# EXTENSIONS QUADRATIQUES D'UN ANNEAU PRINCIPAL

D.M. ALGÈBRE 1 - M1 MATHS

Tous les anneaux considérés sont commutatifs.

**A. Compléments sur les anneaux.**

A1. Montrer qu'un anneau $A$ est principal si et seulement s'il est intègre, noethérien et tout idéal maximal est principal.

*Indications.* Pour montrer le sens non trivial, montrer tout d'abord que $A$ est factoriel. Pour démontrer ensuite que tout idéal $I$ est principal, se réduire au cas où $I = (a, b)$, avec $a$ et $b$ non nuls. Justifier l'existence de $d, \alpha, \beta \in A$ tels que $a = d\alpha, b = d\beta$, avec $\alpha$ et $\beta$ premiers entre eux. Montrer enfin par l'absurde que $(\alpha, \beta) = A$ en utilisant la principalité des idéaux maximaux.

A2. Soit $(A, \delta)$ un anneau euclidien. Montrer qu'il existe $x \in A \setminus A^\times$, tel que la restriction à $A^\times \cup \{0\}$ de la projection canonique $\pi : A \longrightarrow A/(x)$ est surjective.

*Indications.* Traiter à part le cas où $A$ est un corps. Si $A$ n'est pas un corps, choisir $x \in A \setminus A^\times$ tel que $\delta(x)$ est minimal.

A3. Soit $f : A \longrightarrow B$ un morphisme d'anneaux surjectif.

(a) Soit $\mathfrak{m}$ un idéal de $B$. Montrer que l'on a un isomorphisme d'anneaux

$$A/f^{-1}(\mathfrak{m}) \simeq B/\mathfrak{m}.$$

En déduire que $\mathfrak{m}$ est maximal si et seulement si $f^{-1}(\mathfrak{m})$ est maximal.

($b$) Soit $\mathfrak{M}$ un idéal de $A$ contenant $\ker(f)$. Montrer que l'on a un isomorphisme d'anneaux

$$A/\mathfrak{M} \simeq B/f(\mathfrak{M}).$$

En déduire que $f(\mathfrak{M})$ est maximal si et seulement si $\mathfrak{M}$ est maximal.

**B. Anneaux intégralement clos.**

Soit $A$ un anneau intègre, de corps des fractions $K_A$, et soit $L/K_A$ une extension de corps. Un élément de $L$ est dit *entier sur* $A$ s'il est racine d'un polynôme **unitaire** à coefficients dans $A$.

On note $\mathcal{O}_L$ l'ensemble des éléments de $L$ qui sont entiers sur $A$.

B1. Montrer $\mathcal{O}_L$ est un sous-anneau de $L$ contenant $A$.

*Indications.* Soient $\alpha, \beta \in \mathcal{O}_L$, et soient $f, g \in A[X]$ unitaires tels que $f(\alpha) = 0$ et $g(\beta) = 0$, de degrés respectifs $n$ et $m$. Montrer que les polynômes

$$F = \prod_{j=1}^{m} f(X - Y_j)\,, G = \prod_{j=1}^{m} Y_j^n f(X/Y_j) \in A[X, Y_1, \dots, Y_m]$$

sont des éléments de $A[\sigma_1, \ldots, \sigma_m, X]$, où les $\sigma_j$ sont les polynômes symétriques élémentaires en $Y_1, \ldots, Y_m$. Quelles sont les racines de $F$ et $G$ en fonction des racines de $f$ (dans une extension convenable) et des $Y_j$ ?

Un anneau intègre $A$ est dit *intégralement clos* si $\mathcal{O}_{K_A} = A$, c'est-à-dire si les éléments de $K_A$ qui sont entiers sur $A$ sont exactement les éléments de $A$.

B2. Montrer qu'un anneau factoriel est intégralement clos.

B3. Pour chacun des anneaux suivants, dire s'il est intégralement clos ou non (justifier la réponse) : $\mathbb{Q}, \mathbb{Z}[X], \mathbb{Z}[\sqrt{5}]$.

B4. Soit $A$ un anneau intégralement clos, et soit $f \in A[X]$ un polynôme unitaire. Soit $g \in K_A[X]$ unitaire tel que $g \mid f$ dans $K_A[X]$. Montrer que $g \in A[X]$.

*Indications.* Considérer une extension $E/K_A$ dans laquelle $f$ a toutes ses racines et utiliser 1.

B5. Soit $A$ un anneau intégralement clos, et soit $\alpha \in L$ algébrique sur $K_A$. Montrer que $\alpha \in \mathcal{O}_L$ si et seulement si $\mathrm{Irr}(\alpha, K_A) \in A[X]$.

B6. Soit $A$ un anneau intégralement clos, et soit $f \in A[X]$ un polynôme irréductible unitaire. Montrer que $f$ est irréductible dans $K_A[X]$.

B7. Soit $A$ un anneau intègre. On suppose que tout polynôme $f \in A[X]$ unitaire irréductible reste irréductible sur $K_A[X]$. Montrer que $A$ est intégralement clos.

*Indications.* si $\alpha \in K_A$ est entier sur $A$, démontrer tout d'abord l'existence d'un polynôme $g \in A[X]$ unitaire **irréductible** dans $A[X]$ tel que $g(\alpha) = 0$.

B8. On prend $A = \mathbb{Z}$ et $L = \mathbb{C}$. Montrer que $\mathcal{O}_L$ n'est pas un corps et que $\mathcal{O}_L$ est stable par racine carrée. En déduire que $\mathcal{O}_L$ ne possède pas d'éléments irréductibles.

### C. Extensions quadratiques d'un anneau factoriel : propriétés.

Soit $A$ un anneau, et soit $\rho \in A \setminus \{0\}$. On pose

$$A[\sqrt{\rho}] = A[T]/(T^2 - \rho).$$

Il est facile de vérifier que l'application évidente $A \longrightarrow A[\sqrt{\rho}]$ est injective. On identifie alors $A$ avec son image dans $A[\sqrt{\rho}]$. Si $\alpha = \overline{T}$, avec cette identification, tout élément de $A[\sqrt{\rho}]$ s'écrit de manière **unique** sous la forme $u + v\alpha, u, v \in A$. Autrement dit, on a

$$A[\sqrt{\rho}] = \{z = u + v\alpha \mid u, v \in A\},$$

où $\alpha$ vérifie $\alpha^2 = \rho$.

On définit aussi une application

$$\begin{aligned} N \colon K_A[\sqrt{\rho}] &\longrightarrow K_A \\ x + y\alpha &\longmapsto x^2 - \rho y^2. \end{aligned}$$

On vérifie que $N(z_1 z_2) = N(z_1)N(z_2)$ pour tous $z_1, z_2 \in K_A[\sqrt{\rho}]$, et que si $z \in A[\sqrt{\rho}]$, on a $N(z) \in A$. Enfin, si de plus $\rho$ n'est pas un carré dans $K_A$, alors pour tout $z \in K_A[\sqrt{\rho}]$, on a $N(z) = 0 \iff z = 0$.

C1. Montrer que $A[\sqrt{\rho}]$ est noethérien.

C2. Soit $A$ un anneau intègre. On suppose que $\rho$ n'est un pas un carré dans $K_A$. Montrer que $A[\sqrt{\rho}]$ est intègre, et que son corps des fractions s'identifie à $K_A[\sqrt{\rho}]$.

C3. On suppose dans cette question que $A$ est un anneau principal. Le but est de déterminer les idéaux maximaux non nuls de $A[\sqrt{\rho}]$. Soit $\mathfrak{m}$ un idéal maximal non nul de $A[\sqrt{\rho}]$. On note $\mathfrak{M}$ l'image réciproque de $\mathfrak{m}$ par le morphisme surjectif

$$\begin{aligned} A[T] &\longrightarrow A[\sqrt{\rho}] \\ P &\longmapsto P(\sqrt{\rho}). \end{aligned}$$

(a) Montrer que $\mathfrak{M} \cap A$ est un idéal premier non nul. En déduire qu'il existe un élément irréductible $\pi \in A$ tel que $\mathfrak{M} \cap A = (\pi)$.

*Indications.* Si $z \in \mathfrak{m} \setminus \{0\}$, montrer que $N(z) \in \mathfrak{M} \cap A$.

(b) Soit $\tilde{\mathfrak{M}} \subset A/(\pi)[T]$ l'image de $\mathfrak{M}$ par la réduction modulo $\pi$.

Montrer que $\tilde{\mathfrak{M}}$ est un idéal maximal de $A/(\pi)[T]$. En déduire l'existence d'un polynôme unitaire $f \in A[T]$ dont la réduction $\tilde{f}$ modulo $\pi$ est irréductible et vérifiant $\tilde{\mathfrak{M}} = (\tilde{f})$.

(c) Vérifier que $T^2 - \tilde{\rho} \in \mathfrak{M}$. En déduire **soigneusement** que $\tilde{\mathfrak{M}}$ contient un polynôme de $A/(\pi)[X]$ de la forme $T - \tilde{u}, u \in A$.

($d$) Montrer que $(\pi, T-u) \subset \mathfrak{M}$, puis que $\mathfrak{M} = (\pi, T-u) = (\pi, T-u, T^2-\rho)$

*Indications.* Montrer que $(\pi, T-u)$ est un idéal maximal de $A[T]$.

($e$) Montrer que l'on a des isomorphismes

$$A[T]/(T^2-\rho, \pi, T-u) \simeq A/(\pi)[T]/(T^2-\tilde{\rho}, T-\tilde{u}) \simeq A/(\pi)/(\tilde{u}^2-\tilde{\rho}).$$

En déduire que $(T^2-\rho, \pi, T-u)$ est maximal si et seulement si $\tilde{\rho} = \tilde{u}^2 \in A/(\pi)$.

($f$) En déduire que les idéaux maximaux non nuls de $A[\sqrt{\rho}]$ sont les idéaux de la forme $(\pi, \alpha - u)$, où $\pi, u \in A$, $\pi$ est irréductible dans $A$, et $\tilde{\rho} = \tilde{u}^2 \in A/(\pi)$.

Dans la suite, on suppose que $A$ est un anneau factoriel, et on fixe une fois pour toute un s.c.r.i. $\mathcal{P}$. Si $\pi \in \mathcal{P}$, et $a \in A$, on note $v_\pi(a)$ la valuation $\pi$-adique de $a$.

Jusqu'à la fin de cette partie, on suppose que $\rho$ est non nul, non inversible, et sans facteurs carrés (i.e. $\rho$ est produit d'un inversible et d'éléments premiers deux à deux distincts).

C3. Montrer que si $z = u + v\alpha \in A[\sqrt{\rho}]$, et si $\pi$ est un élément irréductible divisant $\rho$, on a $v_\pi(N(z)) = \min(2v_\pi(u), 2v_\pi(v)+1)$.

En déduire que $\alpha$ est un élément irréductible de $A[\sqrt{\rho}]$.

*Indications.* Montrer que $\alpha$ est non nul et non inversible, et soit $\pi$ un diviseur irréductible de $\rho$ fixé. Si $\alpha = z_1 z_2, z_i \in A[\sqrt{\rho}]$, montrer que l'on peut supposer que $v_\pi(N(z_1)) = 1$. En utilisant le premier point, montrer que $u_1 = 0$ et conclure.

C4. Montrer que $A[\sqrt{\rho}]/(\alpha) \simeq A/(\rho)$. En déduire que si $\rho$ n'est pas un élément irréductible de $A$, alors $A[\sqrt{\rho}]$ n'est pas factoriel. Si $\rho$ est irréductible, l'anneau $A[\sqrt{\rho}]$ est-il factoriel ?

C5. On suppose que $2 \in A^\times$. Montrer que $A[\sqrt{\rho}]$ est intégralement clos. Le résultat subsiste-t-il si 2 n'est pas inversible ?

*Indications.* Si $x + y\sqrt{\rho} \in K_A[\sqrt{\rho}]$ est entier sur $A[\sqrt{\rho}]$, montrer que $x + y\sqrt{\rho}$ est entier sur $A$. Utiliser les résultats de la partie B. et l'hypothèse pour montrer que $x$

et $\rho y^2$ sont des éléments de $A$. Écrire $y = y_1/y_2$, avec $y_1$ et $y_2$ premiers entre eux, et conclure.

Il existe ainsi des anneaux intégralement clos non factoriels.

**D. Étude d'une famille d'exemples.**

Dans cette partie, on prend $A = \mathbb{R}[X]$. On suppose que $\rho$ est non nul, sans facteurs carrés.

D1. Montrer que tout idéal maximal de $A[\sqrt{\rho}]$ est de la forme $(X - a, \alpha - b)$, avec $a, b \in \mathbb{R}$ tels que $\rho(a) = b^2$, ou de la forme $(\pi, \alpha - U(X))$, où $\pi \in \mathbb{R}[X]$ est irréductible unitaire de degré 2, et $U$ est de degré $\leq 1$ tels que $\pi \mid (\rho - U^2)$.

D2. On suppose dans cette question que $\rho = -(X^2 + 1)$. Soit $\mathfrak{m}$ un idéal maximal de $A[\sqrt{\rho}]$.

(a) Montrer que $A[\sqrt{\rho}]$ ne possède pas d'idéal maximal de la forme $(X - a, \alpha - b), \rho(a) = b^2$.

(b) On suppose que $\mathfrak{m} = (\pi, \alpha - U(X))$, où $\pi \in \mathbb{R}[X]$ est irréductible unitaire de degré 2, et $U$ est de degré $\leq 1$ tels que $\pi \mid (\rho - U^2)$. Montrer que $\rho - U^2 = c\pi, c \in \mathbb{R}^\times$, et en déduire que $\mathfrak{m} = (\alpha - U(X))$.

(c) En déduire que $A[\sqrt{\rho}]$ est principal.

(d) Montrer que $A[\sqrt{\rho}]^\times = \mathbb{R}^\times$.

*Indications.* Si $z = U + V\alpha$ est inversible, montrer que $U^2 - \rho V^2 = \lambda \in \mathbb{R}^{+\times}$. Écrire $U = \rho Q + aX + b, Q \in \mathbb{R}[X], a, b \in \mathbb{R}$, et évaluer en $\pm i$.

(e) Montrer par l'absurde que $A[\sqrt{\rho}]$ n'est pas euclidien.

On revient au cas général.

Le but de les questions suivantes est d'étudier la principalité de $A[\sqrt{\rho}]$.

D1. Étudier la principalité de $A[\sqrt{\rho}]$ lorsque que $\rho$ est non constant et non irréductible.

D2. On suppose que $\rho$ est constant ou irréductible. En utilisant des changements de variables linéaires adéquats et les résultats de la partie A., montrer que l'on a les isomorphismes suivants :

(a) $A[\sqrt{\rho}] \simeq \mathbb{R}[X][T]/(T^2 - 1)$ si $\rho$ est constant $> 0$ ;

(b) $A[\sqrt{\rho}] \simeq \mathbb{R}[X][T]/(T^2 + 1)$ si $\rho$ est constant $< 0$ ;

(c) $A[\sqrt{\rho}] \simeq \mathbb{R}[X][T]/(T^2 - X)$ si $\rho$ est de degré 1 ;

(d) $A[\sqrt{\rho}] \simeq \mathbb{R}[X][T]/(T^2 - (X^2 + 1)) \simeq \mathbb{R}[X][T]/(T^2 - (X^2 - 1))$ si $\rho$ est irréductible de degré 2, de signe $> 0$ ;

(e) $A[\sqrt{\rho}] \simeq \mathbb{R}[X][T]/(T^2 + (X^2 + 1))$ si $\rho$ est irréductible de degré 2, de signe $< 0$ ;

D3. Étudier la principalité de $A[\sqrt{\rho}]$ dans les cas (a)-(d), et en déduire une condition nécessaire et suffisante sur $\rho$ pour que $A[\sqrt{\rho}]$ soit principal.

*Indications.* Pour le cas (c), montrer que $A[\sqrt{\rho}]$ est isomorphe à $\mathbb{R}[T]$.