Université de Paris **7 octobre 2021**
M2 – Théorie des nombres

Feuille 3 : corps locaux

Exercice 1 : nombres p-adiques

1. Calculer la limite de $\frac{n!}{n!+1}$ dans $\mathbb{R}$ et dans $\mathbb{Q}_p$ pour tout premier p.

La suite tend vers 1 dans $\mathbb{R}$, et vers 0 dans chaque $\mathbb{Q}_p$.

2. On note p_n le n-ième 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 $i \in \{1, \dots \infty\}$, $\lim_{n\to\infty} |z_n - a_i|_{p_i} = 0$ (on pourra utiliser la suite $y_n = 1 + \prod_{i=1}^n p_i^{n+1}$).

Pour tout $n \geqslant 1$, on définit via le lemme chinois x_n tel que $x_n \equiv a_k \bmod p_k^n$ pour $k = 1, \dots n$. Alors $z_n = \frac{x_n}{y_n}$ convient : en effet dans $\mathbb{Q}_p$ on a $y_n \to 1$ et $x_n \to a_n$, et $x_n < \prod p_k^n$ donc $\frac{x_n}{y_n} \to 0$ 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 $\epsilon < 1$ tel que $|f(a_0)| \leqslant \epsilon |f'(a_0)|^2$ avec $f'(a_0) \neq 0$. On considère la suite

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

1. Montrer que $a_n \in A$, $|f'(a_n)| = |f'(a_0)|$ et $|f(a_n)| \leqslant \epsilon^{2^n} |f'(a_0)|^2$.

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 $|\lambda| \leqslant 1$ pour tout $\lambda \in A$.
Par récurrence, il suffit de montrer la propriété pour a_1.
On a $|a_1 - a_0| \leqslant \epsilon |f'(a_0)| < 1$ puisque $f'(a_0) \in A$, donc $a_1 \in A$.
En développant $f'(x)$ on a $f'(a_1) - f'(a_0) \in (a_1 - a_0)A$, or $|a_1 - a_0| \leqslant \epsilon |f'(a_0)|$ d'où $|f'(a_1) - f'(a_0)| < |f'(a_0)|$ et l'égalité $|f'(a_1)| = |f'(a_0)|$.
En développant $f(x)$ on a $f(x) = f(a_0) + f'(a_0)(x-a_0) + m(x-a_0)^2$, pour $m \in A$, et par construction $f(a_1) = m(a_1 - a_0)^2$ donc $|f(a_1)| \leqslant \epsilon^2 |f'(a_0)|^2$.

2. Montrer que a_n converge vers une racine $a \in A$ de f qui vérifie $|a - a_0| \leqslant \epsilon |f'(a_0)|$, et qu'une telle racine est unique.

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

Exercice 3 : Dedekind via complétions

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

On veut appliquer le lemme de Hensel, on cherche des pseudo-racines de valuation au moins 5 puisque $v(f'(a)) = 2$ pour tout a impair. Or $v(f(\pm 1)) = 4$, mais $v(f(\pm 3)) = v(81 - 17 = 64) = 6$. Ainsi, il existe deux racines $\pm a \in \mathbb{Z}_2$ pour $a \equiv 3 \bmod 16$, et $f(x) = (x-a)(x+a)(x^2+a^2)$ dans $\mathbb{Z}_2[x]$. Le dernier facteur est irréductible car $\mathbb{Z}_2$ ne contient pas les racines 4-ièmes de l'unité.

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

On écrit $K \otimes \mathbb{Q}_2 = \prod_{\mathfrak{p}|(2)} K_\mathfrak{p} = \mathbb{Q}_2[x]/(x-a) \times \mathbb{Q}_2[x]/(x+a) \times \mathbb{Q}_2[x]/(x^2+a^2)$, c'est-à-dire, en posant $\alpha = \sqrt[4]{17}$, $\mathbb{Q}(\alpha) \otimes \mathbb{Q}_2 = \mathbb{Q}_2 \times \mathbb{Q}_2 \times \mathbb{Q}_2(i)$ via $p(\alpha) \otimes u \mapsto (f(a)u, f(-a)u, f(ia)u)$.
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 c'est une extension cyclotomique ramifiée en 2, donc $e_3 = 2$ et $f_3 = 1$.
Ainsi $(2) = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3^2$.

Exercice 4 : anneau d'entier non monogène

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 $\mathbb{Z}_K$, ce dernier ne peut pas s'écrire sous la forme $\mathbb{Z}[\alpha]$.

Si $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ pour un entier algébrique α de polynôme minimal $f(x) \in \mathbb{Z}[x]$, on peut appliquer le lemme 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. À l'aide du polynôme $f(x) = x^3 - x + 8$, donner un exemple d'anneau d'entiers non monogène.

Ce polynôme est bien irréductible (il l'est modulo 3). Il faut montrer que 2 est totalement décomposé dans $K = \mathbb{Q}[x]/(f)$. Or on a une décomposition $K \otimes \mathbb{Q}_2 = \prod_{\mathfrak{p}|2} K_\mathfrak{p}$, la décomposition en facteurs irréductibles de $f(x)$ sur $\mathbb{Q}_2$ donne la factorisation de 2 en idéaux premiers.
Or $f(x) \equiv x^3 - x \bmod 8$ a trois racines distinctes modulo 8 en lesquelles $f'(x) = 3x^2 - 1$ est de valuation $\leqslant 1$, on les relève chacune dans $\mathbb{Z}_2$, donc f est scindé sur $\mathbb{Q}_2$ et 2 est totalement décomposé dans K.
D'après la question précédente, $\mathbb{Z}_K$ ne peut être monogène.

Exercice 5 :

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

1. Montrer que $\mathbb{Q}_p^\times = p^\mathbb{Z} \times \mu_{p-1} \times (1 + p\mathbb{Z}_p)$.

On a une suite exacte donnée par la norme $1 \to \mathbb{Z}_p^\times \to \mathbb{Q}_p^\times \to p^\mathbb{Z}$, et une suite exacte $0 \to 1 + p\mathbb{Z}_p \to \mathbb{Z}_p^\times \to \mathbb{F}_p^\times \to 1$, scindée en relevant $\mathbb{F}_p^\times$ dans les racines de $x^{p-1} - 1$ grâce au lemme de Hensel.

2. Montrer que pour p impair, $\mathbb{Q}_p$ n'a que trois extensions quadratiques.

Une telle extension est de la forme $\mathbb{Q}_p(\sqrt{d})$ pour $d \in \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, il suffit de montrer que ce $\mathbb{F}_2$ espace vectoriel 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 $p^{\mathbb{Z}}/p^{2\mathbb{Z}} \times \mathbb{Z}/(p-1)\mathbb{Z}/2\mathbb{Z}/(p-1)\mathbb{Z} \simeq \mathbb{F}_2^2$. En enlevant 1, on a 3 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. Montrer de même que $\mathbb{Q}_2$ possède 7 extensions quadratiques.

Dans le cas $p=2$ la suite donnant les unités est $0 \to 1+4\mathbb{Z}_2 \to \mathbb{Z}_2^\times \to \pm 1 \to 1$, et on a une composante supplémentaire à l'arrivée puisque le sous-groupe des carrés de $1+4\mathbb{Z}_2$ est seulement $1+8\mathbb{Z}_2$ (5 n'est pas un carré modulo 8).

Exercice 6 : Extensions non ramifiées de $\mathbb{Q}_p$

1. Soit $f \geqslant 1$, on note $\overline{\alpha}$ un générateur du groupe multiplicatif $\mathbb{F}_{p^f}^\times$, et $\overline{P}(x) = x^f + \overline{a_1}x^{f-1} + \dots \overline{a_f}$ un polynôme minimal sur $\mathbb{F}_p$. Soient $a_i \in \mathbb{Z}_p$ des relèvements des $\overline{a_i}$, et $\alpha \in \overline{\mathbb{Q}_p}$ 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.

P est irréductible puisqu'il l'est modulo p, et on obtient une extension dont le degré résiduel est f, donc non ramifiée.

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)-ième de l'unité.

Le corps résiduel contient les racines (p^f-1)-ièmes de l'unité et on peut les relever à $\mathbb{Z}_K$ par Hensel. On obtient K par égalité des degrés.

3. Montrer que pour tout n, $\mathbb{Q}_p$ possède une unique extension non ramifiée de degré n.

Questions précédentes. 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 : Extensions totalement ramifiées

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

1. Montrer que si L/K est totalement ramifiée, alors $\mathbb{Z}_L = \mathbb{Z}_K[\pi]$.

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

2. Montrer que si L/K est totalement ramifiée, le polynôme minimal de π est un polynôme d'Eisenstein.

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 $a_i \in \mathbb{Z}_K$. 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 $v(a_i) \geqslant 1$ pour $i \geqslant 1$. Le polynôme est bien un polynôme d'Eisenstein.

3. Montrer que si α est annulé par un polynôme d'Eisenstein sur $\mathbb{Z}_K$, l'extension $K(\alpha)/K$ est totalement ramifiée.

c'est un résultat du TD1.

Exercice 8 : lemme de Krasner

Soit $K/\mathbb{Q}_p$ une extension finie, et $\alpha, \beta \in \overline{\mathbb{Q}_p}$.

1. Montrer que tout $\sigma \in \mathrm{Aut}_K(\overline{\mathbb{Q}_p})$ est une isométrie.

Cours : deux éléments conjugués ont même valuation, la norme sur $\overline{\mathbb{Q}_p}$ vaut $|\alpha| = |\sigma(\alpha)| = \left|N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\right|^{1/[\mathbb{Q}_p(\alpha)/\mathbb{Q}_p)]}$.

Montrer que si $|\alpha - \beta| < |\alpha - \alpha'|$ pour tout conjugué α' de α sur K distinct de α, alors $K(\alpha) \subset K(\beta)$.

Soit $\sigma \in \mathrm{Aut}_{K(\beta)}(\overline{\mathbb{Q}_p})$, on a $|\sigma(\alpha) - \alpha| \leqslant \max(|\sigma(\alpha) - \sigma(\beta)|, |\beta| - \alpha) = |\beta - \alpha|$. Donc d'après l'hypothèse on ne peut avoir $\sigma(\alpha) \neq \alpha$, donc $\alpha \in K(\beta)$.

Exercice 9 : Nombre d'extensions ramifiées

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

1. Soit $f(x) = \sum a_i x^i \in A[x]$ un polynôme irréductible unitaire séparable de degré d, on l'écrit $f(x) = \prod(x - \alpha_i)$ avec $\alpha_i \in \overline{\mathbb{Q}_p}$. Montrer que pour tout $\epsilon > 0$, il existe $\delta > 0$ tel que pour tout polynôme unitaire $g(x) = \sum b_i x^i \in A[x]$ tel que $\max |a_i - b_i| < \delta$ s'écrit $g(x) = \prod(x - \beta_i)$ avec $|\alpha - \beta| < \epsilon$.

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 $(\alpha_i) \mapsto (a_i)$ continue car donnée par les polynômes symétriques (et entre deux espaces de Banach).

2. Soit $E = \left\{a_0 + a_1 x + \cdots + x^d \in A[x], |a_i| < 1, |a_0| = |\pi|\right\}$ l'ensemble des polynômes d'Eisenstein de degré d, 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).

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 $\alpha_1, \ldots \alpha_d$ ses racines, et $\delta = \min_{i \neq j}(|\alpha_i - \alpha_j|)$. D'après la question précédente il existe ϵ tel que pour tout $g \in E$ tel que $|f - g|_\infty < \epsilon$, les racines $\beta_1, \ldots \beta_d$ de g vérifient $|\alpha_i - \beta_j| \leqslant |\alpha_i - \alpha_j|$, de sorte que d'après le lemme de Krasner $K(\alpha) \subset K(\beta)$. Mais par égalité des degrés, ces extensions sont égales.

Puisque E est compact, on le recouvre par un nombre fini de boules de rayon ϵ 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 : Extensions finies de $\mathbb{Q}_p$

Soit $K/\mathbb{Q}_p$ une extension finie de degré $n = ef$.

1. On pose $E = \mathbb{Q}_p(\mu_{p^f-1})$, montrer que E est la plus grande sous-extension non ramifiée de K.

On a $E \subset K$ 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. Montrer que K/E est totalement ramifiée.

clair

3. Montrer que $\mathbb{Q}_p$ n'a qu'un nombre fini d'extensions de degré n.

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