Université de Lille

Master Mathématiques, 2020-21

Feuille d'exercices 6

§1. Complétion

1. Quiz

Soit R un anneau complet pour la filtration par rapport aux puissances d'un idéal I, c'est à dire tel que $R = \lim_k R/I^k$. Soit $J = I^m$ une puissance de cet idéal. Montrer que R est également complet pour la filtration par rapport aux puissances de l'idéal J, soit $R = \lim_k R/J^k$.

2. Exercice

Soit R un anneau complet pour la filtration par rapport aux puissances d'un idéal I, c'est à dire tel que $R = \lim_k R/I^k$. On note $q_0 : R \to R/I$ le morphisme canonique. On a immédiatement $\alpha \in R^\times \Rightarrow q_0(\alpha) \in (R/I)^\times$, puisque pour $\beta = \alpha^{-1}$ la relation $\alpha\beta = 1$ entraîne $q_0(\alpha)q_0(\beta) = 1$.

Le but de cet exercice est de prouver l'assertion réciproque de cette propriété. On se donne un système $\bar{a}_k \in R/I^{k+1}$, $k \geq 0$, tel que $a_k \equiv a_{k-1} (\mathrm{mod}\, I^k)$ représentant notre élément α. On suppose $\bar{a}_0 \in (R/I)^\times$ de sorte qu'il existe $b_0 \in R$ tel que $a_0 b_0 \equiv 1 (\mathrm{mod}\, I)$. On construit par récurrence une suite $\bar{b}_k \in R/I^{k+1}$, $k \geq 0$, tel que $b_k \equiv b_{k-1} (\mathrm{mod}\, I^k)$ et $a_k b_k \equiv 1 (\mathrm{mod}\, I^k)$.

On suppose cette suite construite jusqu'au rang $k-1$. On écrit $x_k = a_k - a_{k-1}$, de sorte que $a_k = a_{k-1} + x_k$ et $a_k \equiv a_{k-1} (\mathrm{mod}\, I^k) \Leftrightarrow a_k \in I^k$. On cherche b_k sous la forme $b_k = b_{k-1} + y_k$. On a $b_k \equiv b_{k-1} (\mathrm{mod}\, I^k) \Leftrightarrow y_k \in I^k$. Exprimer l'équation $a_k b_k \equiv 1 (\mathrm{mod}\, I^k)$ en terme de l'inconnue y_k et déterminer une expression de $y_k \in I^k$ pour résoudre notre équation, en utilisant $a_0 b_0 \equiv 1 (\mathrm{mod}\, I)$. Ceci boucle la récurrence pour construire notre suite $\bar{b}_k \in R/I^{k+1}$, $k \in \mathbb{N}$.

Observer ce système $\bar{b}_k \in R/I^{k+1}$, $k \in \mathbb{N}$, définit un élément $\beta \in R$ tel que $\alpha\beta = 1$ par construction. Conclure.

Dans le cas $R = \mathbb{Z}_p$, on obtient que unités p-adiques sont les nombres $\alpha = x_0 + px_1 + \cdots + p^k x_k + \cdots$ tels que $x \not\equiv 0 (\mathrm{mod}\, p)$. Dans le cas $R = \mathbb{K}[[t]]$, on obtient que éléments inversibles sont les séries formelles $f(t) = c_0 + c_1 t + \cdots + c_k t^k + \cdots$ telles que $c_0 \neq 0$.

3. Problème

Partie 1 (une version basique du lemme de Hensel).

Soit R un anneau complet pour la filtration par rapport aux puissances d'un idéal maximal M. Soit $f(t) \in R[t]$ un polynôme. On suppose que $f(t)$ possède une racine simple modulo M, c'est à dire qu'il existe $\alpha_0 \in R$, tel que $f(\alpha_0) \equiv 0 (\mathrm{mod}\, M)$ et $f'(\alpha_0) \not\equiv 0 (\mathrm{mod}\, M)$.

3.1) Construire par récurrence une famille d'éléments $\alpha_k \in R$ tels que $\alpha_k \equiv \alpha_{k-1} (\mathrm{mod}\, M^k)$ et $f(\alpha_k) \equiv 0 (\mathrm{mod}\, M^{k+1})$. *Indication :* Pour $k \geq 1$, on posera $\alpha_k = \alpha_{k-1} + h$, pour une inconnue $h \in M^k$, et on utilisera un développement $f(u+h) = c_0(u) + c_1(u)h + c_2(u)h^2 + \cdots + c_m(u)h^m$, avec les identifications $c_0(u) = f(u)$, $c_1(u) = f'(u)$.

3.2) Conclure de la question précédente que le polynôme $f(t)$ possède une racine dans R, soit α, telle que $\alpha \equiv \alpha_0 (\mathrm{mod}\, M)$.

3.3) Montrer que cette racine α est uniquement déterminée par la donnée de la classe $\bar{\alpha}_0 \in R/M$ telle que $\alpha \equiv \alpha_0 (\mathrm{mod}\, M)$. *Indication :* On montrera que les équations $\alpha_k \equiv \alpha_{k-1} (\mathrm{mod}\, M^k)$ et $f(\alpha_k) \equiv 0 (\mathrm{mod}\, M^{k+1})$ utilisées pour construire les éléments α_k possèdent une unique solution modulo M^{k+1} en reprenant l'analyse de la question 1.

BF, Courriel : benoit.fresse@univ-lille.fr

3.4) Prouver que le nombre $7 \in \mathbb{Z}$ possède une racine carré dans $\mathbb{Z}_3$.
3.5) Montrer que le polynôme $\phi_p(t) = t^{p-1} - 1$ se scinde complètement dans l'anneau $\mathbb{Z}_p[x]$, pour tout nombre premier p. Les racines de ce polynôme sont les racines $p-1$ème de l'unité dans $\mathbb{Q}_p$. *Remarque :* On peut montrer que le groupe des racines de l'unité de $\mathbb{Q}_p$ se réduit à l'ensemble de ces racines $p-1$ème pour p impair, aux nombres ± 1 pour $p = 2$.
3.6) Soit $f(x, y) \in \mathbb{K}[x, y]$ un polynôme à deux variables sur un corps $\mathbb{K}$. Soit $y = b$ une racine de l'équation $f(a, y) = 0$ telle que $\partial f/\partial y(a, b) \neq 0$. Prouver qu'il existe une série $y(t) \in \mathbb{K}[[t]]$, unique, telle que que $y(a) = b$ et $f(t, y(t)) = 0$. *Indication :* On appliquera le résutat des questions précédentes au complété de l'anneau $R = \mathbb{K}[x]$ par rapport aux puissances de l'idéal maximal $M = (x - a)$.

Partie 2 (une version forte du lemme de Hensel).

On va travailler dans l'anneau des nombres p-adiques $R = \mathbb{Z}_p$ dans cette partie et la partie suivante. On se donne maintenant un élément $\alpha_0 \in \mathbb{Z}_p$ tel que

$$(*) \qquad |f(\alpha_0)|_p < |f'(\alpha_0)|_p^2.$$

On adapte la méthode de Newton pour trouver une solution de l'équation $f(t) = 0$ dans $\mathbb{Z}_p$ à partir de la donnée de α_0.

On construit une suite récurrente α_k, de terme initial l'élément α_0, telle que

$$(**) \qquad \alpha_k = \alpha_{k-1} - \frac{f(\alpha_{k-1})}{f'(\alpha_{k-1})}$$

pour $k \geq 1$. On a $(*) \Rightarrow |f'(\alpha_0)|_p > 0 \Rightarrow f'(\alpha_0) \neq 0$. On va prouver par récurrence que cette suite est bien définie, que l'on a en fait $\alpha_k \in \mathbb{Z}_p$ pour tout $k \geq 1$, et que l'on a les relations

$$(1) \qquad |f'(\alpha_k)|_p = |f'(\alpha_0)|_p \neq 0,$$

$$(2) \qquad |f(\alpha_k)|_p \leq C^{2^k} |f'(\alpha_0)|_p^2 \quad \text{avec} \quad C = \frac{|f(\alpha_0)|_p}{|f'(\alpha_0)|_p^2},$$

pour tout $k \geq 0$. On montrera ensuite que la suite α_k converge vers un élément α tel que

$$(*') \qquad f(\alpha) = 0 \quad \text{et} \quad |\alpha - \alpha_0|_p = \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|_p < |f'(\alpha_0)|_p.$$

On suppose que les propriétés (1-2) sont satisfaites au rang $k-1$ (sachant que c'est trivialement le cas au rang $k = 0$), pour un élément $\alpha_{k-1} \in \mathbb{Z}_p$. On a déjà $|f'(\alpha_{k-1})|_p = |f'(\alpha_0)|_p \neq 0 \Rightarrow f'(\alpha_{k-1}) \neq 0$, de sorte que α_k est bien défini comme élément de $\mathbb{Q}_p$.
3.7) Observer que $|f(\alpha_{k-1})/f'(\alpha_{k-1})|_p \leq 1$. En déduire que l'on a $f(\alpha_{k-1})/f'(\alpha_{k-1}) \in \mathbb{Z}_p$ et $\alpha_k \in \mathbb{Z}_p$.
3.8) Observer que pour un polynôme $p(u) = c_0 + c_1 u + \cdots + c_d u^d \in \mathbb{Z}_p[u]$, on a $p(u) - p(v) = (u-v)q(u, v)$, pour un polynôme $q(u, v) \in \mathbb{Z}_p[u, v]$ et en déduire la relation $|p(u)-p(v)|_p \leq |u-v|_p$, pour tout couple $(u, v) \in \mathbb{Z}_p^2$. En appliquant ce résultat à $p(t) = f'(t)$, $u = \alpha_k$, $v = \alpha_{k-1}$, prouver que l'on a $|f'(\alpha_k) - f'(\alpha_{k-1})|_p < |f'(\alpha_0)|_p = |f'(\alpha_{k-1})|_p$, et utiliser les propriétés ultramétriques pour en déduire la relation $|f'(\alpha_k)|_p = |f'(\alpha_{k-1})|_p$. Conclure quant à l'assertion (1).
3.9) Observer que pour un polynôme $p(u) = c_0 + c_1 u + \cdots + c_d u^d \in \mathbb{Z}_p[u]$, on a $p(u + h) = p(u) + p'(u)h + q(u, h)h^2$, pour un polynôme $q(u, h) \in \mathbb{Z}_p[u, h]$ et en déduire que pour tout couple $(u, v) \in \mathbb{Z}_p^2$, on a une relation de la forme $p(v) = p(u) + p'(u)(v - u) + z(v - u)^2$, pour un

élément $z \in \mathbb{Z}_p$. Montrer en appliquant ces relations à $p(t) = f(t)$, $u = \alpha_{k-1}$, $v = \alpha_k$, que l'on a $|f(\alpha_k)|_p \leq |\alpha_k - \alpha_{k-1}|_p^2$. Utiliser l'expression de $\alpha_k - \alpha_{k-1}$ donnée par la formule $(**)$ et les hypothèses de récurrence pour conclure quant à l'assertion (2).

3.10) Déduire de la formule de récurrence $(**)$ et des propriétés $(1-2)$ que l'on a une majoration de la forme $|\alpha_k - \alpha_{k-1}|_p \leq C^{2^k} |f'(\alpha_0)|_p$. En déduire que α_k est une suite de Cauchy qui converge vers une limite $\alpha \in \mathbb{Z}_p$ et que cette limite vérifie $f'(\alpha) \neq 0$ et $f(\alpha) = 0$.

3.11) On note que dans le cas $f(\alpha_0) = 0$, on a $\alpha_k = \alpha_0$ pour tout k. On suppose dans la suite $f(\alpha_0) \neq 0$. On va montrer par récurrence que l'on a

$$|\alpha_k - \alpha_0|_p = \left| \frac{f(\alpha_0)}{f'(\alpha_0)} \right|_p , \tag{3}$$

pour tout $k \geq 1$, sachant que cette propriété est trivialement satisfaite au rang $k = 1$ par définition $(**)$ de notre suite. On suppose que (3) est satisfaite au rang $k-1$. Observer que l'on a $|\alpha_k - \alpha_{k-1}|_p < |f(\alpha_0)/f'(\alpha_0)|_p$ en revenant sur la majoration obtenue dans la question précédente, puis écrire $\alpha_k - \alpha_0 = (\alpha_k - \alpha_{k-1}) + (\alpha_{k-1} - \alpha_0)$ et utiliser les propriétés ultramétriques pour en déduire que (3) est satisfaite au rang k. Conclure quand à la relation $(*')$ en faisant $\alpha_k \to \alpha$.

Partie 3 (une propriété d'unicité dans le lemme de Hensel).

On va montrer que, dans la partie précédente, les relations

$$f(\alpha) = 0 \quad \text{et} \quad |\alpha - \alpha_0|_p < |f'(\alpha_0)|_p \tag{$*''$}$$

déterminent uniquement la racine α obtenue dans la partie 2.

3.12) On suppose que β vérifie également les contraintes $(*'')$. Utiliser la relation $p(v) = p(u) + p'(u)(v-u) + z(v-u)^2$, obtenue dans la question 8 pour tout polynôme $p(t) \in \mathbb{Z}_p[t]$ et tout couple d'élément $(u, v) \in \mathbb{Z}_p^2$, pour prouver que l'on a une relation $|f'(\alpha)(\beta - \alpha)|_p \leq |\beta - \alpha|_p^2$. Conclure.

Partie 4 (remarques complémentaires).

Une version générale du lemme de Hensel s'énonce comme suit.

THÉORÈME. *Soit R un anneau complet pour la filtration par rapport aux puissances d'un idéal I. Soit $f(t) \in R[t]$ un polynôme. Soit $\alpha_0 \in R$ un élément tel que*

$$f(\alpha_0) \equiv 0 (\mathrm{mod}\, f'(\alpha_0)^2 I). \tag{$*$}$$

On peut alors trouver un élément $\alpha \in R$ tel que

$$f(\alpha) = 0 \quad et \quad \alpha \equiv \alpha_0 (\mathrm{mod}\, f'(\alpha_0) I). \tag{$*'$}$$

Si $f'(\alpha_0)$ n'est pas diviseur de zéro dans R, alors α est uniquement caractérisé par $(*')$.

On pourra vérifier que ce résultat permet de retrouver le résultat obtenu dans les parties 2-3 pour $R = \mathbb{Z}_p$ et $M = p\mathbb{Z}_p$ via l'équivalence $x \equiv y (\mathrm{mod}\, zp\mathbb{Z}_p) \Leftrightarrow |x - y|_p < |z|_p$.

Le lemme de Hensel permet de montrer qu'un anneau local complet R vérifie la propriété suivante. Soit $f(t) \in R[t]$ un polynôme unitaire $f(t) = t^m + c_1 t^{m-1} + \ldots + c_m$. Si on note $K = R/M$ le corps résiduel de R et $\bar{f}(t) \in K[t]$ le polynôme obtenu par réduction des coefficients de $f(t)$ modulo M, alors toute factorisation $\bar{f}(t) = u(t)v(t)$ telle que $pgcd(u, v) = 1$ se relève à $R[t]$. (Il existe $p(t), q(t) \in R[t]$ tels que $f(t) = p(t)q(t)$ et $\bar{p}(t) = u(t)$, $\bar{q}(t) = v(t)$.) On dit que les anneaux locaux complets sont henseliens pour signifier qu'ils vérifient cette propriété (voir [3]

pour la référence originale et [4] pour un manuel exposant des applications de ce sujet en géométrie arithmétique).

§2. Références

La référence [1] est un article d'exposition sur le lemme de Hensel qui a servit de base pour les parties 2 et 3 du problème 3. Le livre [2] est un manuel de référence en algèbre commutative. La théorie des anneaux complets est traitée dans le chapitre 7 de cet ouvrage.

L'article [3], qui est la référence originale sur les anneaux henseliens, est une partie du travail monumental de Grothendieck de refondation de la géométrie algébrique. L'ouvrage [4] est un manuel qui reprend des applications de la théorie de Grothendieck en géométrie arithmétique. Ces références [3,4] sont au delà des objectifs du cours.

1. Keith Conrad. Hensel's Lemma. Notes disponibles sur la page `https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf`
2. David Eisenbud. Commutative Algebra with a View toward Algebraic Geometry. Graduate Texts in Mathematics 150, Springer-Verlag, 1995.
3. Alexander Grothendieck. Éléments de gométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. Inst. Hautes Études Sci. Publ. Math. No. 32 (1967), pp. 5-333
4. James Milne. Étale Cohomology. Princeton Mathematical Series 33, Princeton University Press, 1980.