
Feuille 4 : Corps locaux

- Exercice 1.** 1. Calculer la limite de $\frac{n!}{n!+1}$ dans $\mathbb{R}$ et dans $\mathbb{Q}_p$ pour tout premier p .
2. On note p_n le n -ème nombre premier, et $p_\infty = \infty$. On se donne une famille $a_n \in \mathbb{Z}_{p_n}$, et on pose $a_\infty = 0$. Construire une suite de rationnels $z_n \in \mathbb{Q}$ telle que pour tout $i \in \{1, \dots, \infty\}$, $\lim_{n \rightarrow \infty} |z_n - a_i|_{p_i} = 0$ (on pourra utiliser la suite $y_n = 1 + \prod_{i=1}^n p_i^{n+1}$).

- Indications 1.** 1. La suite tend vers 1 dans $\mathbb{R}$ et vers 0 dans chaque $\mathbb{Q}_p$.
2. Pour tout $n > 1$, on définit via le lemme chinois x_n tel que $x_n \equiv a_k \pmod{p_k}$ pour $k = 1, \dots, n$. Alors

$$z_n = \frac{x_n}{y_n}$$

convient : en effet dans $\mathbb{Q}_p$ on a $y_n \rightarrow 1$ et $x_n \rightarrow a_n$, et $x_n < \prod p_k$, donc $\frac{x_n}{y_n} \rightarrow 0$ dans $\mathbb{R}$.

Exercice 2 (Lemme de Hensel). Soit A un anneau de valuation discrète complet, et $f \in A[x]$. On suppose que $a_0 \in A$ et qu'il existe $\varepsilon < 1$ tel que $|f(a_0)| \leq \varepsilon |f'(a_0)|^2$ avec $f'(a_0) \neq 0$. On considère la suite

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

- Montrer que $a_n \in A$, $|f'(a_n)| = |f'(a_0)|$ et $|f(a_n)| \leq \varepsilon^{2^n} |f'(a_0)|^2$.
- Montrer que a_n converge vers une racine $a \in A$ de f qui vérifie

$$|a - a_0| \leq \varepsilon |f'(a_0)|,$$

et qu'une telle racine est unique.

- Indications 2.** 1. On utilise la formule de Taylor exacte $f(x) = f(a) + f'(a)(x - a) + \lambda(x - a)^2$ pour $\lambda \in A$ obtenue en développant $f(x) = f(a + (x - a))$ par la formule du binôme et le fait que $|\lambda| \leq 1$ pour tout $\lambda \in A$.

Par récurrence, il suffit de montrer la propriété pour a_1 . On a $|a_1 - a_0| \leq \varepsilon |f'(a_0)| < 1$, puisque $f'(a_0) \in A$, donc $a_1 \in A$.

En développant $f'(x)$, on a

$$f'(a_1) - f'(a_0) \in (a_1 - a_0)A,$$

et $|a_1 - a_0| \leq \varepsilon |f'(a_0)|$, donc $|f'(a_1) - f'(a_0)| < |f'(a_0)|$, et finalement $|f'(a_1)| = |f'(a_0)|$.

En développant $f(x)$, on a $f(x) = f(a_0) + f'(a_0)(x - a_0) + m(x - a_0)^2$ où $m \in A$, et par construction $f(a_1) = m(a_1 - a_0)^2$, donc $|f(a_1)| \leq \varepsilon^2 |f'(a_0)|^2$.

2. On a $|a_{n+1} - a_n| < \varepsilon^{2^n} |f'(a_0)|$, donc la suite est de Cauchy et converge vers $a \in A$, qui vérifie $f(a) = 0$ et $|a - a_0| \leq \varepsilon$.
Si on avait une autre racine telle que $|b - a_0| \leq \varepsilon$, alors en écrivant $f(b) = f(a) + f'(a)(b - a) + m(b - a)^2$, on aurait

$$|f'(a_0)| = |f'(a)| \leq |b - a| \leq \min(|b - a_0|, |a - a_0|) < \varepsilon |f'(a_0)|,$$

absurde.

Exercice 3. 1. Factoriser $x^4 - 17$ sur $\mathbb{Q}_2$.

2. Décrire la décomposition de l'idéal (2) dans l'anneau des entiers de $K = \mathbb{Q}(\sqrt[4]{17})$

Indications 3. 1. On veut appliquer le lemme de Hensel. Pour $f(x) = x^4 - 17$ on a que $f'(a_0) = 4a_0^3$ a valuation 2-adique égale à 2 si a_0 impair et donc $|f'(a_0)|_2^2 = 2^{-4}$ pour tout a_0 impair.

- On test $a_0 = 1$. On trouve $|f(1)|_2 = 2^{-4} = |f'(1)|_2^2$ et donc on ne peut pas appliquer le lemme de Hensel.
- On test $a_0 = 3$. On a $v_2(f(3)) = v_2(81 - 17) = v_2(64) = 6$ et donc $|f(3)|_2 = 2^{-6}$ et on peut prendre $\varepsilon = 2^{-2}$. Ainsi, il existe une racine $a \in \mathbb{Z}_2$ de $f(x)$ telle que $|a - 3|_2 \leq 2^{-4}$, c'est-à-dire $a \equiv 3 \pmod{16}$.

On a donc une racine 4-ème a de 17 dans $\mathbb{Z}_2$, donc

$$x^4 - 17 = x^4 - a^4 = (x^2 - a^2)(x^2 + a^2) = (x - a)(x + a)(x^2 + a^2)$$

dans $\mathbb{Z}_2[x]$. Le dernier facteur est irréductible car $\mathbb{Z}_2$ ne contient pas les racines 4-èmes de l'unité et donc $-a^2$ n'est pas un carré (d'une autre manière : si $-a^2$ était un carré dans $\mathbb{Z}_2$ il le serait modulo 8, mais $a \equiv 3 \pmod{8}$ et donc $-a^2 \equiv -1 \pmod{8}$ qui n'est pas un carré).

2. On écrit

$$K \otimes_{\mathbb{Q}} \mathbb{Q}_2 = \prod_{\mathfrak{p} | (2)} K_{\mathfrak{p}} = \mathbb{Q}_2[x]/(x - a) \times \mathbb{Q}_2[x]/(x + a) \times \mathbb{Q}_2[x]/(x^2 + a^2),$$

c'est-à-dire, en posant $\alpha = \sqrt[4]{17}$,

$$\mathbb{Q}(\alpha) \otimes_{\mathbb{Q}} \mathbb{Q}_2 = \mathbb{Q}_2 \times \mathbb{Q}_2 \times \mathbb{Q}_2(i)$$

via $p(\alpha) \otimes u \mapsto (p(a)u, p(-a)u, f(ia)u)$. On a donc trois idéaux $\mathfrak{p}_1, \mathfrak{p}_2$ et $\mathfrak{p}_3$ au-dessus de 2, les deux premiers sont non-ramifiés de degré résiduel 1, et pour le troisième on a $e_3 f_3 = 2$. Or, $\mathbb{Q}_2(i)/\mathbb{Q}_2$ est une extension cyclotomique ramifiée en 2, donc $e_3 = 2$ et $f_3 = 1$ et

$$(2) = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3^2.$$

Exercice 4. Soit $K/\mathbb{Q}$ un corps de nombres de degré n .

1. Montrer que si un nombre premier $p < n$ est totalement décomposé dans l'anneau d'entiers $\mathcal{O}_K$, ce dernier ne peut pas s'écrire sous la forme $\mathbb{Z}[\alpha]$.

2. À l'aide du polynôme $f(x) = x^3 - x + 8$, donner un exemple d'anneau d'entiers non monogène.

Indications 4. 1. Si $\mathcal{O}_K = \mathbb{Z}[\alpha]$ pour un entier algébrique α de polynôme minimal $f(x) \in \mathbb{Z}[x]$, on peut appliquer le critère de Dedekind et le fait que p soit totalement décomposé équivaut au fait que f est scindé à racines simples modulo p , impossible si $p < n$.

2. Ce polynôme est irréductible (il l'est modulo 3). Il faut montrer que 2 est totalement décomposé dans $K = \mathbb{Q}[x]/(f)$. On a une décomposition $K \otimes_{\mathbb{Q}} \mathbb{Q}_2 = \prod_{p|(2)} K_p$, donc la décomposition en facteurs irréductibles de $f(x)$ sur $\mathbb{Q}_2$ donne la factorisation de 2 en idéaux premiers. Pour $a_0 = 0, 1, 3$ on a $f(a_0) \equiv a_0^3 - a_0 \equiv 0 \pmod{8}$ donc $|f(a_0)|_2 \leq 2 - 3$ et de plus $|f'(a_0)|_2 \geq 2^{-1}$. On peut appliquer le lemme de Hensel et on a trois racines (distinctes, parce que elle le sont modulo 4) de $f(x)$ dans $\mathbb{Z}_2$, donc f est scindé sur $\mathbb{Q}_2$ et 2 est totalement décomposé dans K . D'après la question précédente, $\mathcal{O}_K$ ne peut être monogène.

Exercice 5. Soit p un premier impair, on note μ_{p-1} le groupe des racines $(p-1)$ -ème de l'unité dans $\overline{\mathbb{Q}}_p$.

1. Montrer que $\mathbb{Q}_p^* = p^{\mathbb{Z}} \times \mu_{p-1} \times (1 + p\mathbb{Z}_p)$.
2. Montrer que pour p impair, $\mathbb{Q}_p$ n'a que trois extensions quadratiques.
3. Montrer de même que $\mathbb{Q}_2$ possède 7 extensions quadratiques.

Indications 5. 1. On a une suite exacte (évidemment scindée) donnée par la norme

$$1 \rightarrow \mathbb{Z}_p^* \rightarrow \mathbb{Q}_p^* \rightarrow p^{\mathbb{Z}} \rightarrow 1$$

et une suite exacte

$$0 \rightarrow 1 + p\mathbb{Z}_p \rightarrow \mathbb{Z}_p^* \rightarrow \mathbb{F}_p^* \rightarrow 1$$

scindée en relevant $\mathbb{F}_p^*$ dans les racines de $x^{p-1} - 1$ grâce au lemme de Hensel.

2. Une telle extension est de la forme $\mathbb{Q}_p(\sqrt{d})$ pour $d \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, il suffit donc de montrer que cet espace vectoriel sur $\mathbb{F}_2$ est de dimension 2. Or tout élément de $1 + p\mathbb{Z}_p$ est un carré d'après le lemme de Hensel (puisque $x^2 - 1$ a deux racines modulo p), donc le quotient vaut

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \cong p^{\mathbb{Z}}/p^{2\mathbb{Z}} \times \mathbb{Z}/(p-1)\mathbb{Z}/2\mathbb{Z}/(p-1)\mathbb{Z} \cong \mathbb{F}_2^2.$$

En enlevant 1, on a trois extensions quadratiques. Les deux générateurs sont p et un non-carré modulo p , par exemple les extensions de $\mathbb{Q}_3$ sont $\mathbb{Q}_3(\sqrt{3})$, $\mathbb{Q}_3(\sqrt{-1})$ et $\mathbb{Q}_3(\sqrt{-3})$.

3. Dans le cas $p = 2$, la suite donnant les unités est

$$0 \rightarrow 1 + 4\mathbb{Z}_2 \rightarrow \mathbb{Z}_2^* \rightarrow \pm 1 \rightarrow 1$$

et on a une composante supplémentaire à l'arrivée puisque le sous-groupe des carrés de $1 + 4\mathbb{Z}_2$ est seulement $1 + 8\mathbb{Z}_2$ (en effet 5 n'est pas un carré modulo 8).

- Exercice 6.**
1. Pour $f > 1$ soit α un générateur du groupe multiplicatif $\mathbb{F}_{p^f}^*$, et soit $\bar{P}(x) = x^f + \bar{a}_1 x^{f-1} + \cdots + \bar{a}_f$ son polynôme minimal sur $\mathbb{F}_p$. Soient $a_i \in \mathbb{Z}_p$ des relèvements des $\bar{a}_i$, et $\alpha \in \bar{\mathbb{Q}}_p$ une racine de $P(x) = \sum a_i x^i$. Montrer que $\mathbb{Q}_p(\alpha)/\mathbb{Q}_p$ est une extension non ramifiée de $\mathbb{Q}_p$ de degré f .
 2. Soit $K/\mathbb{Q}_p$ une extension non ramifiée de degré f . Montrer que $K = \mathbb{Q}_p(\zeta)$ où ζ est une racine $(p^f - 1)$ -ème de l'unité.
 3. Montrer que pour tout n , $\mathbb{Q}_p$ possède une unique extension non ramifiée de degré n . Cette extension est souvent notée $\mathbb{Q}_{p^f}$ et son anneau des entiers $\mathbb{Z}_{p^f}$.

- Indications 6.**
1. P est irréductible puisqu'il l'est modulo p , et on obtient une extension dont le degré résiduel est f , donc non ramifiée.
 2. Le corps résiduel contient les racines $(p^f - 1)$ -èmes de l'unité et on peut les relever à $\mathcal{O}_K$ par Hensel. On obtient K par égalité des degrés.
 3. Les extensions non ramifiées de $\mathbb{Q}_p$ sont en correspondance avec les extensions $\mathbb{F}_{p^f}/\mathbb{F}_p$ des corps résiduels.

Exercice 7. Soit K un corps local et L/K une extension finie de degré n . On note π une uniformisante de $\mathcal{O}_L$.

1. Montrer que si L/K est totalement ramifiée, alors $\mathcal{O}_L = \mathcal{O}_K[\pi]$.
2. Montrer que si L/K est totalement ramifiée, le polynôme minimal de π est un polynôme d'Eisenstein.
3. Montrer que si α est annulé par un polynôme d'Eisenstein sur $\mathcal{O}_K$, l'extension $K(\alpha)/K$ est totalement ramifiée.

Indications 7.

1. On peut écrire les éléments de $\mathcal{O}_L$ sous la forme $x = \sum_{m \geq 0} x_m \pi^m$, où les coefficients x_m sont dans un système de représentants du corps résiduel $\mathcal{O}_L/(\pi)$ de L . Or, en notant π_K une uniformisante de K , on a $\pi^n \mathcal{O}_L = \pi_K \mathcal{O}_L$ puisque l'extension est totalement ramifiée, donc $\pi^{nq+r} \mathcal{O}_L = \pi_K^q \pi^r \mathcal{O}_L$. On peut également écrire les éléments de $\mathcal{O}_L$ sous la forme $x = \sum_{q \geq 0} \sum_{r=0}^{n-1} y_{q,r} \pi_K^q \pi^r$ où l'on choisit de plus les éléments $y_{q,r}$ dans un système de représentants dans $\mathcal{O}_K$ de $\mathcal{O}_K/\pi_K = \mathcal{O}_L/\pi$. En regroupant les termes par paquet on obtient

$$x = \sum_{r=0}^{n-1} \left(\sum_{q \geq 0} y_{q,r} \pi_K^q \right) \pi^r \in \mathcal{O}_K[\pi].$$

2. Notons v la valuation associée à K , et $\pi^n = \sum_{i=0}^{n-1} a_i \pi^i$ une relation de dépendance intégrale, où $a_i \in \mathcal{O}_K$. Puisque $v(\pi) = 1/n$, les valuations des termes à droite sont deux à deux distinctes, donc $v(\pi^n) = 1 = \min v(a_i \pi^i)$. Ceci impose $v(a_0) = 1$ et $v(a_i) \geq 1$ pour $i \geq 1$. Le polynôme est bien un polynôme d'Eisenstein.
3. C'est un résultat du cours. Regarder aussi *Corps locaux* de Serre, chapitre I, section 6.

Exercice 8 (Lemme de Krasner). Soit $K/\mathbb{Q}_p$ une extension finie, et $\alpha, \beta \in \bar{\mathbb{Q}}_p$.

1. Montrer que tout $\sigma \in \text{Aut}_{\mathbb{Q}_p}(K)$ est une isométrie.
2. Montrer que si $|\alpha - \beta| < |\alpha - \alpha'|$ pour tout conjugué $\alpha' \neq \alpha$ de α , alors $K(\alpha) \subseteq K(\beta)$.

Indications 8. 1. C'est une conséquence immédiate du fait que deux éléments conjugués ont la même valuation.

2. Pour montrer $K(\alpha) \subseteq K(\beta)$ il suffit de montrer que $\sigma(\alpha) = \alpha$ pour tout $\sigma \in \text{Aut}_{K(\beta)}(\bar{\mathbb{Q}}_p)$. Supposons par l'absurde que $\sigma \in \text{Aut}_{K(\beta)}(\bar{\mathbb{Q}}_p)$ soit tel que $\alpha' = \sigma(\alpha) \neq \alpha$. On a

$$\begin{aligned} |\alpha - \beta| &< |\alpha - \alpha'| = |\alpha - \beta + \beta - \alpha'| \leq \max(|\alpha - \beta|, |\beta - \alpha'|) = \\ &= \max(|\alpha - \beta|, |\sigma(\beta) - \sigma(\alpha)|) = \max(|\alpha - \beta|, |\beta - \alpha|) = |\alpha - \beta| \end{aligned}$$

ce qui est absurde.

Exercice 9. Soit $K/\mathbb{Q}_p$ une extension finie, $A = \mathcal{O}_K$ son anneau d'entiers et π une uniformisante.

1. Soit $f(x) = \sum_{i=1}^n a_i x^i \in A[x]$ un polynôme irréductible unitaire séparable de degré n . On écrit $f(x) = \prod_{i=1}^n (x - \alpha_i)$ avec $\alpha_i \in \bar{\mathbb{Q}}_p$. Montrer que pour tout $\varepsilon > 0$, il existe $\delta > 0$ tel que tout polynôme unitaire $g(x) = \sum_{i=1}^n b_i x^i \in A[x]$ tel que $\max |a_i - b_i| < \delta$ s'écrit $g(x) = \prod_{i=1}^n (x - \beta_i)$ avec $|\alpha_i - \beta_i| < \varepsilon$ pour tout i .
2. Soit $E = \{a_0 + a_1 x + \dots + a_n x^n \in A[x], |a_i| < 1, |a_0| = |\pi|\}$ l'ensemble des polynômes d'Eisenstein de degré n , et

$$D = \{K(\alpha), \exists f \in E, f(\alpha) = 0\}$$

l'ensemble des extensions qu'ils définissent. Montrer que D est fini (utiliser le lemme de Krasner).

Indications 9. 1. C'est le lemme de continuité des racines, dans le cas simple où il n'y a pas de racine multiple. On peut appliquer le théorème d'inversion locale à l'application $(\alpha_i) \mapsto (a_i)$ qui est continue car donnée par les polynômes symétriques (et entre deux espaces de Banach).

2. On montre en utilisant la question précédente et le lemme de Krasner que des polynômes proches définissent les mêmes extensions.

Soit $f \in E$, on note $\alpha_1, \dots, \alpha_n$ ses racines, et $\varepsilon = \min_{i \neq j} |\alpha_i - \alpha_j|$. D'après la question précédente, il existe δ tel que pour tout $g \in E$ tel que $|f - g|_\infty < \delta$, les racines $\beta_1, \dots, \beta_d$ de g vérifient $|\alpha_i - \beta_i| < \varepsilon$, de sorte que d'après le lemme de Krasner $K(\alpha_i) \subseteq K(\beta_i)$. Mais par égalité des degrés, ces extensions sont égales. Puisque E est compact, on le recouvre par un nombre fini de boules de rayon δ sur lesquelles on a au plus d extensions, d'où le résultat. Ainsi, K n'a qu'un nombre fini d'extensions totalement ramifiées de degré d , pour tout d .

Exercice 10. Soit $K/\mathbb{Q}_p$ une extension finie de degré $n = ef$, où e est le degré de ramification et f le degré d'inertie.

1. On pose $E = \mathbb{Q}_p(\mu_{p^f-1})$, montrer que E est la plus grande sous-extension non ramifiée de K .
2. Montrer que K/E est totalement ramifiée.
3. Montrer que $\mathbb{Q}_p$ n'a qu'un nombre fini d'extensions de degré n .

Indications 10. 1. On a $E \subseteq K$ d'après le lemme de Hensel en relevant les racines de l'unité du corps résiduel. Réciproquement, toute extension non ramifiée est de la forme $\mathbb{Q}_p(\zeta_m)$ avec $m \mid (p^f - 1)$.

2. Clair.
3. Il n'y a qu'un nombre fini d'extensions $E/\mathbb{Q}_p$ non ramifiées de degré divisant n , et pour chacune un nombre fini d'extensions totalement ramifiées K/E de degré n/d .