i+1) \geq q \geq 4ij$. In this case, either $\alpha \geq i$ or $\beta \geq j$. If $\alpha \geq i$, we take $F_n = x^{2(\alpha-i)} y^{2\beta+1}$ and if $\beta \geq j$, we take $F_n = x^{2\alpha+i} y^{2(\beta-j)}$. Thus proves $(*)$ and hence also $(**)$. This gives $C_q/C_{q+1} \approx (A^{(q)} \cap A')/(A^{(q)} \cap A' \cap \underline{q}), q \geq 4ij$. Hence $C_q/C_{q+1}, q \geq 4ij$ is a k-free module of finite rank, say $n(q)$. Hence*
73 *$C(A') \approx C_{4ij-1}/C_{4ij} \oplus C_{4ij}$, where C_{4ij} is a k-free module of finite rank $N(i,j) = \sum_{q \geq 4ij} n(q)$. We now determine the integer $N(i,j)$. We observe that in A, the ideal $\underline{q}$ admits a supplement generated by the monomials*

$x^q y^b$ such that $a < 2i, b < 2j$. Since $x^{2i+1} + y^{2i+1} \in \underline{q}$, in A', the ideal $\underline{q} \cap A'$ admits a supplement generated by the monomials $x^{2a}y^{2b}$ such that $2a < 2i, 2b < 2j$. Thus $N(i, j)$ is equal to the number of monomials $x^{2a}y^{2b}$, with $0 \leq 2\alpha < 2i, 0 \leq 2\beta < 2j$ and weight of $x^{2a}y^{2b} \geq 4ij$. Hence we have the

Theorem 5.2. *Let k be a factorial ring of characteristic 2, and i, j two integers with $(2i + 1, 2j + 1) = d$. Let $A' = k[[X, Y, Z]]$, where $Z^2 = X^{2i+1} + Y^{2j+1}$. Then the divisor class group $C(A') \approx H \oplus G$, where, H is a group of type $(2, \ldots, 2)$ of order 2^f, $f \leq d - 1$; (if k contains the algebraic closure of the prime field $\mathbb{F}_2$, then H is of order 2^{d-1}); further $G \approx k^{N(i,j)}$, where $N(i, j)$ is the number of pairs of integers (a, b) with $0 \leq a < i$, $0 \leq b < j$ and $(2j + 1)a + (2i + 1)b \geq 2ij$.*

Remarks. 1) The function $N(i, j) \sim ij/2$

2) $N(i, j) = 0$ if and only if the pair $(a, b) = (i - 1, j - 1)$ does not satisfy the inequality $(2j + 1)a + (2i + 1)b \geq 2ij$, i.e. if (i, j) satisfies the inequality $2ij - i - j < 2$. This is satisfied only by the pairs (1, 1), (1, 2) and (1, 3), barring the trivial cases $i = 0$ or $j = 0$. Hence, upto a permutation the only factorial ring we obtain is, except for the trivial cases, $k[[X, Y, Z]]$, $Z^2 = X^3 + Y^5$. In view of Theorem 4.1 and Theorem 5.2, the pairs $(2i + 1, 2j + 1) \neq (3,5), (5, 3)$, for which $2i + 1$ **74**
and $2j + 1$ are relatively prime, provide examples of factorial rings whose completions are not factorial.

(c) Power series ring. Let k be a regular factorial ring of characteristic 2. Let $A = k[x, y]$ (resp. $k[[x, y]]$) and $R = A[[T]]$. We define a k-derivation $D : R \to R$ by $Dx = y^{2j}$, $Dy = x^{2i}$, $DT = 0$. Then $\operatorname{Ker} D = A'[[T]]$, where $A' = k[x^2, y^2, x^{2i+1} + y^{2j+1}]$ (Resp. $k[[x^2, y^2, x^{2i+1} + y^{2i}]]$). For a Krull ring B, let $\mathscr{L}(B)$ and $\mathscr{L}'(B)$ denote the group of logarthmic derivatives in B and the group of logarthmic derivatives of the units of B, respectively. We will compute $C(R) = \mathscr{L}(R)/\mathscr{L}'(R)$. An $F \in R$ is in $\mathscr{L}(R)$ if and only if $DF = F^2$ (since $D^2 = 0$). Let $F = \sum_n a_n T^n$. Then $F \in \mathscr{L}(R)$ if and only if $Da_o = a_o^2$, $Da_{2n+1} = 0$, $Da_{2n} = a_n^2$. Since by Lemma 5.1, $\mathscr{L}'(R) = \mathscr{L}(R) \cap \underline{q}$, where $\underline{q} = (Dx, Dy)$, we have $F \in \mathscr{L}'(R)$ if and only if $Da_o = a_o^2$, $Da_{2n+1} = 0$, $Da_{2n} = a_n^2$ and $a_n \in (Dx, Dy)$. Thus $F \in \mathscr{L}(R)$ $(resp.\ .\mathscr{L}'(R))$ implies $a_o \in \mathscr{L}(A)$ $resp.\ .a_o \in \mathscr{L}'(A))$. Further, $\mathscr{L}(R)/\mathscr{L}'(R) \approx \mathscr{L}(A)/\mathscr{L}'(A) \oplus \dfrac{\mathscr{L}(R) \cap TR}{\mathscr{L}'(R) \cap TR}$. As before we assign weights $2j+1$, $2i+1$ to x and y respectively. Let $q(n) = 0(a_n)$. Now if $F \in \mathscr{L}(R)$, then $Da_n = a_n^2$. Hence $q(2n)+q \leq 2q(n)$, where $q = 4ij-1$. That is , $q(2n)-q \leq 2(q(n)-q)$. By induction, we get $q(2^r n) - q \leq 2^r(q(n) - q)$ for $r \geq 1$. Since $q(2^r n) \geq 0$, we conclude that $q(n) \geq q$. A computation similar to that in Theorem 5.2 shows that the 'integration' of $Da_{2n} = a_n^2$ is possible. Further if $a_n \in \underline{q} = (Dx, Dy)$, then a_{2n} can be chosen in $\underline{q}$.

75 Let $A^{(q)}$ be the set of elements of order $\geq q$. In computing $F \in \mathscr{L}(R)$, each integration introduces an 'arbitrary element' of $A' \cap A^{(q)}$. In computing $F \in \mathscr{L}'(R)$, each integration introduces an arbitrary constant of $A' \cap A^{(q)} \cap \underline{q}$. Hence $(\mathscr{L}(R) \cap TR)/\mathscr{L}'(R) \cap TR$ is the product of countably many copies of $V = (A' \cap A^{(q)}/(A' \cap A^{(q)} \cap \underline{q})$. As in the last example, V is a k-free module of rank equal to the number $N(i, j)$ of pairs (a, b) with $0 \leq a < i$, $0 \leq b < j$, $(2j+1)2a + (2i+1)2b \geq q = 4ij - 1$ and this inequality is equivalent to $(2j+1)a + (2i+1)b \geq 2ij$. Hence we have the

Theorem 5.3. *Let k be a factorial ring of characteristic 2, and i, j two integers. Let $A' = k[X, Y, Z]$ (or $k[[X, Y, Z]]$) with $Z^2 = X^{2i+1} + Y^{2j+1}$. Then $C(A'[[T]])/C(A') \approx (k[[T]])^{N(i,j)}$ where $N(i, j)$ is the number of pairs (a, b) with $0 \leq a < i$, $0 \leq b < j$ and $(2j+1)a + (2i+1)b \geq 2ij$.*

Remarks. (1) Take $A' = k[x^2, y^2, x^{2i+1} + y^{2j+1}]$ with $(2i+1, 2j+1) = 1$ and $N(i, j) > 0$. Then A' is factorial, but $A'[[T]]$ is not. (We have thus to exclude only $Z^2 = X^3 + Y^5$ and trivial cases.)

(2) Let A' be the complete local ring $A' = k[[X, Y, Z]]$, $Z^2 = X^{2i+1} + Y^{2j+1}$. Then A' and $A'[[T]]$ are simultaneously factorial or simultaneously non-factorial.

(3) In general, the mapping $C(A') \to C(A'[[T]])$ is not surjective.

Appendix

The alternating group operating on a power series ring

We have seen (Chap. 3, §1) that the ring A' of invariants of the 76 alternating group A_n operating on the polynomial ring $k[x_1, \ldots, x_n]$ is factorial for $n \geq 5$. Let us study the analogous question for the power series ring $A = k[[x_1, \ldots, x_n]]$; let U be the group of units in A, m the maximal ideal of A, and A' the ring of invariants of A_n (operating by permutations of the variables). We recall (Chap. 3, §1) that $C(A') \approx H^1(A_n, U)$ since A is divisorially unramified over A'. We have already seen (Chap. 3, §1, Corollary to Proposition 1.3) that $H^1(A_n, U) = 0$ if the characteristic p of k is prime to the order of A_n, i.e. if $p > n$. Thus what we are going to do concerns only fields of "small" characteristic.

Theorem. *Suppose that $p \neq 2, 3$. Then with the notation as above, A' is factorial for $n \geq 5$. For $n = 3, 4$, $C(A')$ is isomorphic to the group of cubic roots of unity contained in k.*

Our statement means that $C(A') \approx H^1(A_n, k^*) = Hom(A_n, k^*)$. In view of the exact sequence $0 \to 1 + \mathscr{M} \to U \to k^* \to 0$, we have only to prove that $H^1(A_n, 1 + \mathscr{M}) = 0$. For this it is sufficient to prove that

$$H^1(A_n, (1 +_{\mathscr{M}} s)/(1 +_{\mathscr{M}} s + 1) = 0 \text{ for every } j \geq 1. \qquad (1)$$

In fact, given a cocycle (x_s) in $1 + \mathscr{M} (s \in A_n, x_s \in 1 + \mathscr{M})$, it is a 77 coboundary modulo $1 + \mathscr{M}^2$, i.e. there exists $y_1 \in 1 + \mathscr{M}$ such that $x_s \equiv s(y_1)y_1^{-1} \mod 1 + \mathscr{M}^2$. We set $x_{2,s} = x_s y_1 s(y_1)^{-1}$; now $x_{2,s}$ is a cocycle in $1 + \mathscr{M}^2$, and therefore a coboundary modulo $1 + \mathscr{M}^3$. By induction we find elements $y_1, \ldots, y_{j1} \cdots (y_j \in 1 + \mathscr{M}^j)$ and $x_{js} \in 1 + \mathscr{M}^j$ such that $x_{1,s} = x_s$ and $x_{j+1,s} = x_{j,s} y_j s(y_j^{-1})$. The product $\prod_{j=1}^{\infty} y_j$ converges since A is *complete*; calling y its value, we have $x_s y s(y^{-1}) = 1$ for every $s \in A_n$, which proves that (x_s) is a coboundary.

In order to prove (1), we notice that the multiplicative group $(1 + \mathscr{M}^j)/(1 + \mathscr{M}^{j+1})$ is isomorphic to the additive group $\mathscr{M}^j/\mathscr{M}^{j+1}$, i.e. to the vector space W_j of homogeneous polynomials of degree j. Our theorem is thus a consequence of the following lemma:

Lemma 1. *Let $S_n(resp. .A_n)$ operate on $k[x_1, \ldots, x_n]$ by permutations of the variables, and let W_j be the vector space of homogeneous polynomials of degree j. Then*

a) $H^1(S_n, W_j) = 0$ *if the characteristic p is $\neq 2$;*

b) $H^1(A_n, W_j) = 0$ *if* $p \neq 2, 3$

We consider a monomial $x = x_1^{j(1)} \cdots x_1^{j(n)}$ of degree j and its transforms by $S_n(resp. .A_n)$. These monomials span a stable subspace V of W_j, and W_j is a direct sum of such stable subspaces V. We need only prove that $H^1(S_n, V) = 0 (resp. .H^1(A_n, V) = 0)$. Now the distict trans-
78 forms x_θ of the monomial x are indexed by $G/H (G = S_n$ or $A_n)$, where H is the stability group of x; we have $s(x_\theta) = x_{s\theta}$ for $a \in G$. We are going to prove, in a moment, that

$$H^1(G, V) = \text{Hom}\,(H, k)\ (G = S_n \text{ or } A_n) \tag{2}$$

Let us first see how (2) implies Lemma 1. The stability subgroup H is the set of all s in S_n (or A_n) such that $\prod_i x_i^{j(i)} = x = s(x) = \prod_i x_{s(i)}^{j(i)} = \prod_i x^{j(s^{-1}(i))}$, i.e. such that $j(s^{-1}(i)) = j(i)$ for every i. Thus H is the set of all s in S_n or A_n which, for every exponent r, leave the set of indices $s^{-1}(\{r\})$ globally invariant. Denote by $n(r)$ the cardinality of $s^{-1}(\{r\})$ (i.e. the number of variables x_i having exponent r in the monomial x). In the case of S_n, H is the direct product of the groups $S_{n(r)}$; since a nontrivial factor group of $S_{n(r)}$ is necessarily cyclic of order 2, we have $\mathrm{Hom}(H,K) = 0$ in characteristic $\neq 2$; hence we get a) in Lemma 1. In the case of A_n, H is the subgroup of $\prod_r S_{n(r)}$ consisting of the elements (s_r) such that the number of indices for which $s_r \in S_{n(r)} - A_{n(r)}$ is even; thus H contains $H^1 = \prod_r A_{n(r)}$ as an invariant subgroup, and H/H^1 is a commutative group of type $(2,2,\ldots,2)$; on the other hand a nontrivial commutative factor group of $A_{n(r)}$ is necessarily cyclic of order 3 (this happens only for $n(r) = 3,4$); thus, if $p \neq 2$ and 3, who have Hom $(H,k) = 0$, and this proves b).

We are now going to prove (2). More precisely we have the following lemma (probably well known to specialists in homological algebra; probably, also, high-powered cohomological methods could make the proof less computational).

Lemma 2. *Let G be a finite group, H a subgroup of G, k a ring, V a free k-module with a basis (e_θ) indexed by G/H. Let G operate on V by $s(e_\theta) = e_{s\theta}$. Then $H^1(G,V) \approx$ Hom (H,k).* 79

A system $(v_s = \sum_{\theta\in G/H} a_{s,\theta}e_\theta)$ $(s \in G, a_{s,\theta} \in k)$ is a cocycle if and only if $v_{ss'} = v_s + s(v_{s'})$ i.e. if and only if

$$a_{ss',\theta} = a_{s,\theta} + a_{s',s^{-1}\theta}. \tag{3}$$

It is a coboundary if and only if there exists $y = \sum_{\theta\in G/H} b_\theta\, e_\theta$ such that $v_s = s(y) - y$, i.e. if and only if there exist elements b_θ of k such that

$$a_{s,\theta} = b_{s^{-1}\theta} - b_\theta. \tag{4}$$

Let ε denote the unit class H in G/H and, given a cocycle (v_s) as above, set $\varphi_v(h) = a_{h,\varepsilon}$ for h in H. Since $h\varepsilon = \varepsilon(h \in H)$, (3) shows that φ_v is a homomorphism of H into k. We obviously have $\varphi_{v+v'} = \varphi_v + \varphi_{v'}$, whence a homomorphism

$$\varphi : Z^1(G,V) \text{ (``cocycles'')} \to \text{ Hom } (H,k).$$

By (4), we see that φ is zero on the coboundaries. Conversely if $\varphi_v = 0$, we prove that (v_s) is a coboundary. In fact, for $\theta \in G/H$, choose

$t \in G$ such that $\theta = t^{-1}\varepsilon$, and set $b_\theta = a_{t,\varepsilon}$; this element does not depend on the choice of t since, if $t^{-1}\varepsilon = u^{-1}\varepsilon$, then $ut^{-1} \in H$ and $u = ht$ with $h \in H$; by (3), we have $a_{u,\varepsilon} = a_{hv,\varepsilon} = a_{h,\varepsilon} + a_{t,h^{-1}\varepsilon} = a_{t,\varepsilon}$ (since $\varphi_a = 0$).
80 Now, if $\theta = t_\varepsilon^{-1}$ and if $s \in G$, we have $s^{-1}\theta = (ts)^{-1}\theta$, whence $b_\theta = a_{t,\varepsilon}$ and $b_{s^{-1}\theta} = a_{ts,\varepsilon}$. From (3) we get $b_{s^{-1}\theta} - b_\theta = a_{ts,\varepsilon} - a_{t,\varepsilon} = a_{s,t^{-1}\varepsilon} = a_{s,\theta}$, thus proving that (v_s) is a coboundary.

Thus the proof of lemma 2 will be complete if we show that φ is surjective. Let c be a homomorphism of H into k. For every θ in G/H, we choose $t(\theta)$ in G such that $\theta = t(\theta)^{-1}\varepsilon$. Then every $s \in G$ may be written uniquely as $s = h.t(\mu)$ $(h \in H, \mu = s^{-1}H)$. We set

$$a_{s,\theta} = c(h), \tag{5}$$

where h is the unique element of H such that $t(\theta) \cdot s = h.t(s^{-1}\theta)$ (notice that $t(\theta).s.t(s^{-1}\theta)^{-1}.\varepsilon = t(\theta)s.s^{-1}\theta = t(\theta).\theta = \varepsilon$, whence $t(\theta).s.t(s^{-1}\theta)^{-1} \in H$). Let us verify the "cocycle condition" (3). We have $a_{ss',\theta} = c(h), a_{s,\theta} = c(h_1)$ and $a_{s',s^{-1}\theta} = c(h_2)$, with $t(\theta)ss' = h.t(s'^{-1}s^{-1}\theta)$, $t(\theta)s = t(\ )s = h_1 t(s^{-1}\theta)$ and $t(s^{-1}\theta).s' = h_2 t(s'^{-1}s^{-1}\theta)$. From this we immediately deduce that $h = h_1 h_2$. Since c is a homomorphism, we have $c(h) = c(h_1) + c(h_2)$, i.e. $a_{ss'}, \theta = a_{s,\theta} + a_{s' s^{-1}\theta}$. Thus $v_s = \sum_\theta a_s \theta e_\theta$ is a cocycle. For this cocycle, we have (for $h \in H)\varphi_v^\theta(h) = a_{h,\varepsilon} = c(h_1)$, where, by (5), h_1 is such that $t(\varepsilon).h = h_1 t(h^{-1}\varepsilon) = h_1 t(\varepsilon)$; since the additive group of k is commutative, we have $c(h) = c(h_1)$, whence $\varphi_v(h) = c(h)$ for every $h \in H$. Q.E.D