Jean Fresnel, le 14 août 2013

Exemples peu classiques d'anneaux principaux

0. Introduction

Si A est la clôture intégrale de l'anneau $\mathbb{Z}$ des entiers dans une extension finie du corps $\mathbb{Q}$ des rationnels, on dira que A est l'anneau des entiers d'un corps de nombres. On sait alors que A est un anneau de **Dedekind** , que $A^\times$ le groupe des inversibles de A est de type fini et que pour tout idéal $\mathfrak{a}$ de A avec $\mathfrak{a}\neq\{0\}$, on a $\frac{A}{\mathfrak{a}}$ qui est fini.

En 1964 **Oscar Goldman** [G] a montré que pour tout entier $n\geq 1$, il existe un anneau de **Dedekind** A tel que le groupe $A^\times$ des inversibles de A est de type fini, que pour tout idéal non nul $\mathfrak{a}$ de A l'anneau quotient $\frac{A}{\mathfrak{a}}$ est fini et enfin que le corps des fractions de A est une extension de $\mathbb{Q}$ dont le degré de transcendance est n .

On s'intéresse ici à la situation où A est un anneau principal. On sait peu de choses sur les anneaux d'entiers d'un corps de nombres qui sont principaux ([N] , p. 37) . Par exemple on ne sait pas s'il existe une infinité d'anneaux principaux dont le corps des fractions est une extension quadratique réelle de $\mathbb{Q}$. De même existe-t-il des anneaux d'entiers de corps de nombres qui sont principaux et dont le corps des fractions est de degré sur $\mathbb{Q}$ aussi grand que l'on veut.

Ici nous montrons que pour tout entier $n\geq 1$, il existe un anneau principal A tel que le groupe $A^\times$ des inversibles de A est de type fini, que pour tout $a\in A-\{0\}$, l'anneau $\frac{A}{aA}$ est fini et enfin que le corps des fractions de A est une extension de $\mathbb{Q}$ dont le degré de transcendance est n (corollaire 1 du théorème 1).

En caractéristique $p\geq 0$, on a le même type de résultats (corollaire 1 du théorème 1).

Le second sujet abordé dans cette note est suscité par le résultat qui suit. On sait que si A est un anneau euclidien et si le groupe $A^\times$ des inversibles de A est fini, alors pour tout $a\in A-\{0\}$, l'anneau quotient $\frac{A}{aA}$ est fini.

Si A est un anneau principal de caractéristique nulle, on sait que si $A^\times$ est fini, alors $A^\times$ est cyclique d'ordre 2 , 4 , ou 6 (lemme 3) . Ici nous montrons qu'il existe un anneau principal A dont le groupe des inversibles est cyclique d'ordre 2 (resp. 4 , 6) et pour lequel il existe $a\in A-\{0\}$ de façon que l'anneau $\frac{A}{aA}$ soit infini (corollaire 2 du théorème 2).

On a le même résultat en caractéristique $p>0$ et pour tout groupe cyclique dont l'ordre est de la forme $p^\alpha-1$ (corollaire 2 du théorème 2). .

1. Exemples d'anneaux principaux avec groupe des inversibles de type fini et anneaux résiduels finis

Théorème 1 *Soient A un anneau principal, K son corps des fractions. On suppose que le groupe $A^\times$ des inversibles de A est de type fini et que pour tout irréductible p de A, le corps $\frac{A}{pA}$ est fini. Soient $A[X]$ l'anneau des polynômes de la variable X, à coefficients dans A, $K(X)$ le corps des fractions rationnelles de la variable X à coefficients dans K. Alors il existe un sous-anneau S de $K(X)$ avec les propriétés suivantes.*

1. *On a $A[X]\subset S\subset K(X)$ et donc $\mathrm{Fr}S=K(X)$.*
2. *L'anneau S est un anneau principal. Soient $\mathcal{R}$ un système de représentants des irréductibles de $A[X]$ modulo $A[X]^\times=A^\times$, $\mathrm{Max}S$ l'ensemble des idéaux maximaux de S, alors il existe une bijection $u:\mathcal{R}\to\mathrm{Max}S$ telle que pour tout $t\in\mathcal{R}$ on a $t\in u(t)$.*
3. *Si $A^\times$ (resp. $S^\times$) désigne le groupe des inversibles de A (resp. S), alors $A^\times=S^\times$.*
4. *Pour tout irréductible π de S, le corps $\frac{S}{\pi S}$ est fini.*

Démonstration

Soit $\mathcal{P}$ un système de représentants des irréductibles de A modulo $A^\times$.

0) *Si $\mathcal{P}$ est fini, alors A est un corps fini, ainsi $S:=A[X]$ convient.*

Comme $A^\times$ est de type fini, il suit alors que $K^\times$ est de type fini ; on sait alors que K est un corps fini (Fr, ex. 3.8.17, p. 180). Il suit facilement que $A=K$.

On suppose désormais que $\mathcal{P}$ est infini.

1) *L'anneau A est dénombrable.*

Montrons cela. Soit $\mathcal{P}$ un système de représentants des irréductibles de A modulo $A^\times$. Montrons que $\mathcal{P}$ est dénombrable. Soit $m\geq 1$ un entier et $\mathcal{P}_m:=\{p\in\mathcal{P}\mid \mathrm{card}(\frac{A}{pA})\leq m\}$, montrons que l'ensemble $\mathcal{P}_m$ est fini. En effet, soient $a_0,a_1,\ldots,a_m\in A$ des éléments distincts, $c:=\prod_{0\leq i<j\leq m}(a_i-a_j)$, $\rho_p:A\to\frac{A}{pA}$ est la surjection canonique. Si $p\in\mathcal{P}_m$ on a donc $\rho_p(c)=0$. Cela veut dire que $p\mid c$; comme A est principal et que $c\neq 0$, il existe seulement un nombre fini d'éléments $p\in\mathcal{P}$ qui divisent c. Ainsi $\mathcal{P}_m$ est fini. Comme pour tout $p\in\mathcal{P}$, on sait que $\frac{A}{pA}$ est fini, on a bien $\mathcal{P}=\bigcup_{m\geq 1}\mathcal{P}_m$, ce qui montre que $\mathcal{P}$ est dénombrable.

Sachant que $A^\times$ est un groupe abélien de type fini, il suit que $A^\times$ est dénombrable et sachant que A est principal, il suit que A est dénombrable.

2) *Soit* $A[X]^\times = A^\times$ *le groupe des inversibles de* $A[X]$. *Alors l'ensemble des irréductibles de* $A[X]$ modulo $A[X]^\times$ *est dénombrable.*

Soit $\mathfrak{Q}$ un système de représentants modulo le groupe $A[X]^\times = A^\times$, des polynômes $f \in A[X]$, qui sont des irréductibles de $K[X]$, de contenu 1, on rappelle que tout élément $a \in K - \{0\}$ s'écrit de façon unique sous la forme $a = \varepsilon(a) \prod_{p \in \mathcal{P}} p^{v_p(a)}$ où $v_p(a) \in \mathbb{Z}$ et $v_p(a) = 0$ pour tout $p \in \mathcal{P}$, sauf un nombre fini et $\varepsilon(a) \in A^\times$, de plus on définit $v_p(0)$ par $v_p(0) = \infty$; si $f(X) = \sum_i a_i X^i \in K[X]$, le contenu de f est défini par $\operatorname{cont} f := \prod_{p \in \mathcal{P}} p^{\alpha(p)}$ où $\alpha(p) := \min_i v_p(a_i)$. Alors on sait que $\mathcal{P} \cup \mathfrak{Q}$ est un système de représentants des irréductibles de $A[X]$ modulo $A[X]^\times = A^\times$. Comme A est dénombrable, il en est de même de $A[X]$, il suit que $\mathcal{P} \cup \mathfrak{Q}$ est dénombrable, ainsi il existe une bijection $i \mapsto t_i$ de $\mathbb{N}$ sur $\mathcal{P} \cup \mathfrak{Q}$.

3) *Il existe une suite* $(\mathfrak{m}_k)_{k \geq 1}$ *d'idéaux maximaux de* $A[X]$ *avec la propriété que* $t_n \in \mathfrak{m}_n$ *pour tout* $n \geq 0$ *et que* $t_0 t_1 \ldots t_{n-1} \notin \mathfrak{m}_n$ *pour tout* $n \geq 1$ (*l'élément* t_n *est défini en* 2)).

On peut décrire les idéaux maximaux $\mathfrak{m}_n$ *de façon plus précise.*

On rappelle que $\mathcal{P}$ *est un système de représentants des irréductibles de* A modulo $A^\times$ *et que* $\mathfrak{Q}$ *est un système de représentants modulo le groupe* $A[X]^\times = A^\times$, *des polynômes* $f \in A[X]$, *qui sont des irréductibles de* $K[X]$, *de contenu* 1 .

Si $p \in \mathcal{P}$, *on note* $\rho_p : A \to \frac{A}{pA}$ *la surjection canonique, on note aussi* $\rho_p : A[X] \to \frac{A}{pA}[X]$ *la surjection définie par* $\rho_p(\sum_i a_i X^i) := \sum_i \rho_p(a_i) X^i$.

3.1) *Si* $t_0 = p \in \mathcal{P}$, i.e. *un irréductible de* A, *alors on définit* $\mathfrak{m}_0$ *par* $\mathfrak{m}_0 := pA[X] + XA[X]$.

3.2) *Si* $t_0 = f \in \mathfrak{Q}$; i.e. *un irréductible de* $K[X]$ *avec* $\operatorname{cont} f = 1$, *on définit* $\mathfrak{m}_0$ *par* $\mathfrak{m}_0 := pA[X] + hA[X]$, *on choisit* $p \in \mathcal{P}$ *de façon que* $\deg f = \deg \rho_p(f)$, *que* $\rho_p(f)$ *soit séparable et on choisit* h *de façon que* $\rho_p(h) \mid \rho_p(f)$ *dans* $\frac{A}{pA}[X]$ *et que* $\rho_p(h)$ *soit un irréductible de* $\frac{A}{pA}[X]$.

Si $t_0 t_1 \ldots t_{n-1} = p_1 p_2 \ldots p_s f_1 f_2 \ldots f_r$ *où* $p_i \in \mathcal{P}$ *et les* $f_i \in \mathfrak{Q}$ $(s + r = n)$.

3.3) *Si* $t_n = p \in \mathcal{P}$, *on définit* $\mathfrak{m}_n$ *par* $\mathfrak{m}_n := pA[X] + hA[X]$ *avec* h *unitaire de façon que* $\rho_p(h)$ *soit un irréductible de* $\frac{A}{pA}[X]$, *que* $\rho_p(h)$ *soit séparable et que* $\rho_p(h) \nmid \rho_p(f_1 f_2 \ldots f_r)$.

3.4) *Si* $t_n = f \in \mathfrak{Q}$, *on définit* $\mathfrak{m}_n$ *par* $\mathfrak{m}_n := pA[X] + hA[X]$. *Soit* $F = f_1 f_2 \ldots f_r$, *on choisit* $p \in \mathcal{P}$ *de façon que* $p \notin \{p_1, p_2, \ldots, p_s\}$, *que* $\rho_p(F)$ *soit séparable et que* $\rho_p(f)$ *soit séparable et on choisit* h *tel que* $\rho_p(h)$ *soit un irréductible de* $\frac{A}{pA}[X]$, *que* $\rho_p(h) \mid \rho_p(f)$ *et que* $\rho_p(h) \nmid \rho_p(F)$.

Le choix de $\mathfrak{m}_0$ en 3.1) et 3.2) ne présente pas difficultés.
Pour 3.3), il suit de la définition de t_n que $p \notin \{p_1, p_2, \dots, p_s\}$, par ailleurs le choix de h ne présente pas de difficultés non plus. On a bien $t_n = p \in \mathfrak{m}_n$. Il reste à montrer que $t_0 t_1 \dots t_{n-1} \notin \mathfrak{m}_n$. Sinon on aurait $\rho_p(t_0 t_1 \dots t_{n-1}) = \rho_p(p_1 p_2 \dots p_s)\, \rho_p(f_1 f_2 \dots f_r) \in \rho_p(\mathfrak{m}_n) = \rho_p(h)\frac{A}{pA}[X]$. Comme $\rho_p(p_1 p_2 \dots p_s) \neq 0$, cela impliquerait que $\rho_p(h) \mid \rho_p(f_1 f_2 \dots f_r)$ dans $\frac{A}{pA}[X]$, ce qui est contraire à la définition de h.
Pour 3.4) Comme $t_n \notin \{t_0, t_1, \dots, t_{n-1}\}$, on a $f \nmid f_1 f_2, \dots f_r =: F$ dans $A[X]$ et d'autre part F est sans facteur multiple, i.e. $\operatorname{res}(F, F') \neq 0$. Ainsi pour tout $p \in \mathcal{P}$, sauf un nombre fini, on a $\operatorname{res}(\rho_p(F), \rho_p(F')) \neq 0$. Par ailleurs pour tout p, sauf un nombre fini, on a $\rho_p(f) \nmid \rho_p(F)$ dans $\frac{A}{pA}[X]$ (c'est le lemme 2). Soit donc $\mathcal{S}$ la réunion des deux ensembles finis évoqués ci-dessus. Soit $p \in \mathcal{P} - \mathcal{S}$, alors il existe $h \in A[X]$ unitaire tel que $\rho_p(h)$ soit un irréductible de $\frac{A}{pA}[X]$, que $\rho_p(h) \mid \rho_p(f)$ dans $\frac{A}{pA}[X]$ et $\rho_p(h) \nmid \rho_p(F)$ dans $\frac{A}{pA}[X]$ parce que $\rho_p(F)$ est sans facteur multiple. Alors on a $f \in pA[X] + hA[X]$ et $F \notin pA[X] + hA[X]$. Si $p \in \mathcal{P} - \mathcal{S}$ et en plus $p \notin \{p_1, p_2, \dots, p_s\}$ et choisissant h comme ci-dessus, posant $\mathfrak{m}_n := pA[X] + hA[X]$, il suit que $t_n \in \mathfrak{m}_n$ et $t_1 t_2 \dots t_{n-1} \notin \mathfrak{m}_n$.
4) *Il existe sur* $K(X)$ *une suite de valuations discrètes* $(w_k)_{k \geq 0}$, *avec* $w_k(K(X) - \{0\}) = \mathbb{Z}$, $w_k(t_n) \geq 0$ *pour tout* $k \geq 0, n \geq 0$, $w_k(t_k) = 1$ *pour tout* $k \geq 0$ *et* $w_n(t_k) = 0$ *pour* $0 \leq k < n$ *si* $n \geq 1$.
En plus $\mathfrak{m}_k = \{x \in A[X] \mid w_k(x) \geq 1\}$ *(la suite* $(\mathfrak{m}_k)_{k \geq 0}$ *est définie en* 3)).
Enfin il existe une suite $(\theta_k)_{k \geq 0}$, *d'éléments de* $K(X)$ *avec la propriété que* $w_k(\theta_k) = 1$ *pour tout* $k \geq 0$ *et* $w_k(\theta_n) = 0$ *pour tout* $k \geq 0$, $n \geq 0$ *et* $k \neq n$.
Si O_{w_k} (resp. $\mathfrak{m}_{w_k}$) *est l'anneau de valuation de* w_k (resp. l'idéal de valuation de w_k), *alors* $\frac{O_{w_k}}{\mathfrak{m}_{w_k}}$ *est une extension finie de* $\frac{A[X]}{\mathfrak{m}_k}$, *en particulier* $\frac{O_{w_k}}{\mathfrak{m}_{w_k}}$ *est un corps fini.*
Enfin pour tout $x \in K(X) - \{0\}$, *il existe* $n \geq 0$, $\beta_0, \beta_1, \dots, \beta_n \in \mathbb{Z}$, $\varepsilon \in A^\times$ *tel que* $x = \varepsilon\, \theta_1^{\beta_1} \theta_2^{\beta_2} \dots \theta_n^{\beta_n}$.
Montrons cela.
4.1) Si $n = 0$ et si $t_0 = p \in \mathcal{P}$, on peut appliquer à $\mathfrak{m}_0$ défini en 3.1), la partie 1. du lemme 1, ça montre l'existence de w_0 avec les propriétés voulues.
Si $n = 0$ et si $t_0 = f \in \mathbb{Q}$, on peut appliquer à $\mathfrak{m}_0$ défini en 3.2), la partie 2. du lemme 1, ça montre l'existence de w_0 avec les propriétés voulues.

4.2) Si $n \geq 1$ et si $t_n = p \in \mathcal{P}$, on peut appliquer à $\mathfrak{m}_n$ défini en 3.3), la partie 1. du lemme 1, ça montre l'existence de w_n avec en particulier $w_n(p) = 1$, i.e. $w_n(t_n) = 1$.
Si $n \geq 1$ et si $t_n = f \in \mathfrak{Q}$, on peut appliquer à $\mathfrak{m}_n$ défini en 3.4), la partie 2. du lemme 1, ça montre l'existence de w_n avec en particulier $w_n(p) = 1$, $w_n(f) = 1$, i.e. $w_n(t_n) = 1$.
4.3) Pour tout $n \geq 0$, on a $A[X] \subset \{ x \in K(X) \mid w_n(x) \geq 0 \}$, on a donc $w_n(t_k) \geq 0$ pour tout $k \geq 0$. Comme $t_0 t_1 \ldots t_{n-1} \notin \mathfrak{m}_n$, cela veut dire que $w_n(t_1 t_2 \ldots t_{n-1}) = 0$, il suit donc que $w_n(t_k) = 0$ pour $0 \leq k \leq n-1$. Enfin, on sait par le lemme 1, que $\frac{O_{w_k}}{\mathfrak{m}_{w_k}}$ est un corps fini.
4.4) Montrons l'existence d'une suite $(\theta_n)_{n \geq 0}$ avec $w_n(\theta_n) = 1$ et $w_k(\theta_n) = 0$ pour $k \neq n$. On écrit θ_n sous la forme $\theta_n = t_0^{\alpha_0} t_1^{\alpha_1} \ldots t_n^{\alpha_n}$ avec $\alpha_i \in \mathbb{Z}$. Si $k > n$, on a bien $w_k(\theta_n) = 0$ (c'est 4.3)). Il reste à montrer qu'il existe $\alpha_0, \alpha_1, \ldots, \alpha_n \in \mathbb{Z}$ avec $w_0(\theta_n) = w_1(\theta_n) = \ldots = w_{n-1}(\theta_n) = 0$ et $w_n(\theta_n) = 1$.
Cela donne le système (*) suivant :

$$\begin{aligned}
\alpha_0 w_0(t_0) + \alpha_1 w_0(t_1) + \alpha_2 w_0(t_2) + \ldots + \alpha_n w_0(t_n) &= 0 \\
\alpha_1 w_1(t_1) + \alpha_2 w_1(t_2) + \ldots + \alpha_n w_1(t_n) &= 0 \\
\ldots & \\
\alpha_{n-1} w_{n-1}(t_{n-1}) + \alpha_n w_{n-1}(t_n) &= 0 \\
\alpha_n w_n(t_n) &= 1
\end{aligned}$$

Sachant que $1 = w_0(t_0) = w_1(t_1) = \ldots = w_n(t_n)$, la matrice $M := [\, w_i(t_j) \,]_{\substack{0 \leq i \leq n \\ 0 \leq j \leq n}}$ est triangulaire supérieure, avec des 1 sur la diagonale, ce qui veut dire que $M \in S\ell_{n+1}(\mathbb{Z})$. il suit de cela que le système (*) admet une solution unique en $\alpha_0, \alpha_1, \ldots, \alpha_n$ avec $\alpha_n = 1$ et $\alpha_k \in \mathbb{Z}$.
Si donc on écrit la relation ci-dessus pour $k = 1, 2, \ldots, n$ on a des éléments $\alpha_{ij} \in \mathbb{Z}$ tels que $\theta_0 = t_0$, $\theta_1 = t_0^{\alpha_{10}} t_1$, $\theta_2 = t_0^{\alpha_{20}} t_1^{\alpha_{21}} t_2, \ldots,$
$\theta_n = t_0^{\alpha_{n0}} t_1^{\alpha_{n1}} \ldots t_{n-1}^{\alpha_{nn-1}} t_n$. Il suit facilement de cela qu'il existe
$z_{n0}, z_{n1}, \ldots, z_{nn-1} \in \mathbb{Z}$ avec $t_n = \theta_0^{z_{n0}} \theta_1^{z_{n1}} \ldots \theta_{n-1}^{z_{nn-1}} \theta_n$.
Il suit bien de cela que pour tout $x \in K(X) - \{0\}$, il existe $n \geq 0$, $\beta_0, \beta_1, \ldots, \beta_n \in \mathbb{Z}$, $\varepsilon \in A^\times - \{0\}$, $x = \varepsilon \theta_0^{\beta_0} \theta_1^{\beta_1} \ldots \theta_n^{\beta_n}$.
5) *Soient $(w_k)_{k \geq 0}$ l'ensemble des valuations discrètes définies en* 4), $S := \{ x \in K(X) \mid w_i(x) \geq 0$ *pour tout* $k \geq 0 \}$. *Alors S est un anneau principal, on a $S^\times = A^\times$, la suite $(\theta_k)_{k \geq 0}$ définie en* 4) *est un système de représentants des irréductibles de S et pour tout $k \geq 0$, $\frac{S}{\theta_k S}$ est un corps fini. De plus on a $A[X] \subset S$ et donc* $\mathrm{Fr}\, S = K(X)$.

Montrons cela.

5.1) Il suit de 4) que les éléments de S sont ceux de la forme $\varepsilon\,\theta_0^{\alpha_0}\theta_1^{\alpha_1}\ldots\theta_n^{\alpha_n}$ avec $n\geq 0$, $\varepsilon\in A^\times$, $\alpha_i\in\mathbb{N}$. En particulier l'élément $x:=\varepsilon\,\theta_0^{\alpha_0}\theta_1^{\alpha_1}\ldots\theta_n^{\alpha_n}\in S^\times$, si et seulement si $w_k(x)=0$ pour tout $k\geq 0$, donc si et seulement si $\alpha_k=0$ pour tout $k\geq 0$. Ainsi on a $A^\times=S^\times$.

5.2) Soit $\mathfrak{N}_k:=\{\,x\in S\mid w_k(x)\geq 1\,\}$. Soient O_{w_k} (resp. $\mathfrak{M}_{w_k}$) l'anneau de valuation de w_k (resp. l'idéal de valuation de w_k). Facilement on a les inclusions suivantes : $\frac{A[X]}{\mathfrak{m}_k}\hookrightarrow\frac{S}{\mathfrak{N}_k}\hookrightarrow\frac{O_{w_k}}{\mathfrak{M}_{w_k}}$. Il suit du lemme 1 que $\frac{S}{\mathfrak{N}_k}$ est fini, donc c'est un corps et alors $\mathfrak{N}_k$ est maximal. Facilement on a $\theta_k\in\mathfrak{N}_k$. Si $x=\varepsilon\,\theta_0^{\alpha_0}\theta_1^{\alpha_1}\ldots\theta_n^{\alpha_n}\in\mathfrak{N}_k$, comme $w_k(x)\geq 1$, cela veut dire que $\alpha_k\geq 1$ et donc $x\,\theta_k^{-1}\in S$. Ainsi $\mathfrak{N}_k\subset\theta_k S$ et donc $\theta_k S$ est un idéal maximal de S.

5.3) Montrons que les idéaux premiers non nuls de S sont les $\theta_k S$. En effet si $\mathfrak{P}$ est un premier non nul, il existe $x\in\mathfrak{P}$, $x\neq 0$, $x\notin S^\times$. On peut donc écrire x sous la forme $x=\varepsilon\,\theta_0^{\alpha_0}\theta_1^{\alpha_1}\ldots\theta_n^{\alpha_n}\in\mathfrak{P}$, il suit de ce qui précède qu'il existe $k\geq 0$ avec $\alpha_k>0$ et $\theta_k\in\mathfrak{P}$; comme $\theta_k S$ est maximal on a $\theta_k S=\mathfrak{P}$.

Ainsi les idéaux premiers non nuls de S sont les $\theta_k S$, d'autre part comme ils sont principaux, cela montre que S est un anneau principal (F.M. ex. 92, p. 255) et que la suite $(\theta_k)_{k\geq 0}$ est un système de représentants des irréductibles de S modulo $S^\times$.

Corollaire 1 *Soit $s\geq 0$, $n\geq 1$, $m\geq 1$ des entiers.*

1. *Soit C un groupe cyclique d'ordre* 2 (resp. 4, 6). *Alors il existe un anneau S qui est principal, de caractéristique nulle avec les propriétés suivantes. Le groupe $S^\times$ des inversibles de S est isomorphe à $C\times\mathbb{Z}^s$, pour tout $a\in S-\{0\}$ l'anneau $\frac{S}{aS}$ est fini et enfin le corps des fractions de S est une extension de $\mathbb{Q}$ de degré de transcendance n.*

2. *Il existe un anneau S qui est principal, de caractéristique p avec les propriétés suivantes. Le groupe $S^\times$ des inversibles de S est isomorphe à $C\times\mathbb{Z}^s$ où C est le groupe cyclique d'ordre p^m-1, pour tout $a\in S-\{0\}$ l'anneau $\frac{S}{aS}$ est fini et enfin le corps des fractions de S est une extension de $\mathbb{F}_q(T)$ de degré de transcendance n.*

Démonstration

1) Montrons 1. . Soient $p_1, p_2, \ldots, p_s$ des nombres premiers distincts avec $p_k > 0$, $A := \mathbb{Z}[\frac{1}{p_1 p_2 \ldots p_s}]$, alors A est principal, $A^\times$ est isomorphe à $\{\pm 1\} \times \mathbb{Z}^s$. On utilise le théorème 1 pour cet anneau A , soit alors S_1 l'anneau S du théorème. Il a bien les propriétés du corollaire avec le fait que son corps des fractions est de degré de transcendance 1 sur $\mathbb{Q}$. On remplce alors A par S_1 dans le théorème 1 et on obtient S_2 qui satisfait le corollaire avec le degré de transcendance 2 , et l'on obtient facilement par récurrence un anneau principal S_n qui satisfait le corollaire en caractéristique nulle. Pour où C est d'ordre 4 (resp. 6) il suffit de remplacer $\mathbb{Z}$ par $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[j]$) avec $i^2 = -1$, $j^3 = 1$ et $j \neq 1$.

2) Montrons 2. . Soient $q := p^m$, $\mathbb{F}_q[T]$ l'anneau des polynômes en la variable T à coefficients dans le corps $\mathbb{F}_q$ à q éléments. Soient $p_1, p_2, \ldots, p_s$ des irréductibles de $\mathbb{F}_q[T]$ non équivalents modulo $\mathbb{F}_q[T]^\times = (\mathbb{F}_q)^\times$, $A := \mathbb{F}_q[T][\frac{1}{p_1 p_2 \ldots p_s}]$, alors A est principal, $A^\times$ est isomorphe à $(\mathbb{F}_q)^\times \times \mathbb{Z}^s$. On utilise alors le procédé de 1).

Remarque Si A est un anneau principal, il existe un procédé "canonique" qui plonge A dans un annea u B qui est euclidien avec le fait qu'un système de représentants des irréductibles de A modulo $A^\times$ est aussi un système de représentants des irréductibles de B modulo $B^\times$. En revanche $B^\times$ est "beaucoup plus gros" que $A^\times$ et pour tout irréductible p de A le corps $\frac{B}{pB}$ est un espace vectoriel de dimension infinie sur $\frac{A}{pA}$ ([H] théorème 5 p. 43).

2. Anneaux principaux avec groupe des inversibles fini

Théorème 2 *Soient A un anneau principal qui n'est pas un corps, K son corps des fractions. On suppose que le groupe $A^\times$ des inversibles de A est fini et que pour tout irréductible p de A , le corps $\frac{A}{pA}$ est fini. Soient $A[X]$ l'anneau des polynômes de la variable X , à coefficients dans A , $K(X)$ le corps des fractions rationnelles de la variable X à coefficients dans K . Alors il existe un sous-anneau S de $K(X)$ avec les propriétés suivantes.*

1. *On a $A[X] \subset S \subset K(X)$ et donc $\mathrm{Fr}\, S = K(X)$.*
2. *L'anneau S est un anneau principal.*
3. *Si $A^\times$ (resp. $S^\times$) désigne le groupe des inversibles de A* (resp. S) , *alors $A^\times = S^\times$.*

4. *Soient* $\mathcal{P}$ *un système de représentants des irréductibles de* A modulo $A^\times$, $\mathcal{Q}$ *un système de représentants modulo* $A^\times$ *des polynômes de* $A[X]$ *qui sont des irréductibles de* $K[X]$ *de contenu* 1 . *Soit* $\mathrm{Max}\,S$ *l'ensemble des idéaux maximaux de* S , *alors il existe une bijection* $u:\mathcal{P}\cup\mathcal{Q}\to\mathrm{Max}\,S$ *telle que pour tout* $t\in\mathcal{P}\cup\mathcal{Q}$ *on a* $t\in u(t)$. *De plus pour tout* $t\in\mathcal{P}$, *le corps* $\frac{S}{u(t)}$ *est infini. et pour tout* $t\in\mathcal{Q}$, *le corps* $\frac{S}{u(t)}$ *est fini.*

Démonstration

1) *L'ensemble* $\mathcal{P}\cup\mathcal{Q}$ *est dénombrable.*

Ce sont les parties 1) et 2) de la démonstration du théorème 1 , sachant que $\mathcal{P}$ est infini (lemme 4). Il suit qu'il existe une bijection $i\mapsto t_i$ de $\mathbb{N}$ sur $\mathcal{P}\cup\mathcal{Q}$ avec $t_0\in\mathcal{P}$.

2) *Il existe une suite* $(\mathfrak{p}_k)_{k\geq 1}$ *d'idéaux premiers de* $A[X]$ *avec la propriété que* $t_n\in\mathfrak{p}_n$ *pour tout* $n\geq 0$ *et que* $t_0t_1\dots t_{n-1}\notin\mathfrak{p}_n$ *pour tout* $n\geq 1$ (*l'élément* t_n *est défini en* 1)).

On peut décrire les idéaux premiers $\mathfrak{p}_n$ *de façon plus précise.*

On rappelle que $\mathcal{P}$ *est un système de représentants des irréductibles de* A modulo $A^\times$ *et que* $\mathcal{Q}$ *est un système de représentants modulo le groupe* $A[X]^\times=A^\times$, *des polynômes* $f\in A[X]$, *qui sont des irréductibles de* $K[X]$, *de contenu* 1 .

Si $p\in\mathcal{P}$, *on note* $\rho_p:A\to\frac{A}{pA}$ *la surjection canonique, on note aussi* $\rho_p:A[X]\to\frac{A}{pA}[X]$ *la surjection définie par* $\rho_p(\sum_i a_iX^i):=\sum_i\rho_p(a_i)X^i$.

3.1) *Comme* $t_0=p\in\mathcal{P}$ *est un irréductible de* A , *alors on définit* $\mathfrak{p}_0$ *par* $\mathfrak{p}_0:=pA[X]$.

Ensuite, on suppose $\mathfrak{p}_0,\mathfrak{p}_1,\dots,\mathfrak{p}_{n-1}$ *choisis avec les propriétés indiquées.*

On écrit $t_0t_1\dots t_{n-1}=p_1p_2\dots p_sf_1f_2\dots f_r$ *où* $p_i\in\mathcal{P}$ *et les* $f_i\in\mathcal{Q}$ $(s+r=n)$.

3.2) *Si* $t_n=p\in\mathcal{P}$, *on définit* $\mathfrak{p}_n$ *par* $\mathfrak{p}_n:=pA[X]$.

3.3) *Si* $t_n=f\in\mathcal{Q}$, *on définit* $\mathfrak{p}_n$ *par* $\mathfrak{p}_n:=pA[X]+hA[X]$ *en choisissant* p *et* h *comme il suit. Soit* $F=f_1f_2\dots f_r$, *on choisit* $p\in\mathcal{P}$ *de façon que* $p\notin\{p_1,p_2,\dots,p_s\}$, *que* $\rho_p(F)$ *soit séparable et que* $\rho_p(f)$ *soit séparable et on choisit* h *tel que* $\rho_p(h)$ *soit un irréductible de* $\frac{A}{pA}[X]$, *que* $\rho_p(h)\mid\rho_p(f)$ *et que* $\rho_p(h)\nmid\rho_p(F)$. *Dans ce cas* $\mathfrak{p}_n$ *est un maximal.*

Il est clair que $\mathfrak{p}_0$ est premier.

Pour 3.2) , on a bien $t_n=p\in pA[X]=:\mathfrak{p}_n$ et $\mathfrak{p}_n$ est premier.

Il reste à montrer que $t_0t_1\dots t_{n-1}\notin\mathfrak{p}_n$. Sinon on aurait $t_0t_1\dots t_{n-1}=t_n\lambda$ avec $\lambda\in A[X]$. Comme $A[X]$ est factoriel et que la famille $(t_k)_{k\geq 0}$ est un système de représentants des irréductibles de $A[X]$, ce n'est pas possible.

Pour 3.3), comme $t_n \notin \{t_0, t_1, \dots, t_{n-1}\}$, on a $f \nmid f_1 f_2 \dots f_r =: F$ dans $A[X]$ et d'autre part F est sans facteur multiple, i.e. $\mathrm{res}(F, F') \neq 0$. Ainsi pour tout $p \in \mathcal{P}$, sauf un nombre fini, on a $\mathrm{res}(\rho_p(F), \rho_p(F')) \neq 0$. Par ailleurs pour tout p, sauf un nombre fini, on a $\rho_p(f) \nmid \rho_p(F)$ dans $\frac{A}{pA}[X]$ (c'est le lemme 2). Soit donc $\mathcal{S}$ la réunion des deux ensembles finis évoqués ci-dessus. Soit $p \in \mathcal{P} - \mathcal{S}$, alors il existe $h \in A[X]$ unitaire tel que $\rho_p(h)$ soit un irréductible de $\frac{A}{pA}[X]$, que $\rho_p(h) \mid \rho_p(f)$ dans $\frac{A}{pA}[X]$ et $\rho_p(h) \nmid \rho_p(F)$ dans $\frac{A}{pA}[X]$ parce que $\rho_p(F)$ est sans facteur multiple. Alors on a $f \in pA[X] + hA[X]$ et $F \notin pA[X] + hA[X]$. Si $p \in \mathcal{P} - \mathcal{S}$ et en plus $p \notin \{p_1, p_2, \dots, p_s\}$ et choisissant h comme ci-dessus, posant $\mathfrak{p}_n := pA[X] + hA[X]$, il suit que $t_n \in \mathfrak{p}_n$.

Il reste à montrer que $t_0 t_1 \dots t_{n-1} \notin \mathfrak{p}_n$. Sinon on aurait $\rho_p(t_0 t_1 \dots t_{n-1}) = \rho_p(p_1 p_2 \dots p_s)\, \rho_p(f_1 f_2 \dots f_r) \in \rho_p(\mathfrak{p}_n) = \rho_p(h)\frac{A}{pA}[X]$. Comme $\rho_p(p_1 p_2 \dots p_s) \neq 0$, cela impliquerait que $\rho_p(h) \mid \rho_p(f_1 f_2 \dots f_r)$ dans $\frac{A}{pA}[X]$, ce qui est contraire à la définition de h.

4) *Il existe sur* $K(X)$ *une suite de valuations discrètes* $(w_k)_{k \geq 0}$, *avec* $w_k(K(X) - \{0\}) = \mathbb{Z}$, $w_k(t_n) \geq 0$ *pour tout* $k \geq 0, n \geq 0$, $w_k(t_k) = 1$ *pour tout* $k \geq 0$ *et* $w_n(t_k) = 0$ *pour* $0 \leq k < n$ *si* $n \geq 1$.

En plus $\mathfrak{p}_k = \{x \in A[X] \mid w_k(x) \geq 1\}$ *(la suite* $(\mathfrak{p}_k)_{k \geq 0}$ *est définie en* 3)).

Enfin il existe une suite $(\theta_k)_{k \geq 0}$, *d'éléments de* $K(X)$ *avec la propriété que* $w_k(\theta_k) = 1$ *pour tout* $k \geq 0$ *et* $w_k(\theta_n) = 0$ *pour tout* $k \geq 0$, $n \geq 0$ *et* $k \neq n$.

Si $t_k \in \mathfrak{Q}$ *et si* O_{w_k} (resp. $\mathfrak{m}_{w_k}$) *est l'anneau de valuation de* w_k (resp. *l'idéal de valuation de* w_k), *alors* $\frac{O_{w_k}}{\mathfrak{m}_{w_k}}$ *est un corps fini.*

Enfin pour tout $x \in K(X) - \{0\}$, *il existe* $n \geq 0$, $\beta_0, \beta_1, \dots, \beta_n \in \mathbb{Z}$, $\varepsilon \in A^\times$ *tel que* $x = \varepsilon\, \theta_1^{\beta_1} \theta_2^{\beta_2} \dots \theta_n^{\beta_n}$.

Montrons cela.

4.1) Si $t_k = p \in \mathcal{P}$, soient v_p la valuation discrète sur K définie par $v_p(p) = 1$ et w_k la valuation discrète sur $K(X)$ définie par $w_k(\frac{U}{V}) := v_p(\mathrm{cont}\, U) - v_p(\mathrm{cont}\, V)$, où $U, V \in K[X]$ et "cont" signifie contenu. On a bien $w_k(K(X) - \{0\}) = \mathbb{Z}$, $w_k(t_k) = 1$, $w_k(U) \geq 0$ pour tout $U \in A[X]$. Enfin $\{U \in A[X] \mid w_k(U) \geq 1\} = pA[X] = \mathfrak{p}_k$.

4.2) Si $n \geq 1$ et si $t_n = f \in \mathfrak{Q}$, on peut appliquer à $\mathfrak{p}_n$ défini en 3.3), la partie 2. du lemme 1, ça montre l'existence de w_n avec en particulier $w_n(p) = 1$, $w_n(f) = 1$, i.e. $w_n(t_n) = 1$.

4.3) Pour tout $n\geq 0$, il suit de 4.1) et de la partie 2. du lemme 1, que $A[X]\subset\{x\in K(X)\mid w_n(x)\geq 0\}$, on a donc $w_n(t_k)\geq 0$ pour tout $k\geq 0$. Comme $t_0 t_1 \dots t_{n-1}\notin \mathfrak{p}_n$, cela veut dire que $w_n(t_0 t_1 \dots t_{n-1})=0$, il suit donc que $w_n(t_k)=0$ pour $0\leq k\leq n-1$.

Si $t_k\in\mathfrak{Q}$, il suit du lemme 1 partie 2. que $\frac{O_{w_k}}{\mathfrak{m}_{w_k}}$ est un corps fini.

4.4) Montrons l'existence d'une suite $(\theta_n)_{n\geq 0}$ avec $w_n(\theta_n)=1$ et $w_k(\theta_n)=0$ pour $k\neq n$. On écrit θ_n sous la forme $\theta_n=t_0^{\alpha_0} t_1^{\alpha_1}\dots t_n^{\alpha_n}$ avec $\alpha_i\in\mathbb{Z}$. Si $k>n$, on a bien $w_k(\theta_n)=0$ (c'est 4.3)). Il reste à montrer qu'il existe $\alpha_0,\alpha_1,\dots,\alpha_n\in\mathbb{Z}$ avec $w_0(\theta_n)=w_1(\theta_n)=\dots=w_{n-1}(\theta_n)=0$ et $w_n(\theta_n)=1$.

Cela donne le système (*) suivant :

$$\begin{aligned}
&\alpha_0 w_0(t_0)+\alpha_1 w_0(t_1)+\alpha_2 w_0(t_2)+\dots+\alpha_n w_0(t_n)=0\\
&\qquad\alpha_1 w_1(t_1)+\alpha_2 w_1(t_2)+\dots+\alpha_n w_1(t_n)=0\\
&\qquad\qquad\vdots\\
&\qquad\alpha_{n-1} w_{n-1}(t_{n-1})+\alpha_n w_{n-1}(t_n)=0\\
&\qquad\qquad\alpha_n w_n(t_n)=1
\end{aligned}$$

Sachant que $1=w_0(t_0)=w_1(t_1)=\dots=w_n(t_n)$, la matrice $M:=[w_i(t_j)]_{\substack{0\leq i\leq n\\ 0\leq j\leq n}}$ est triangulaire supérieure, avec des 1 sur la diagonale, ce qui veut dire que $M\in S\ell_{n+1}(\mathbb{Z})$. il suit de cela que le système (*) admet une solution unique en $\alpha_0,\alpha_1,\dots,\alpha_n$ avec $\alpha_n=1$ et $\alpha_k\in\mathbb{Z}$.

Si donc, on écrit la relation ci-dessus pour $k=0,1,\dots,n$ on a des éléments $\alpha_{ij}\in\mathbb{Z}$ tels que $\theta_0=t_0$, $\theta_1=t_0^{\alpha_{10}}t_1$, $\theta_2=t_0^{\alpha_{20}}\,t_1^{\alpha_{21}}t_2,\dots,$
$\theta_n=t_0^{\alpha_{n0}}\,t_1^{\alpha_{n1}}\dots t_{n-1}^{\alpha_{nn-1}}t_n$. Il suit facilement de cela qu'il existe $z_{n0},z_{n1},\dots,z_{nn-1}\in\mathbb{Z}$ avec $t_n=\theta_0^{z_{n0}}\theta_1^{z_{n1}}\dots\theta_{n-1}^{z_{nn-1}}\theta_n$.

Il suit bien de cela que pour tout $x\in K(X)-\{0\}$, il existe $n\geq 0$, $\beta_0,\beta_1,\dots,\beta_n\in\mathbb{Z}$, $\varepsilon\in A^\times-\{0\}$, $x=\varepsilon\theta_0^{\beta_0}\theta_1^{\beta_1}\dots\theta_n^{\beta_n}$.

5) *Soient $(w_k)_{k\geq 0}$ l'ensemble des valuations discrètes définies en* 4), $S:=\{x\in K(X)\mid w_i(x)\geq 0$ *pour tout* $k\geq 0\}$. *Alors S est un anneau principal, on a $S^\times=A^\times$, la suite $(\theta_k)_{k\geq 0}$ définie en* 4) *est un système de représentants des irréductibles de S. Pour tout $k\geq 0$ tel que $t_k\in\mathcal{P}$, $\frac{S}{\theta_k S}$ est un corps infini et et pour tout $k\geq 0$ tel que $t_k\in\mathfrak{Q}$, $\frac{S}{\theta_k S}$ est un corps fini. De plus on a $A[X]\subset S$ et donc* $\mathrm{Fr}S=K(X)$.

Montrons cela.

5.1) Il suit de 4) que les éléments de S sont ceux de la forme $\varepsilon\,\theta_0^{\alpha_0}\theta_1^{\alpha_1}\dots\theta_n^{\alpha_n}$ avec $n\geq 0$, $\varepsilon\in A^\times$, $\alpha_i\in\mathbb{N}$. En particulier l'élément

$x:=\varepsilon\,\theta_0^{\alpha_0}\theta_1^{\alpha_1}\ldots\theta_n^{\alpha_n}\in S^\times$, si et seulement si $w_k(x)=0$ pour tout $k\geq 0$, donc si et seulement si $\alpha_k=0$ pour tout $k\geq 0$. Ainsi on a $A^\times=S^\times$.

5.2) On a $\theta_k S=\{x\in S \mid w_k(x)\geq 1\}$. En effet, si $x=\varepsilon\,\theta_0^{\alpha_0}\theta_1^{\alpha_1}\ldots\theta_n^{\alpha_n}$, comme $w_k(x)\geq 1$, cela veut dire que $\alpha_k\geq 1$ et donc $x\,\theta_k^{-1}\in S$. Il suit de cela que les $\theta_k S$ sont des idéaux premiers de S .

5.3) Soient k tel que $t_k\in\mathbb{Q}$, on a $\{x\in S \mid w_k(x)\geq 1\}=\theta_k S$. Soient O_{w_k} (resp. $\mathfrak{M}_{w_k}$) l'anneau de valuation de w_k (resp. l'idéal de valuation de w_k). Facilement on a les inclusions suivantes : $\frac{A[X]}{\mathfrak{p}_k}\hookrightarrow\frac{S}{\theta_k S}\hookrightarrow\frac{O_{w_k}}{\mathfrak{M}_{w_k}}$. Si donc $t_k\in\mathbb{Q}$, il suit de 4) que $\frac{S}{\theta_k S}$ est fini, donc c'est un corps et alors $\theta_k S$ est maximal.

5.4) Montrons que les idéaux premiers non nuls de S sont les $\theta_k S$. En effet si $\mathfrak{P}$ est un premier non nul, il existe $x\in\mathfrak{P}, x\neq 0$, $x\notin S^\times$. On peut donc écrire x sous la forme $x=\varepsilon\,\theta_0^{\alpha_0}\theta_1^{\alpha_1}\ldots\theta_n^{\alpha_n}\in\mathfrak{P}$, il suit de ce qui précède qu'il existe $k\geq 0$ avec $\alpha_k>0$ et $\theta_k\in\mathfrak{P}$; il s'agit encore de montrer que $\theta_k S=\mathfrak{P}$. Si $t_k\in\mathbb{Q}$, on sait par 5.3) que $\theta_k S$ est maximal, ainsi $\theta_k S=\mathfrak{P}$. On suppose maintenant que $t_k\in\mathcal{P}$. S'il existe $x\in\mathfrak{P}$ et $x\notin\theta_k S$, il suit de l'écriture de x sous la forme $x=\varepsilon\,\theta_0^{\alpha_0}\theta_1^{\alpha_1}\ldots\theta_n^{\alpha_n}$, que $\alpha_k=0$ et qu'il existe $i\neq k$ avec $\theta_i\in\mathfrak{P}$. Si $t_i\in\mathbb{Q}$, on sait par ce qui précède que $\theta_i S=\mathfrak{P}$; on a donc $\theta_k=\theta_i s$ avec $s\in S$, sachant que $w_i(\theta_k)=0$, on obtient donc une contradiction. Il nous reste à supposer que $t_i\in\mathcal{P}$. Sachant que $w_n(t_n)=1$ pour tout $n\geq 0$ et $w_k(t_n)\geq 0$ pour tout $n\geq 0$, $k\geq 0$, il suit que $t_k=\theta_k s_k$ et $t_i=\theta_i s_i$ avec $s_k, s_i\in S$ ainsi donc $t_k, t_i\in\mathfrak{P}$. Sachant que $t_k, t_i\in\mathcal{P}$, que l'anneau A est principal et que $k\neq i$, alors il existe $u, v\in A$ avec $u\,t_k+v\,t_i=1$; ainsi $1\in\mathfrak{P}$, c'est impossible. En conséquence, l'hypothèse $\theta_k S\subset\mathfrak{P}$ et $\theta_k S\neq\mathfrak{P}$ est à rejeter. Ce qui veut dire que $\theta_k S=\mathfrak{P}$.

Avec 5.2) cela montre bien que les idéaux premiers non nuls de S sont les $\theta_k S$. Comme ils sont principaux, cela montre que S est un anneau principal (F.M. ex. 92, p.255) et que la suite $(\theta_k)_{k\geq 0}$ est un système de représentants des irréductibles de S modulo $S^\times$.

5.5) Soient k tel que $t_k=p\in\mathcal{P}$, il suit de la définition de w_k que $\{x\in A[X] \mid w_k(x)\geq 1\}=pA[X]$ et que $\{x\in S \mid w_k(x)\geq 1\}=\theta_k S$. Soient O_{w_k} (resp. $\mathfrak{M}_{w_k}$) l'anneau de valuation de w_k (resp. l'idéal de valuation de w_k). Facilement on a les inclusions suivantes : $\frac{A[X]}{pA[X]}\hookrightarrow\frac{S}{\theta_k S}\hookrightarrow\frac{O_{w_k}}{\mathfrak{M}_{nk}}$.

Comme $\frac{S}{\theta_k S}$ est un corps qui contient $\frac{A[X]}{pA[X]}\simeq\frac{A}{pA}[X]$, il suit que $\frac{S}{\theta_k S}$ contient $\frac{A}{pA}(X)$ qui est infini.

Corollaire 2

1. *Il existe un anneau* S *qui est principal, de caractéristique nulle, dont le groupe* $S^\times$ *des inversibles est cyclique d'ordre* 2 (resp. 4 , 6) *et pour lequel il existe* $a \in S-\{0\}$ *tel que* $\frac{S}{aS}$ *soit infini*

2. *Soit* p *un nombre premier,* $m \geq 1$ *un entier. Alors existe un anneau* S *qui est principal, de caractéristique* p , *dont le groupe* $S^\times$ *des inversibles est cyclique d'ordre* p^m *et pour lequel il existe* $a \in S-\{0\}$ *tel que* $\frac{S}{aS}$ *soit infini*

Démonstration

1) Pour montrer 1. on utilise le théorème 2 avec $A=\mathbb{Z}$ (resp. $\mathbb{Z}[i]$, $\mathbb{Z}[j]$ avec $i^2=-1$, $j^3=1$ et $j \neq 1$). Alors l'anneau S du théorème 2 convient.

1) Pour montrer 2. on utilise le théorème 2 avec $A=\mathbb{F}_q[T]$ où $q=p^m$, $\mathbb{F}_q$ est le corps fini à q éléments et $\mathbb{F}_q[T]$ est l'anneau des polynômes en la variable T à coefficients dans $\mathbb{F}_q$. Alors l'anneau S du théorème 2 convient.

Lemme 1 *Soient* A *un anneau principal,* K *son corps des fractions. On suppose que* A *est dénombrable. Soient* $A[X]$ *l'anneau des polynômes de la variable* X , *à coefficients dans* A , $K(X)$ *le corps des fractions rationnelles de la variable* X *à coefficients dans* K .

Soient $\mathcal{P}$ *est un système de représentants des irréductibles de* A modulo $A^\times$ *et* $\mathcal{Q}$ *est un système de représentants modulo le groupe* $A[X]^\times=A^\times$, *des polynômes* $f \in A[X]$, *qui sont des irréductibles de* $K[X]$, *de contenu* 1 .

Si $p \in \mathcal{P}$, *on note* $\rho_p : A \to \frac{A}{pA}$ *la surjection canonique, on note aussi* $\rho_p : A[X] \to \frac{A}{pA}[X]$ *la surjection définie par* $\rho_p(\sum_i a_i X^i) := \sum_i \rho_p(a_i) X^i$.

Soit $\mathfrak{m}=pA[X]+hA[X]$ *un idéal maximal de* $A[X]$ *avec* $p \in \mathcal{P}$, $h \in A[X]$ *unitaire, de façon que* $\rho_p(h)$ *soit un irréductible de* $\frac{A}{pA}[X]$.

1. *Alors il existe une valuation discrète* v *sur* $K(X)$ *avec* $v(K(X)-\{0\})=\mathbb{Z}$, $v(p)=1$, $A[X] \subset \{x \in K(X) \mid v(x) \geq 0\}$, $\mathfrak{m}=\{x \in A[X] \mid v(x) \geq 1\}$. *Si* O_v (resp. $\mathfrak{m}_v$) *est l'anneau de valuation de* v (resp. *l'idéal de valuation de* v), *alors* $\frac{O_v}{\mathfrak{m}_v}$ *est une extension finie de* $\frac{A}{pA}$.

2. *On suppose ici en plus qu'il existe* $f \in \mathcal{Q}$ *de façon que* $\rho_p(f)$ *soit un polynôme séparable avec* $\deg f = \deg \rho_p(f)$ *et que* $\rho_p(h) \mid \rho_p(f)$ *dans* $\frac{A}{pA}[X]$. *Alors il existe une valuation discrète* v *sur* $K(X)$ *avec* $v(K(X)-\{0\})=\mathbb{Z}$, $v(p)=1$, $v(f)=1$, $A[X] \subset \{x \in K(X) \mid v(x) \geq 0\}$, $\mathfrak{m}=\{x \in A[X] \mid v(x) \geq 1\}$. *Si* O_v

(resp. $\mathfrak{m}_v$) *est l'anneau de valuation de* v (resp. *l'idéal de valuation de* v), *alors* $\frac{O_v}{\mathfrak{m}_v}$ *est une extension finie de* $\frac{A}{pA}$.

Démonstration

1) Montrons d'abord 1. . Notons v_p la valuation discrète sur K définie par $v_p(p)=1, K_p$ le complété de K pour cette valuation et $A_p := \{ x \in K_p \mid v_p(x) \geq 0 \}$. Soit $z_1 \in (K_p)^{alg}$ tel que $h(z_1)=0$, sachant que $\rho_p(h)$ est un irréductible de $\frac{A}{pA}[X]$, il suit que $K_p[z_1]$ sur K_p est une extension non ramifiée de degré, le degré de h . Notons encore v_p le prolongement de v_p à $K_p[z_1]$; comme $h(X) \in A_p[X]$ est un polynôme unitaire, on a $v_p(z_1) \geq 0$. Soit $B := \{ x \in K_p[z_1] \mid v_p(x-z_1) \geq 1 \}$, on sait que cette boule n'est pas dénombrable, donc elle contient un élément z transcendant sur K , sachant que A est dénombrable, donc aussi K . Comme $v_p(z-z_1) \geq 1$, il suit facilement que $v_p(h(z)) \geq 1$.

Soit $i : K(X) \to K_p[z_1]$ l'homomorphisme injectif défini par $i(r(X)) := r(z)$ et v la valuation sur $K(X)$ défini par $v(r(X)) := v_p(r(z))$. Ainsi on a $v(X) = v_p(z)$ et comme $v_p(z_1) \geq 0$, on a $v(X) = v_p(z) \geq 0$. Il suit de cela que $A[X] \subset \{ x \in K(X) \mid v(x) \geq 0 \}$; ensuite on a $\mathfrak{m} \subset \{ x \in A[X] \mid v(x) \geq 1 \}$ et comme $\mathfrak{m}$ est maximal, on a bien $\mathfrak{m} = \{ x \in A[X] \mid v(x) \geq 1 \}$. Soit O (resp. $\mathfrak{N}$) l'anneau de valuation de $K_p[z_1]$ (resp. l'idéal de valuation de $K_p[z_1]$) ; comme $K_p[z_1]$ sur K_p est non ramifié de degré, le degré de h , il suit que $\frac{O}{\mathfrak{N}}$ est une extension $\frac{A}{pA}$ de degré, le degré de h . Soient O_v (resp. $\mathfrak{m}_v$) l'anneau de valuation de v (resp. l'idéal de valuation de v), facilement, on a $O_v = i^{-1}(O)$, $\mathfrak{m}_v = i^{-1}(\mathfrak{N})$ et $\mathfrak{m}_v \cap A[X] = \mathfrak{m}$. Il suit de cela les inclusions suivantes : $\frac{A[X]}{\mathfrak{m}} \hookrightarrow \frac{O_v}{\mathfrak{m}_v} \hookrightarrow \frac{O}{\mathfrak{N}}$; ainsi $\frac{O_v}{\mathfrak{m}_v}$ est une extension finie de $\frac{A}{pA}$.

2) Montrons 2. . Soient v_p, K_p, A_p , comme précédemment. Puisque $\rho_p(h) \mid \rho_p(f)$ dans $\frac{A}{pA}[X]$, il existe $u \in A_p[X]$ avec $\rho_p(f) = \rho_p(h)\rho_p(u))$. Comme $\rho_p(f)$ est séparable on a $1 = \text{pgcd}(\rho_p(h), \rho_p(u))$. Il suit du lemme de Hensel que $f = h_1 u_1$ avec $h_1, u_1 \in A_p[X]$, $\deg h_1 = \deg h$, $\rho_p(h_1) = \rho_p(h)$, $\rho_p(u_1) = \rho_p(u)$.

Soit $z_1 \in (K_p)^{alg}$ tel que $h_1(z_1)=0$, alors $K_p[z_1]$ sur K_p est non ramifié de degré, le degré de h . Notons encore v_p le prolongement unique de v_p à $K_p[z_1]$. Facilement $v_p(z_1) \geq 0$; soient O (resp. $\mathfrak{N}$) l'anneau de valuation de $K_p[z_1]$ (resp. son idéal de valuation). Soit $\mu : O \to \frac{O}{\mathfrak{N}}$ la surjection canonique, on a donc $\rho_p(h)(\mu(z_1)) = 0$ et comme $\rho_p(f)$ est

séparable, on a $\rho_p(f)'(\mu(z_1))\neq 0$ et donc $v_p(f'(z_1))=0$. Il suit facilement de cela que $v_p(f(z_1+p))=1$. Soient $z_2:=z_1+p$,
$B:=\{x\in K_p[z_1] \mid v_p(x-z_2)\geq 2\}$, cette boule n'est pas dénombrable, ainsi B contient un élément z qui est transcendant sur K , sachant que K est dénombrable , facilement on a encore $v_p(z)\geq 0$, $v_p(f(z))=1$.
Soit $i:K(X)\to K_p[z_1]$ l'homomorphisme injectif défini par $i(r(X)):=r(z)$ et v la valuation sur $K(X)$ défini par $v(r(X)):=v_p(r(z))$.
Ainsi on a $v(x)=v_p(x)$ pour $x\in K$, $v(f)=v_p(f(z))=1$ et $v(X)=v_p(z)\geq 0$.
Il suit de cela que $A[X]\subset\{x\in K(X) \mid v(x)\geq 0\}$; ensuite on a bien $\mathfrak{m}\subset\{x\in A[X] \mid v(x)\geq 1\}$ et comme $\mathfrak{m}$ est maximal on a bien $\mathfrak{m}=\{x\in A[X] \mid v(x)\geq A\}$.
Comme $K_p[z_1]$ est une extension non ramifiée de K_p de degré, le degré de h , il suit que $\frac{O}{\mathfrak{N}}$ est une extension de $\frac{A}{pA}$ de degré, le degré de h .
Soient $O_v:=\{x\in K(X) \mid v(x)\geq 0\}$, $\mathfrak{m}_v:=\{x\in K(X) \mid v(x)\geq 1\}$; donc $O_v=i^{-1}(O)$, $\mathfrak{m}_v=i^{-1}(\mathfrak{N})$ et $\mathfrak{m}_v\cap A[X]=\mathfrak{m}$. Il suit de cela des inclusions suivantes : $\frac{A[X]}{\mathfrak{m}}\hookrightarrow\frac{O_v}{\mathfrak{m}_v}\hookrightarrow\frac{O}{\mathfrak{N}}$; ainsi $\frac{O_v}{\mathfrak{m}_v}$ est une extension finie de $\frac{A}{pA}$.

Lemme 2 *Soient A un anneau principal, K le corps des fractions de A , p un irréductible de A , $\rho_p:A\to\frac{A}{pA}$ la surjection canonique, par ailleurs si $A[X]$* (resp. $\frac{A}{pA}[X]$) *désigne l'anneau des polynômes à coefficients dans A* (resp. $\frac{A}{pA}$) *, on note encore $\rho_p:A[X]\to\frac{A}{pA}[X]$, l'homomorphisme défini par $\rho_p(\sum_i a_iX^i):=\sum_i\rho_p(a_i)X^i$.*

Soit $\mathcal{P}$ un système de représentants des irréductibles de A modulo les inversibles de A . On suppose que $\mathcal{P}$ est infini. Soient $u,v\in A[X]$, $u\neq 0$, avec $u\nmid v$ dans $K[X]$. Alors il existe une partie finie S de $\mathcal{P}$ de façon que pour tout $p\in\mathcal{P}-S$, on a $\rho_p(u)\nmid\rho_p(v)$ dans $\frac{A}{pA}[X]$.

Démonstration
1) Facilement, il existe une partie S_1 de $\mathcal{P}$ telle que pour tout $p\in\mathcal{P}-S_1$, on a $\deg u=\deg\rho_p(u)$.
2) Soit K le corps des fractions de A , alors la division euclidienne de v par u dans $K[X]$ dit que $v(X)=u(X)\,q(X)+r(X)$ avec $q(X),r(X)\in K[X]$, $\deg r<\deg u$ et $r\neq 0$ parce que $u\nmid v$ dans $K[X]$. Facilement il existe $d\in A-\{0\}$ tel que $d\,v(X)=u(X)\,dq(X)+d\,r(X)$ avec $d\,q$, $dr\in A[X]$. Soit S_2 l'ensemble des éléments de $\mathcal{P}$ qui divisent d . Si donc $p\in\mathcal{P}-(S_1\cup S_2)$,

l'égalité $\rho_p(dv)=\rho_p(u)\,\rho_p(dq)+\rho_p(dr)$ est bien la division euclidienne de $\rho_p(dv)$ par $\rho_p(u)$ puisque $\deg\rho_p(u)=\deg(u)$ et $\deg r=\deg\rho_p(dr)$.
Soit maintenant S_3, l'ensemble des éléments de $\mathcal{P}$ tels que $\rho_p(dr)=0$; S_3 est fini parce que $dr\neq 0$. Si donc $p\in\mathcal{P}-(S_1\cup S_2\cup S_3)$, on a $\rho_p(dr)\neq 0$, ce qui veut bien dire que $\rho_p(u)\nmid\rho_p(dv)$ dans $\frac{A}{pA}[X]$, sachant que $\rho_p(d)\neq 0$, cela veut bien dire que $\rho_p(u)\nmid\rho_p(v)$ dans $\frac{A}{pA}[X]$.

Remarque Si $\mathcal{P}$ est fini, on peut dire que le lemme est encore vrai, mais il faut prendre $S=\mathcal{P}$. En effet supposons $\mathcal{P}=\{p_1,p_2,\ldots,p_r\}$, soient $u=X$, $v=X+p_1p_2\ldots p_r$, facilement $u\nmid v$ dans $K[X]$, mais $\rho_{p_i}(u)=\rho_{p_i}(v)$ pour $1\leq i\leq r$.

Lemme 3 *Soient A un anneau commutatif unitaire intègre, $A^\times$ le groupe des inversibles de A. On suppose que $A^\times$ est fini.*
1. *Si* $\mathrm{car}A=0$, *alors* $A^\times$ *est cyclique d'ordre* 2, 4 *ou* 6.
2. *Si* $\mathrm{car}A=p$, *alors il existe un entier* $m\geq 1$ *et* $A^\times$ *est le groupe cyclique d'ordre* p^m-1.
Pour chacun des ordres, il existe un exemple d'anneau.

Démonstration
Comme $A^\times$ est un sous-groupe fini de $(\mathrm{Fr}A)^\times$, il est cyclique.
1) Montrons 1.. Comme $-1\in A$ avec $-1\neq 1$, il suit que $o(A^\times)=2m$ avec $m\geq 1$. Ainsi il existe $\xi\in A^\times$ avec $o(\xi)=2m$. Il suit de cela que $\mathbb{Z}[\xi]^\times\subset A^\times$. On sait que $\mathbb{Z}[\xi]^\times\simeq C\times\mathbb{Z}^s$ avec C cyclique d'ordre $2m$. Si $\xi=-1$, on a $\mathbb{Z}[\xi]^\times=\mathbb{Z}^\times=\{\pm 1\}$; si $\xi\in\mathbb{C}-\mathbb{R}$ on a $s=(\frac{1}{2}\varphi(2m))-1$ où φ est l'indicateur d'Euler. Comme $A^\times$ est fini, on a donc $s=0$; i.e. $\varphi(2m)=2$ si $\xi\in\mathbb{C}-\mathbb{R}$. Cela implique facilement que $m=2$ *ou* 3. Ainsi $A^\times$ cyclique d'ordre 2, 4 ou 6.
2) Montrons 2.. C'est plus facile. Comme $\mathrm{car}A=p$, on peut supposer que $\mathbb{F}_p\subset A$, comme tout élément de $A^\times$ est algébrique sur $\mathbb{F}_p$, il existe $m\geq 1$ tel que $\mathbb{F}_p[A^\times]\simeq\mathbb{F}_{p^m}$; cela montre que $(\mathbb{F}_p[A^\times])^\times=A^\times$.
3) Montrons que les ordres sont possibles.
En caractéristique nulle, ce sont les anneaux $\mathbb{Z},\mathbb{Z}[i],\mathbb{Z}[j]$ avec $i^2=-1$, $j^3=1$ et $j\neq 1$. En caractéristique p, c'est $A=\mathbb{F}_{p^m}$.

Lemme 4 *Soient A un anneau principal dont le groupe $A^\times$ des inversibles est fini. Alors A est soit un corps fini, soit un anneau admettant une infinité d'idéaux maximaux.*

Démonstration

1) Si A est un corps, alors $A^\times = A - \{0\}$, ainsi A est fini.

2) *On suppose maintenant que A n'est pas un corps.* Ainsi A contient au moins un idéal maximal. Il s'agit de montrer l'ensemble des idéaux maximaux de A est infini. Supposons le contraire, ainsi $\{\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_r\}$ est l'ensemble des idéaux maximaux de A. Il suit facilement de cela que $A = (\mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots \cup \mathfrak{M}_r) \cup A^\times$, en effet si $a \in A$ et $a \notin (\mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots \cup \mathfrak{M}_r)$, alors a est inversible puisque tout élément non-inversible est contenu dans un idéal maximal.

2.1) Supposons $\mathrm{car} A = 0$, alors $\mathbb{Z} \subset A$. Facilement $\mathfrak{M}_i \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$, ainsi $\mathfrak{M}_i \cap \mathbb{Z} = \{0\}$ ou $\mathfrak{M}_i \cap \mathbb{Z} = p_i\mathbb{Z}$ avec p_i irréductible. Si $\mathfrak{M}_i \cap \mathbb{Z} = \{0\}$ pour tout i, cela veut dire que $\mathbb{Z} - \{0\} \subset A^\times$, c'est impossible puisque $A^\times$ est fini. Sinon il existe $q_1, q_2, \ldots, q_s$ des irréductibles de $\mathbb{Z}$ avec $(\mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots \cup \mathfrak{M}_r) \cap \mathbb{Z} = q_1\mathbb{Z} \cup q_2\mathbb{Z} \cup \ldots \cup q_s\mathbb{Z}$. Il existe un irréductible q de $\mathbb{Z}$ avec $q \nmid q_1 q_2 \ldots q_s$ dans $\mathbb{Z}$, ce qui veut dire que $q \notin q_1\mathbb{Z} \cup q_2\mathbb{Z} \cup \ldots \cup q_s\mathbb{Z}$, donc $q \in A^\times$. Comme l'application $z \mapsto q^z$ de $\mathbb{N}$ dans $\mathbb{Z}$ est injective, il suit que $A^\times$ serait infini. Ce qui est une contradiction.

2.2) On suppose que $\mathrm{car} A = p$, alors on a $\mathbb{F}_p \subset A$, si tout élément de A est algébrique sur $\mathbb{F}_p$, cela veut dire que A est un corps, ce qui contredit notre hypothèse. Ainsi il existe $T \in A$ qui est transcendant sur $\mathbb{F}_p$, ainsi le sous-anneau de A engendré par $\mathbb{F}_p$ et T est isomorphe à l'anneau des polynômes à une variable à coefficients dans $\mathbb{F}_p$. Ensuite on procède comme en 2.1) pour aboutir à une contradiction.

Lemme 5 *Soit A un anneau principal.*

1. *Soit B un anneau fini, alors le nombre d'idéaux aA de A, tels que $\frac{A}{aA}$ est isomorphe à B, est fini.*
2. *Soit $N \geq 1$ un entier, alors le nombre d'idéaux aA de A, tels que $\mathrm{card}(\frac{A}{aA}) \leq N$, est fini.*

Démonstration

1) Il s'agit de montrer 1..

1.1) Si A est fini, comme A est intègre, c'est un corps, ainsi il y a seulement deux idéaux.

1.2) On suppose que A est infini et que $N = \mathrm{card}\, B$. Il existe donc $x_0, x_1, \ldots, x_N \in A$ et distincts. Soit $c := \prod_{0 \leq i < j \leq N} (x_i - x_j)$, alors l'image de c

dans $\frac{A}{aA}$ est nulle ; ce qui veut dire que $c=a\lambda$ avec $\lambda\in A$. Or le nombre de diviseur de c modulo les inversibles est fini. Ce qui montre que le nombre d'idéaux aA est fini.

2) Il s'agit de montrer 2. . Comme sur un ensemble fini, il y a seulement un nombre fini de structures d'anneaux, il suit qu'il y a seulement à isomorphisme près, un nombre fini d'anneaux B avec $\text{card}B\leq N$. Notons $\mathcal{B}$ cet ensemble. Si donc $\text{card}(\frac{A}{aA})\leq N$, il existe $B\in\mathcal{B}$ tel que $\frac{A}{aA}$ est isomorphe à B, il suit alors de 1. que le nombre d'idéaux aA, tels que $\text{card}\frac{A}{aA}\leq N$, est fini.

Lemme 6 *Soit A un anneau euclidien. On suppose que le groupe $A^\times$ des inversibles de A est fini. Alors pour tout $a\in A-\{0\}$, l'anneau $\frac{A}{aA}$ est fini.*

Démonstration

On peut supposer que l'algorithme euclidien $\varphi:A\to\mathbb{N}$ est surjectif et donc que $\varphi(0)=0$ et que $\varphi(A^\times)=\{1\}$.

Soient $n\geq 0$ et $A_n:=\{a\in A\mid \varphi(a)\leq n\}$. Montrons que A_n est fini et que pour tout $a\in A_n$ et $a\neq 0$, on a $\frac{A}{aA}$ qui est fini.

C'est bien vrai pour $n=1$, puisque si $a\in A_1$ et $a\neq 0$, on a $a\in A^\times$, alors $\frac{A}{aA}$ est l'anneau nul. Si $a\in A_n$, alors par division euclidienne par a, on a $A=aA+A_{n-1}$, il suit de cela que $\text{card}\frac{A}{aA}\leq\text{card}(A_{n-1})$. Si donc par hypothèse de récurrence sur n, on sait que $\text{card}(A_{n-1})$ est fini, alors on a $\text{card}\frac{A}{aA}$ qui est fini.

Par ailleurs le lemme 5 dit que le nombre d'idéaux aA tels que $\text{card}\frac{A}{aA}\leq\text{card}A_{n-1}$ est fini. Comme $A^\times$ est fini, il suit que le nombre de a tels que $\text{card}(\frac{A}{aA})\leq\text{card}A_{n-1}$ est fini, ainsi A_n est fini.

Comme pour tout $a\in A$, il existe $n\geq 0$ tel que $a\in A_n$, le lemme suit.

Bibliographie

[F] **Fresnel Jean** *Anneaux Hermann* 2001

[F, M] **Fresnel Jean & Matignon Michel** *Algèbre et Géométrie Hermann* 2011

[G] **Goldman Oscar** *On special class of Dedekind domains Topology Vol. 3, Suppl. 1, pp. 113-118. Pergamon Press. 1964*

[H] **Hiblot Jean-Jacques** *Sur les anneaux euclidiens Bull. Soc. math. France 104, 1976, p. 33-50*

[N] **Neukirch Jürgen** *Algebraic number theory Springer, Grundlehren der mathematischen Wissenschaften 322, 1999*

[S] **Samuel Pierre** *About Euclidean Rings Journal of Algebra 19, 282-301 (1971)*