INSTITUTUL
DE
MATEMATICA

INSTITUTUL NATIONAL
PENTRU CREATIE
STIINTIFICA SI TEHNICA

ISSN 0250 3638

COMMUTATIVE RINGS HAVING ONLY A FINITE NUMBER OF IDEALS

by

Horia POP

PREPRINT SERIES IN MATHEMATICS

No.48/1981

BUCURESTI

COMMUTATIVE RINGS HAVING ONLY A FINITE NUMBER OF IDEALS

by

Horia POP *)

June 1981

*) Department of Mathematics, National Institute for Scientific and Technical Creation, Bd. Pacii 220, 79622 Bucharest, Romania

COMMUTATIVE RINGS HAVING ONLY A FINITE NUMBER OF IDEALS

by

Horia POP

INTRODUCTION

This paper tries to describe all commutative unitary rings having only a finite number of ideals, providing also an simplified proof of I.S.Cohen's Structure Theorems for artinian local rings.

The condition to have only a finite number of ideals for a local artinian ring is that either the ring is finite or else his maximal ideal is principal.

If both conditions are satisfied and the characteristic of the residual field is unramified, then, in some way the ring looks like finite fields.

Since in ann artinian local ring $(A,\underline{m})$, its $\underline{m}$-adic topology is discrete we can get an easy proof of I.S.Cohen's Structure Theorems.

The ideas and techniques leading to structure theorems for complete discrete valuation rings belong F.K.Schmidt, H.Hasse, E.Witt and O. Teichmüller.

The new problems which appeared for an arbitrary local ring were overcomed by I.S.Cohen in [3].

For artinian rings some simplification are available.

In the equal characteristic case (i.e. char (A)= char $(A/\underline{m})$) we use an elementary polynomial trick instead of Hensel's lemma. One semiplifies also A.Geddes' argument (see [7], chap.7, §12,

which didn't use p-bases) by finding the field of representatives not using projective limits, but simply using Zorn's lemma.

In unequal characteristic case (i.e. char $(A)=p^n$ with $n>1$, and char $(A/\underline{m})=p$) the proof use Teichmüller techniques to find a multiplicative system of representatives for a perfect residual field. If the residual field is not perfect, the remark that Teichmüller process works for a subfield k^{p^n} of k make the problem easier in the sense that we need not to embed the ring in a larger one with perfect residue field (as [3] and [5]).

PRELIMINARIES

Let A be an artinian ring. Then A is noetherian, every prime ideal of A is maximal, and the number of maximal ideals is finite.

By the structure theorem for artinian rings one can write A as a finite direct product of artinian local rings (see [2] chap.8). This is the reason for considering from now on only local artinian rings.

Denote by $\underline{m}$ the maximal ideal in an artinian local ring A. As the prime radical of A is $\underline{m}$ one can write $\underline{m}=(x_1,\dots x_n)$ with $x_i^{n_i}=0$ for suitable $n_i>0$.

If A has a unique nontrivial ideal one has $\underline{m}=(x)$ for every $x\in\underline{m}$; moreover $x^2=0$ because $\underline{m}=\underline{m}^2\neq 0$ implies by Nakayama's lemma $\underline{m}=0$.

Assuming that the characteristic of A is $n\neq 0$ and writing $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}\in\underline{m}$ with p_i prime it follows that there is an i such that $p_i\in\underline{m}$ and p_i must be nilpotent.

Therefore char (A) is of one of the following forms 0, p or p^n with p prime.

PROPOSITION 1. Let $(A,\underline{m})$ be a local ring with a finite number of ideals. Then either the residual field $A/\underline{m}$ is finite and in this case A is itself finite, or its maximal ideal is principal, in which case all ideals of A are powers of $\underline{m}$.

PROOF. Using Nakayama's lemma one can choose a minimal system of generators $(x_1,x_2,\ldots,x_n)$ for $\underline{m}$ (which is a basis of $\underline{m}/\underline{m}^2$ over $A/\underline{m}$).

If $A/\underline{m}$ is finite then A is finite.

If $A/\underline{m}$ is infinite and m is not principal, consider the ideals of the form $(x_1+ax_2)+\underline{m}^2$ where a runs over an infinite set of representatives for the residual fields. Their images in $\underline{m}/\underline{m}^2$ are distinct because ortherwise we obtain a dependence relation of x_1 and x_2 in $\underline{m}/\underline{m}^2$ over $A/\underline{m}$, a contradiction.

If $\underline{m}$ is principal all the ideals are powers of $\underline{m}$ (see [2], chap.8)

Q.E.D.

Now we give a polynomial version of Hensel's lemma.

LEMMA 1. Let $P(X)$ be an irreducible separable polynomial over a field k. Then for every $n\geq 1$ there is a polynomial $\varphi_n(X)$ such that

$$P^n(X)/P(\varphi_n(X))$$

PROOF. Because $P(X)$ and $P'(X)$ are relatively prime each other one can find $Q(X)$, $R(X) \in k[X]$ such that $Q(X)P(X)+R(X)P'(X)=1$.

Set $U(X)=R(X)P(X)$ and $\varphi(X)=X-U(X)=X-R(X)P(X)$.

Then by Tayler expansion

$$P(\varphi(X))=P(X)-U(X)P'(X)+U^2(X)P_1(X)=$$
$$=P(X)(1-P'(X)R(X))+P^2(X)R^2(X)P_1(X)=$$
$$=P^2(X)(Q(X)+R^2(X)P_1(X))=P^2(X)V(X).$$

Repeating this argument with $\varphi(X)$ instead of X . We get

$$P(\varphi(\varphi(X)))=P^2(\varphi(X))V(\varphi(X))$$

and iterating n-times one gets

$$P(\varphi_n(X)=P^{2^n}(X)V^{2^{n-1}}(X)\ldots V(\varphi_{n-1}(X))$$

where

$$\varphi_n=\underbrace{\varphi\circ\varphi\circ\ldots\circ\varphi}_{n}$$

Q.E.D.

COROLLARY. For any irreducible separable polynomial $P(X)$ over a field k we have an isomorphism

$$k[X]/(P^n(X))\simeq K[T]/(T^n)$$

where $K=k(z)$ with z a root of $P(X)$.

PROOF. Using the above lemma set $z=\varphi(X)$ such that $P^n(X)/P(\varphi(X))$ then z is a root of $P(X)$ in $k[X]/(P^n(X))$ and $k[z]$ is a field.

If $K=k(z)$ and $y=P(X)$ then $y^n=0$ and

$$k[X]/(P^n(X)) = K[y]\simeq K[Y]/(y^n)$$

Q.E.D.

LEMMA 2. If the prime number p is in $\underline{m}$ and $a \equiv b \pmod{\underline{m}}$, then $a^{p^n} \equiv b^{p^n} \pmod{\underline{m}^{n+1}}$.

PROOF. For n=0 there is nothing to prove. If $a \equiv b \pmod{\underline{m}^k}$, $a=b+x$ with $x \in \underline{m}^k$ and one has

$$a^p = b^p + \sum_1 \binom{p}{l} x^l b^{p-l} = b^p + pxy$$

where $px \in \underline{m}^{k+1}$

so that $a^p \equiv b^p \pmod{\underline{m}^{k+1}}$.

Iterating this several times one gets the lemma.

RESULTS

For our purposes it is necessary to find "good" representatives for the residual field $A/\underline{m}$ of A.

The answer is given by the following two theorems, due to H.Hasse, F.K.Schmidt, E.Witt, O.Teichmüller in complete discrete valuation rings and to I.S.Cohen for complete local rings. If A is artinian we give direct and simplified proofs of these two results.

THEOREM 1. Let A be an artinian ring of characteristic 0 or p for a prime p. Then A contains a field of representatives for the residual field k which is isomorphic to k via the restriction of the canonical homomorphism $A \to A/\underline{m}$.

PROOF. If the characteristic of A is 0 one has

$\mathbb{Z} \subset A - \underline{m}$ so that $\mathbb{Q} \subset A$.

If the characteristic of A is p and $\underline{m}^1=0$, A^{p^1} is a subring in A and actually is a field because any element of A not invertible is in $\underline{m}$ and $\underline{m}^{p^1}=0$.

By Zorn's lemma one can find a maximal field K in A containing $\mathbb{Q}$ if char(A)=0 else containing A^{p^1} if char(A)=p.

Denote by $\bar{x}$ the image of $x\in A$ in $A/\underline{m}$.

If $\bar{K}\neq k$ take x a representative for an element $\bar{x}\in k-\bar{K}$.

If $\bar{x}$ is transcendental over $\bar{K}$ then x is transcendental over K so that $K\subset K(x)$ and this contradicts the maximality of K.

If $\bar{x}$ is algebraic over $\bar{K}$ then for some irreducible $0\neq P(X)\in k[X]$ one has $\bar{P}(\bar{x})=0$, it follows $P(x)\in\underline{m}$ and then $P^1(x)=0$.

If the characteristic of A is 0, P(X) is separable and by Corollary to lemma 1 one can find a root y of P(X) in A. Then $K\subset K[y]\subset A$ and this contradicts the maximality of K.

If the characteristic of A is p there is a minimal e such that $x^{p^e}\in K$ (because $K\supset A^{p^e}$).

Let $\alpha=x^{p^e}$ then $\alpha\notin K^p$ and $X^{p^e}-\alpha\in K[X]$ is irreducible.

Again the inclusion $K\subset K(x)$ contradicts the maximality of K.

Therefore K is a system of representative for k and K=k.

Q.E.D.

Recall that a p-basis in a field k of characteristic p is a set of elements M such that

1. $[k^p(x_1,\ldots,x_n):k^p]=p^n$ for any distinct $x_1,\ldots,x_n\in M$

2. $k=k^p(M)$.

By Zorn's lemma a p-basis always exists.

Moreover $k=k^{p^n}(M)$

The ring A is said to be unramified if $p\in\underline{m}-\underline{m}^2$ for $p=\mathrm{char}(A/\underline{m})$

Now we shall use Teichmüller embedding process (see [4] chap.6)

to deal with the unequal-characteristic case.

THEOREM 2. Let A be an unramified artinian local ring with maximal ideal $\underline{m}$ and residual field $A/\underline{m}=k$. Denote by n the smallest natural number such that $\underline{m}^{n+1}=0$.

a) For $K=k^{p^n}$ there is a unique multiplicative system of representatives in A^{p^n}. If the characteristic of A is p then this system is a subfield of A.

b) If the residual field is perfect we know by a) that there is a unique multiplicative system of representatives for k. Moreover if the characteristic of A is p^r $(r>1)$ the ring generated by this system over $\mathbb{Z}/p^r\mathbb{Z}$ is isomorphic to the ring of truncated Witt vectors $W_r(k)$ and this is a minimal subring of A containing a system of representatives for k.

c) If the residual field k is not perfect a system of representatives for the residual field may be obtained in the following way: consider a set M of representatives for a p-basis of k and the multiplicative system of representatives $f(k^{p^n})$ for k^{p^n} given by a). The ring generated by $f(k^{p^n})\cup M$ over $\mathbb{Z}/p^r\mathbb{Z}$ contains a system of representatives for k (i.e. a coefficient ring for k which we shall denote again by $W_r(k)$).

PROOF. For $a\in k^{p^n}$ take α a representative for $a^{p^{-n}}\in k$ and construct $f:k^{p^n}\longrightarrow A$ by $f(a)=\alpha^{p^n}$.

This does not depend on the representative chosen because if β is another representative for $a^{p^{-n}}$ we have $\alpha\equiv\beta \pmod{\underline{m}}$ so by lemma 2 $a^{p^n}\equiv b^{p^n} \pmod{\underline{m}^{n+1}}$ and $\underline{m}^{n+1}=0$.

Denoting by $-$ the natural homomorphism $A\longrightarrow A/\underline{m}$ one has

$$\overline{f(a)}=\overline{\alpha}^{p^n}=(a^{p^{-n}})^{p^n}=a$$

and

$$f(a).f(b)=\alpha^{p^n}\cdot\beta^{p^n}=(\alpha\beta)^{p^n}=f(ab)$$

Thus $f(k^{p^n})$ is a multiplicative system of representatives for k^{p^n}.

Remark that $f(k^{p^n})\subset A^{p^n}$, and A^{p^n} is not necessarily a subring of A.

If $g:k^{p^n}\longrightarrow A$ is another multiplicative system of representative for k^{p^n} in A^{p^n} using lemma 2 we get

$$g(a)=\beta^{p^n} \quad \text{because } f(k^{p^n})\subset A^{p^n}$$

and $f(a)=\alpha^{p^n}$ so $\overline{g(a)}=\overline{f(a)}$ implies $\overline{\beta}^{p^n}=\overline{\alpha}^{p^n}$ in k so $\overline{\beta}=\overline{\alpha}$ then $\beta^{p^n}\equiv\alpha^{p^n} \pmod{\underline{m}^{n+1}}$ and $\underline{m}^{n+1}=0$.

It follows $f(a)=g(a)$ such that the system is unique.

If the characteristic of A is $p>0$ we have

$$f(a)+f(b)=\alpha^{p^n}+\beta^{p^n}=(\alpha+\beta)^{p^n}=f(a+b)$$

so that $f(k^{p^n})$ is actually a field.

Assume now that k is perfect. Then $k=k^p=k^{p^n}$ so by a) we have a multiplicative system of representatives for k.

Considering now the set of elements of type

$$x=\sum_{i=0}^{r-1} f(x_i)p^i, \qquad x_i\in k.$$

We shall prove by an inductive argument (examining addition and multiplication) that they form a ring whose structure is uniquely determined by k and the characteristic p^r.

In both cases of addition and multiplication it would be

necessary to know who is $f(a)+f(b)$ (namely to find for it an expansion $\sum_{i=0}^{r-1} f(x_i)p^i$).

We have

$$f(a)+f(b)=\alpha^{p^n}+\beta^{p^n}=(\alpha+\beta)^{p^n}-\sum_{s=1}^{p^n-1}\binom{p^n}{s}\alpha^s\beta^{p^n-s}=$$
$$=f(a+b)-\sum_{t=1}^{n-1}p^{n-t}\Big(\sum_{(h,p)=1}\frac{1}{p^{n-t}}\binom{p^n}{hp^t}\cdot\alpha^{hp^t}\beta^{p^n-hp^t}\Big)$$

because

$p^n/\binom{p^n}{s}$ if $(s,p)=1$ and $p^{n-t}/\binom{p^n}{hp^t}$ if $(h,p)=t$. Note also that p^r/p^{n+1} and set

$$c_{t,n}=\frac{1}{p^{n-t}}\binom{p^n}{np^t}\in\mathbb{Z}.$$

Then

$$f(a)+f(b)=f(a+b)+\sum_t p^{n-t}\sum_u c_{t,h}f(a^{p^{n-u}hp^t})\cdot f(b^{p^{n-u}})^{p^n-hp^t}=$$
$$=f(a+b)+\sum_t p^{n-t}u_t$$

where

$$u_t=\sum_u c_{ht}f(x_{ht}),\qquad x_{ht}=a^{\frac{hp^t}{p^u}}b^{\frac{p^u-hp^t}{p^u}}$$

Now iterate this rule for addition inside the sum representing u_t and remark that we need a fewer number of coefficients (because we have factors p^{n-t} and $p^{n+1}=0$). After at most n steps we get the expansion for $f(a)+f(b)$.

Since $f(a).f(b)=f(ab)$ using the rule above the multiplication can be obtained also inductively. Therefore the element of the type $\sum_i f(x_i)p^i$ form a subring of A of characteristic p^r whose residual field is $f(k)\cong k$ and this is the ring generated by $f(k)$ over $\mathbb{Z}/p^r\mathbb{Z}$. Such a ring could be obtained also as the ring of truncated

Witt vector $W_r(k)$ so we may suppose

$W_r(k) \subset A$ (by the isomorphism $\mathbb{Z}/p^r\mathbb{Z}[f(k)] \simeq W_r(k)$).

If k is not perfect take $\overline{M}$ a p-basis for k and M any set of representatives for $\overline{M}$ in A.

Denote by $B=\mathbb{Z}/p^r\mathbb{Z}\left[f(k^{p^n}) \cup M\right] \subset A$.

First we show that this subring is concordant with A i.e.

$B \underline{m} = p.B$

Take

$$x=\sum u_n f(a_n) x_1^{n_1} \dots x_k^{n_k} \in \underline{m} \cap B$$

$a_i \in k^{p^n}$, $x_i \in M$, $u_i \in \mathbb{Z}/p^r\mathbb{Z}$ and $n_i \leq p^n-1$

Then in $A/\underline{m}$ we have

$\overline{x} = \sum \overline{u}_n a_n \overline{x}_1^{n_1} \dots \overline{x}_k^{n_k} = 0$ and, because $\overline{M}$ is a p-basis $\overline{u}_n=0$ and therefore $u_i \in p\mathbb{Z}/p^r\mathbb{Z}$ and $x \in pB$.

Next any element $x \in k$ has a representative of the type $\sum u_n f(a_n) x_1^{n_1} \dots x_k^{n_k}$ with $a_i \in k^{p^n}$, $x_i \in M$ because $k=k^{p^n}(M)$ so that this subring is in fact a ring of coefficients.

Q.E.D.

This subring actually has Witt vectors addition and multiplication being a subring of $W_r(k^{p^{-\infty}})$ were $k^{p^{-\infty}} = \cup k^{p^{-n}}$ is the perfect closure of k.

Now we give the structure theorem.

THEOREM 3. If (A,m) is an artinian local ring of characteristic 0 or p, with residual field k there A is isomorphic to a factor ring of

$$k\left[X_1, \dots, X_s\right] / (X_1^{n_1}, \dots, X_s^{n_s})$$

If A has characteristic p^r and is unramified then A is isomorphic to a factor ring of

$$W_r(k)[X_1,\dots,X_s]/(X_1^{n_1},\dots,X_s^{n_s}).$$

PROOF. By theorems 1 and 2 one may suppose that $k\subset A$ (in the equal-characteristic case) or $W_n(k)\subset A$ (in the unequal - characteristic case).

Take $m=(x_1,\dots,x_s)$ we know that there are $n_i>0$ with $x_i^{n_i}=0$ and the proof is obvious.

Q.E.D.

COROLLARY. Let A be a ring with a unique nontrivial ideal and residual field k. Then:

a) A is isomorphic to $k[X]/(X^2)$ if char(A)=0 or p

b) A is isomorphic to $W_2(k)$ it char(A)=p .

If the residual field is finite $\mathbb{F}_q$ then $A\simeq \mathbb{Z}/p^2\mathbb{Z}(\xi)$ for ξ a q-1 primitive root of 1 over $\mathbb{Z}/p^2\mathbb{Z}$.

PROOF. Indeed p is unramified because $m^2=0$ so Theorem 3 works. If $\mathbb{F}_q=\mathbb{F}_p(\bar{\xi})$ with $\bar{\xi}$ a q-1 primitive root of 1 select ξ a representative for $\bar{\xi}$ and replace it by $\xi+p\xi^k$ if necessary

Q.E.D.

Consider from now on A a commutative ring having only a finite number of ideals, by the structure theorem of artinian rings we can restrict ourselves to the case were A is local.

The characteristic of A is 0, p or p^n (for a prime p).

We have seen (proposition 1) that A is eiter finite or else the maximal ideal of A is principal m=(x) and all the ideal of A are:

$$A\supset m\supset\dots\supset m^n=0$$

From now on asum that $\underline{m}=(x)$ is principal.

In this special case if $\underline{m}=(p)$, A is unramified, else $(p)=(x^e)$ with $e>1$ and e is called the ramification index of p.

The residual field k, char(A), the number of ideals, and the ramification index e are in general not enough to determine the ring A as shows the following example:

$A_1 = \mathbb{Z}/5\mathbb{Z}[X]/(X^3, X^2-3)$

$A_2 = \mathbb{Z}/5\mathbb{Z}[X]/(X^3, X^2-6)$

$A_1 \not\simeq A_2$ because $3 \in A_1^2$, but $3 \notin A_2^2$

THEOREM.4. Let $(A,\underline{m})$ be a local ring of residual field $k=A/\underline{m}$. Assume that $\underline{m}=(x)$ is principal. Then:

a) If the characteristic of A is 0 or p (p prime) A is isomorphic to $k[X]/(X^n)$

b) If the characteristic of A is p^n with $n>1$, p prime then A is isomorphic to $W_n(k)$ if p is unramified and to an Eisenstein extension of type

$$W_n(k)[X]/(X^e+pa_{e-1}X^{e-1}+\ldots+pa_o),\ a_o \not\equiv 0 \pmod{\underline{m}}$$

if p is ramified.

PROOF. In case a) by theorem 1, $k \subset A$. Since $m=(x)$, $x^n=0$ any element $y \in A$ can be written as

$$y=a_0+a_1x+\ldots+a_{n-1}x^{n-1} \quad \text{with } a_i \in k$$

so $A \simeq k[X]/(X^n)$.

If $\text{char}(A)=p^n$ one may assume $W_n(k) \subset A$.

If p is not ramified $\underline{m}=(p)$ and for any element $y \in A$

$$y=a_o a_1 p+\ldots+a_{n-1}p^{n-1}, \qquad a_i \in W_n(k)$$

so that $A=W_n(k)$.

If $(p)=(x^e)$ we have $x^e=\alpha p$, α invertible in A. Because any $y \in A$ can be written as

$$y=a_o+a_1 x+\ldots+a_{n-1}x^{n-1} \quad \text{in particular}$$

$\alpha=\alpha_o+\alpha_1 x+\ldots+\alpha_{n-1}x^{n-1}$ with $\alpha_o \not\equiv o \pmod{\underline{m}}$ because α is invertible.

Substituting now the expansion of α in the relation $x^e=p\alpha$ and replacing the power of x greater than e by the same relation $x^e=p\alpha$ we get

$$x^e=pa_{e-1}x^{e-1}+pa_{e-2}x^{e-2}+\ldots+pa_o$$

so x is a root of an Eisenstein polynomial.

Q.E.D.

COROLLARY. If $(A,\underline{m})$ is an unramified local artinian ring with $m=(x)$ and finite residual field $\mathbb{F}_q$ (by the previous theorem isomorphic to $W_n(\mathbb{F}_q)$) one has

$$A \simeq \mathbb{Z}/p^n\mathbb{Z}(\xi)$$

with ξ a q-1 primitive root of 1 over $\mathbb{Z}/p^n\mathbb{Z}$.

PROOF. If $\mathbb{F}_q=\mathbb{F}_p(\bar{\xi})$, with $\bar{\xi}$ a q-1 primitive root of 1 take ξ a representative of $\bar{\xi}$. The order of ξ must be divisible by q-1, thus replacing eventually ξ by one of its powers we may suppose a q-1 root of 1.

B I B L I O G R A P H Y

1. E.Artin - Algebraic Numbers and Algebraic Functions, Gordon and Breach, 1967.

2. M.Atiyah, I.Mc.Donald - Introduction to Commutative Algebra, Addison-Wesley, 1969.

3. I.S.Cohen - On the structure and ideal theory of complete local rings, Trans.Amer.Math.Soc.59,(1946), pp.54-106.

4. M.Greenberg-Lectures on forms in many variables, W.A.Benjamin, 1969.

5. S.MacLane - Subfields and automorphism groups of p-adic fields, Ann.of Math.vol.40(1939), pp.423-442.

6. J.P.Serre - Corps locaux, Hermann, 1962.

7. O.Zariski, P.Samuel - Commutative algebra, D.van Nostrand, 1958.