Devoir maison

Alexandre Guillemot

6 novembre 2022

1 Préliminaires et divers

1. Le morphisme canonique $\pi : R \to R/I$ induit une bijection entre les idéaux de R contenant I et les idéaux de R/I (en envoyant un tel idéal $I \subseteq J \overset{\text{id}}{\subseteq} R$ sur $\pi(I)$). Alors remarquons que

$$\begin{aligned}\pi(\sqrt{I}) &= \{\pi(x) \in R/I \mid x \in \sqrt{I}\} \\ &= \{\pi(x) \in R/I \mid x \in R \text{ et } \exists N \in \mathbb{N},\, x^N \in I\} \\ &= \{\pi(x) \in R/I \mid x \in R \text{ et } \exists N \in \mathbb{N},\, \pi(x)^N = 0\} \\ &= \{y \in R/I \mid \exists N \in \mathbb{N},\, y^N = 0\} = \sqrt{(0)}\end{aligned}$$

(Plus généralement on a $\pi(\sqrt{J}) = \sqrt{\pi(J)}$ pour tout $I \subseteq J \overset{\text{id}}{\subseteq} R$). Ainsi si $I = \sqrt{I}$, alors $\sqrt{(0)} = \pi(I) = \{0\}$, et si $\sqrt{(0)} = \{0\}$, $\pi(\sqrt{I}) = \{0\}$ et donc $\sqrt{I} \subseteq I$, d'où $\sqrt{I} = I$.

2. Pour calculer la dimension d'un idéal, on calcule une famille génératrice de $I \cap k[y_1, \cdots, y_n]$ pour tout $\{y_1, \cdots, y_d\} \subseteq \{x_1, \cdots, x_n\}$, et on renvoie le plus grand d tel que $I \cap k[y_1, \cdots, y_n] = \{0\}$: A finir

Algorithm 1 Calcule la dimension de l'idéal $I = \langle f_1, \cdots, f_r \rangle \overset{\text{id}}{\subseteq} k[x_1, \cdots, x_n]$

```
function IDEAL DIMENSION(f_1, ..., f_r ∈ k[x_1, ..., x_n])
    G ← Groebner_basis(f_1, ..., f_n)
    for {y_1, ... y_d} ⊆ {x_1, ..., x_n} do
    end for
end function
```

3.

Considérons la factorisation en irréductibles unitaires

$$h = \lambda \prod_{i=1}^{s} h_i^{\alpha_i} \tag{1}$$

où $\lambda \in L$, $h_i \in L[x_1, \cdots, x_n]$ sont deux à deux distincts et $\alpha_i \in \mathbb{Z}_{>0}$. Alors considérons $\ell = \prod_{i=1}^{s} h_i$, comme les h_i sont deux à deux distincts, ℓ est sans carré. Maintenant soit $f \in L[x_1, \cdots, x_n]$ sans facteurs carrés, tel que $f \mid h$, alors f s'écrit comme

$$f = \lambda' \prod_{i=1}^{s} h_i^{\beta_i}$$

avec $\lambda' \in L$, $0 \leq \beta_i \leq \alpha_i$ pour tout $1 \leq i \leq s$. Mais comme f est sans facteurs carrés, on doit avoir que pour tout $1 \leq i \leq s$, $\beta_i \leq 1$, et ainsi $f \mid g$. Finalement, si on dispose d'un autre tel diviseur sans carré maximal l', alors $\ell \mid \ell'$ et $\ell' \mid \ell$, donc ℓ et ℓ' sont associés dans $L[x_1, \cdots, x_n]$, i.e. $\exists \mu \in L$ tel que $\ell = \mu \ell'$ et donc ℓ est unique à multiplication par un scalaire près.

Montrons que $\sqrt{\langle h \rangle} = \langle \ell \rangle$:

1. $\supseteq$: Il suffit de montrer que $\ell \in \sqrt{\langle h \rangle}$: Pour cela, considérons $\alpha := \max_{1 \leq i \leq s}\{\alpha_i\}$, alors $h \mid \ell^\alpha$ au vu de la définition de ℓ, et donc $\ell^\alpha \in \langle h \rangle$, i.e. $\ell \in \sqrt{\langle h \rangle}$.
2. $\subseteq$: Soit $f \in \sqrt{\langle h \rangle}$, alors $\exists N \geq 0$ tel que $f^N \in \langle h \rangle$, i.e. $\exists N \geq 0$ et $g \in L[x_1, \cdots, x_n]$ tels que $f^N = gh$. Maintenant pour tout $1 \leq i \leq s$, $h_i \mid gh$ donc $h_i \mid f^N$, et comme h_i est irréductible, $h_i \mid f$, et donc finalement $\ell = \prod h_i \mid f$ puisque les h_i sont irréductibles et distincts deux à deux.

2 Cas d'un idéal de dimension nulle

1.

Pour calculer les h_i, on calcule une base de grobner G pour I et l'ordre lexicographique induit par $x_1 < x_2 < \cdots < x_{i-1} < x_{i+1} < \cdots < x_n < x_i$, puis on intersecte G avec $k[x_i]$. Ainsi d'après le théorème d'élimination, $k[x_i] \cap G$ est une base de Groebner pour $k[x_i] \cap I$, donc en particulier un ensemble générateur. Il suffit alors de prendre le plus petit élément pour la relation de divisibilité dans $k[x_i] \cap G$. Remarquons que si la base G calculée est réduite, alors on ne peut pas avoir deux éléments dans $G \cap k[x_i]$ (car si on a au moins deux éléments le terme dominant de l'un doit diviser le terme dominant de l'autre), ce qui contredit la définition d'une base de Groebner réduite. Ainsi dans ce cas il suffit de prendre un (le seul !) élément de $G \cap k[x_i]$.

PGCD du polynome et de sa dérivée ?

2. On a $I \subseteq \sqrt{I}$, puis $\ell_i \in \sqrt{\langle h_i \rangle}$ d'après la question 3, et $h_i \in I$ donc $\sqrt{\langle h_i \rangle} \subseteq \sqrt{I}$. Ainsi $I + \langle l_1, \cdots, l_n \rangle \subseteq \sqrt{I}$.

3.a. Rappelons le théorème des restes chinois dans un anneau principal :

Théorème 2.1. *Soit R un anneau principal, puis $\{x_i\}_{1\leq i\leq s} \subseteq R$ une famille d'éléments premiers entre eux deux à deux [$\langle x_i\rangle + \langle x_j\rangle = R$ pour tout $i \neq j$]. Notons $x = \prod_{i=1}^{s} x_i$, alors*

$$R/\langle x\rangle \simeq \prod_{i=1}^{s} (R/\langle x_i\rangle)$$

Démonstration. A faire ? □

Or ici on peut écrire $\ell_1 = \lambda \prod_{i=1}^{s} \ell_1^i$, où les ℓ_1^i sont irréductibles et différents deux à deux (donc premier entre eux deux à deux). Remarquons tout de suite que λ n'a pas d'importance, puisque $\langle \ell\rangle = \langle \ell/\lambda\rangle$, et ainsi on peut supposer que $\lambda = 1$. Finalement, d'après le théorème, on a bien

$$k[x_1]/\langle \ell_1\rangle \simeq \prod_{i=1}^{s} k[x_1]/\left\langle \ell_1^i\right\rangle$$

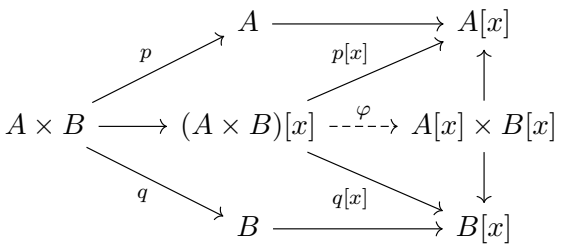
et les $k[x_1]/\left\langle \ell_1^i\right\rangle$ sont des extensions finies de k vu que les ℓ_1^i sont irréductibles.

3.b. Montrons plus généralement que

Lemme 2.1. *Soient A, B des anneaux commutatifs, alors*

$$(A \times B)[x] \simeq A[x] \times B[x]$$

Démonstration. On dispose d'un morphisme canonique $(A \times B)[x] \to A[x] \times B[x]$, induit par les morphismes $(A \times B)[x] \to A[x]$ et $(A \times B)[x] \to B[x]$, eux-mêmes induits par les projections canoniques $A \times B \to A$, $A \times B \to B$:



Comme le foncteur d'oubli des anneaux commutatifs vers les groupes abéliens réfléchis les isomorphismes (en effet, le foncteur d'oubli **CRings** $\to$ **Sets** les réfléchis, du fait qu'un morphisme d'anneau est un isomorphisme s'il est bijectif), il suffit de vérifier que φ est un isomorphisme vu comme un morphisme de groupes abéliens. Maintenant pour tout anneau

commutatif C, $C[x] \simeq \bigoplus_{\mathbb{N}} C$ en tant que groupes abéliens, et au travers de cet isomorphisme φ correspond au morphisme canonique

$$\bigoplus_{\mathbb{N}} (A \oplus B) \to \left(\bigoplus_{\mathbb{N}} A\right) \oplus \left(\bigoplus_{\mathbb{N}} B\right)$$

qui est bien un isomorphisme dans la catégorie des groupes abéliens (puisque les colimites commutent toujours avec les colimites). □

Finalement, par récurrence on conclut que le lemme précédent est vrai pour n'importe quel produit fini d'anneaux, et donc en particluier pour n'importe quel produit fini d'extensions finies d'un corps k.

3.c. Comme précédemment, considérons un anneau commutatif C, et deux C-algèbres A et B, puis un élément $\ell \in C[x]$. Alors si on regarde ℓ comme un élément de $A[x]$ et $B[x]$ via $C[x] \to A[x]$ et $C[x] \to B[x]$, on a

$$A[x]/\langle \ell \rangle \times B[x]/\langle \ell \rangle \simeq (A[x] \times B[x])/\langle (\ell, \ell) \rangle$$

(Plus généralement on a $A/I \times B/J \simeq (A \times B)/(I \times J)$ avec A, B des anneaux commutatifs et $I \overset{\text{id}}{\subseteq} A$, $J \overset{\text{id}}{\subseteq} B$). Maintenant A finir, de manière élémentaire si pas le temps

3.d. Dans cette question, on regarde les éléments de $k[x_1, \cdots, x_{t+1}]$ comme des éléments de $k[x_1, \cdots, x_t][x_{t+1}]$. Alors considérons les morphismes

$$\begin{aligned}
&p : k[x_1, \cdots, x_t] \to k[x_1, \cdots, x_t]/\langle \ell_1, \cdots, \ell_t \rangle \\
&p[x_{t+1}] : k[x_1, \cdots, x_t][x_{t+1}] \to (k[x_1, \cdots, x_t]/\langle \ell_1, \cdots, \ell_t \rangle)[x_{t+1}] \\
&q : (k[x_1, \cdots, x_t]/\langle \ell_1, \cdots, \ell_t \rangle)[x_{t+1}] \to (k[x_1, \cdots, x_t]/\langle \ell_1, \cdots, \ell_t \rangle)[x_{t+1}]/\langle \ell_{t+1} \rangle
\end{aligned}$$

où ℓ_{t+1} est un abus de notation pour $p[x_{t+1}](\ell_{t+1})$ dans le membre de droite du dernier morphisme. Alors déjà pour tout $1 \leq i \leq t$, $p[x_{t+1}](\ell_i) = 0$ (vu que $p(\ell_i) = 0$) et donc $(q \circ p[x_{t+1}])(\ell_i) = 0$, puis $(q \circ p[x_{t+1}])(\ell_{t+1}) = 0$, donc $\langle \ell_1, \cdots, \ell_{t+1} \rangle \subseteq \ker(q \circ p[x_{t+1}])$. Pour l'inclusion réciproque, prenons $P \in k[x_1, \cdots, x_t][x_{t+1}]$ qui vérifie $(q \circ p[x_{t+1}])(P) = 0$. Alors on peut écrire $p[x_{t+1}](P) = p[x_{t+1}](Q_{t+1})p[x_{t+1}](\ell_{t+1})$ pour un certain $Q_{t+1} \in k[x_1, \cdots, x_n]$, et ainsi $p[x_{t+1}](P - Q_{t+1}\ell_{t+1}) = 0$, et donc il existe $Q_1, \cdots, Q_t$ tels que

$$P - Q_{t+1}\ell_{t+1} = \sum_{i=1}^{t} Q_i \ell_i$$

et donc $P \in \langle \ell_1, \cdots, \ell_{t+1} \rangle$. On a donc prouvé que

$$k[x_1, \cdots, x_{t+1}]/\langle \ell_1, \cdots, \ell_{t+1} \rangle \simeq (k[x_1, \cdots, x_t]/\langle \ell_1, \cdots, \ell_t \rangle)[x_{t+1}]/\langle \ell_{t+1} \rangle$$

3.e. Prouvons par récurrence que pour tout $t \geq 1$, $R/\langle \ell_1, \cdots, \ell_t \rangle$ est un produit d'extensions finies de k. Si $t = 1$, $R/\langle \ell_1 \rangle$ est un produit d'extensions finies de corps, d'après la question 3.a.. Maintenant par récurrence, on a vu à la question précédente que

$$k[x_1, \cdots, x_{t+1}]/\langle \ell_1, \cdots, \ell_{t+1} \rangle \simeq \left(k[x_1, \cdots, x_t]/\langle \ell_1, \cdots, \ell_t \rangle\right)[x_{t+1}]/\langle \ell_{t+1} \rangle$$

Alors par hypothèse de récurrence, $k[x_1, \cdots, x_t]/\langle \ell_1, \cdots, \ell_t \rangle$ est un produit d'extensions finies de corps : notons

$$k[x_1, \cdots, x_t]/\langle \ell_1, \cdots, \ell_t \rangle \simeq \prod_{i=1}^{s} F_i$$

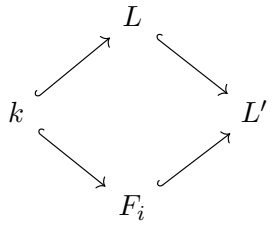
Maintenant d'après la question 3.c. on a

$$\left(\prod_{i=1}^{s} F_i\right)[x_{t+1}]/\langle \ell_{t+1} \rangle \simeq \prod_{i=1}^{s} F_i[x_{t+1}]/\langle \ell_{t+1} \rangle$$

Il reste donc à montrer que $F_i[x_{t+1}]/\langle \ell_{t+1} \rangle$ est un produit d'extensions finies de k. Pour cela, décomposons ℓ_{t+1} dans $k[x_{t+1}]$ en irréductibles (deux à deux disjoints puisque ℓ_{t+1} est sans facteurs carrés) :

$$\ell_{t+1} = \lambda \prod_{j=1}^{r} f_j$$

avec $f_j \in k[x_{t+1}]$ pour tout $1 \leq j \leq r$. Maintenant comme les f_j sont irréductibles et que k est parfait, ils sont sans facteurs carrés dans $F_i[x_{t+1}]$: en effet, notons L, L' respectivement des corps de décomposition pour $f_j \in k[x_{t+1}]$ et $f_j \in F_i[x_{t+1}]$, alors comme L' est une extension de k dans laquelle f_j est scindé, c'est une extension de L telle que le diagramme



commute. Maintenant si f_j à un facteur carré dans F_i, alors il a au moins une racine multiple dans L', ce qui est absurde puisqu'il n'a pas de racine multiple dans L (comme k est parfait) donc dans L'. Finalement, les f_j sont sans facteurs carrés, et doivent encore être premiers entre eux deux à deux (réaliser l'algorithme de gcd sur $F_i[x_{t+1}]$ ou sur $k[x_{t+1}]$ doit donner le même résultat, mais il donne un élément de k dans $k[x_{t+1}]$), donc ℓ_{t+1} est

encore sans facteurs carrés dans $F_i[x_{t+1}]$, et on utilise de nouveau le théorème des restes chinois pour conclure que $F_i[x_{t+1}]/\langle \ell_{t+1}\rangle$ est un produit d'extensions finies de k, pour tout $1 \leq i \leq s$.

4.

Dans un premier temps, si A, B sont des anneaux commutatifs, alors un idéal de $A \times B$ peut toujours s'écrire comme $I \times J$ avec $I, J \overset{\text{id}}{\subseteq} A, B$. En effet, si $K \overset{\text{id}}{\subseteq} A \times B$, alors considérons $I := \{i \in A \mid (i,0) \in K\}$, $J := \{j \in B \mid (0,j) \in K\}$. Alors déjà, $K = I \times J$ puisque si $(i,j) \in K$, alors $(1,0) \times (i,j) = (i,0) \in K$ donc $i \in I$, puis de même, $j \in J$. Ensuite si $i \in I$, $j \in J$, alors $(i,j) = (i,0) + (0,j) \in K$. Enfin I, J sont bien des idéaux du fait que K est un idéal. Enfin, par récurrence, on a le même résultat pour un produit fini d'anneaux commutatifs.

Ensuite, considérons un produit de corps $S = \prod_{i=1}^{s} K_i$, alors les idéaux des K_i sont soit K_i tout entier, soit $\{0\}$, et comme un idéal I de S est un produit d'idéaux des K_i, on peut l'écrire $I = \prod_{i=1}^{s} I_i$ avec $I_i = K_i$ ou $\{0\}$. Ainsi un quotient d'un produit de corps est encore un produit de corps (du fait que l'on a toujours $(A \times B)/(I \times J) \simeq A/I \times B/J$ avec $I, J \overset{\text{id}}{\subseteq} A, B \in \mathbf{CRings}$). Mais si $x = (x_1, \cdots, x_s) \in S = \prod_{i=1}^{s} K_i$ est un élément d'un produit de corps, tel que $x^N = 0$ pour un certain $N > 0$, alors $x_i^N = 0 \in K_i$ pour tout i et donc $x_i = 0$ par intégrité de K_i, ce qui prouve que $x = 0$ et donc S est réduit.

Pour conclure, il faut remarquer que pour tout A anneau commutatif, $I, J \overset{\text{id}}{\subseteq} A$, si on note $\pi : A \to A/I$, on a $A/(I+J) \simeq (A/I)/\pi(J)$. A faire ?. Ainsi

$$R/I + \langle \ell_1, \cdots, \ell_n\rangle \simeq (R/\langle \ell_1, \cdots, \ell_n\rangle)/\pi(I)$$

où $\pi : R \to R/\langle \ell_1, \cdots, \ell_n\rangle$ désigne la projection canonique. Mais comme $R/\langle \ell_1, \cdots, \ell_n\rangle$ est un produit de corps, on en conclut par le point précédent que $R/\langle \ell_1, \cdots, \ell_n\rangle + I$ est un anneau réduit.

5. D'après la question 1. des préliminaires, $I + \langle \ell_1, \cdots, \ell_n\rangle = \sqrt{I + \langle \ell_1, \cdots, \ell_n\rangle}$, et $\sqrt{I} \subseteq \sqrt{I + \langle \ell_1, \cdots, \ell_n\rangle}$, donc $\sqrt{I} \subseteq I + \langle \ell_1, \cdots, \ell_n\rangle$. On conclut, grâce à la question 2., que

$$\sqrt{I} = I + \langle \ell_1, \cdots, \ell_n\rangle$$

6.

3 Problème d'appartenance au radical

1. Prouvons l'implication directe : supposons que $f \in \sqrt{I}$, alors $\exists n > 0$ tel que $f^n \in I$. Mais il existe $Q \in k[x_1, \cdots, x_n, t]$ tel que $f^n t^n - 1 = (ft-1)Q$, et donc

$$1 = f^n t^n - (ft-1)Q \in \langle I, ft-1\rangle$$

2.a Pour prouver l'implication réciproque, on procède par contraposée : supposons que $f \notin \sqrt{I}$, comme K est algébriquement clos, $f \notin \mathcal{I}(\mathcal{V}(I))$ (Nullstellensatz de Hilbert). Ainsi il existe $\underline{p} \in \mathcal{V}(I)$ tel que $f(\underline{p}) \neq 0$, et comme $\underline{p} \in \mathcal{V}(I)$, $g(\underline{p}) = 0$ pour tout $g \in I$.

2.b Si $g \in I$, alors $\varepsilon(g) = g(\underline{p}) = 0$, et $\varepsilon(ft-1) = f(\underline{p})f(\underline{p})^{-1} - 1 = 0$, donc on a bien $\langle I, ft-1\rangle \subseteq \ker\varepsilon$. Enfin, $\varepsilon(f) = f(\underline{p}) \neq 0$ donc $f \in k[x_1, \cdots, x_n, t] \setminus \ker\varepsilon$, et ainsi $\langle I, ft-1\rangle \subseteq \ker\varepsilon \nsubseteq k[x_1, \cdots, x_n, t]$. Ainsi $k[x_1, \cdots, x_n, t]/\langle I, ft-1\rangle \neq \{0\}$, et donc $1 \notin \langle I, ft-1\rangle$.