Feuille de TD 3

Exercice 1. — *Soit p un nombre premier impair.*

- *Montrer, en utilisant le lemme de Hensel, qu'un élément $v \in \mathbb{Q}_p^\times$ qu'on écrit sous la forme $v = p^r u$ avec $u \in \mathbb{Z}_p^\times$, est un carré si et seulement si r est pair et u est un carré modulo p.*
- *Déduire de la question précédente que $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z})^2$.*
  Remarque. On pourra aussi montrer que $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z})^3$.
- *Quelles sont les extensions quadratiques de $\mathbb{Q}_p$?*

Remarque. Contrairement au cas de $\mathbb{Q}$, il n'y a donc qu'un nombre fini d'extensions quadratiques de $\mathbb{Q}_p$. Cette propriété est plus générale, puisque que $\mathbb{Q}_p$ n'admet qu'un nombre fini d'extension de degré n, comme nous allons le montrer dans les exercices suivants. Pour le montrer, on vérifie tout d'abord que toute extension $L/\mathbb{Q}_p$ admet une unique sous-extension $K/\mathbb{Q}_p$ qui est non ramifiée. En utilisant le lemme de Krasner ci-après, on peut montrer que K admet un nombre fini d'extension totalement ramifiée, ce qui donne donc un nombre fini de possibilité pour L/K.

Exercice 2. — *Soit $\alpha \in \overline{\mathbb{Q}}_p$. On définit alors $\bar{v}_p(x) := \frac{1}{[\mathbb{Q}_p[\alpha]:\mathbb{Q}_p]} v_p\big(N_{\mathbb{Q}_p[\alpha]/\mathbb{Q}_p}(\alpha)\big)$.*

- *Soit σ un automorphisme du corps $\overline{\mathbb{Q}}_p$. Montrer que pour tout $\alpha \in \overline{\mathbb{Q}}_p$, on a $\bar{v}_p(\sigma(\alpha)) = w(\alpha)$.*
- ***(Lemme de Krasner)** Soit $\alpha_1 \in \overline{\mathbb{Q}}_p$ séparable de conjugués $\alpha_2, \cdots, \alpha_n$. On suppose qu'il existe $\beta \in \overline{\mathbb{Q}}_p$ tel que $\bar{v}_p(\beta - \alpha_1) > \bar{v}_p(\beta - \alpha_i)$ pour tout $i = 2, \cdots, n$. Montrer alors que $\mathbb{Q}_p(\alpha_1) \subset \mathbb{Q}_p(\beta)$.*
- *Soit $f(X) = \prod_{i=1}^n (X - \alpha_i) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Q}_p[X]$. Montrer que pour tout $i = 1, \cdots, n$, on a $|\alpha_i| := p^{-\bar{v}_p(\alpha_i)} < ||f||_1 := a_1 + \cdots + a_n$.*
- *Avec les notations précédentes, construire un réel δ strictement positif tel que si $g(X) \in \mathbb{Q}_p[X]$ est un polynôme unitaire vérifiant $||f - g||_1 \leq \delta$. Montrer alors que pour tout racine β de $g(X)$, il existe α_j tel que pour tout $i \neq j$, on ait $|\alpha_j - \beta| < |\alpha_j - \alpha_i|$, et en déduire $K(\beta) = K(\alpha_j)$ puis que $g(X)$ est irréductible et séparable.*

Exercice 3. — *Soit p premier impair. Montrer que les racines de l'unité de $\mathbb{Q}_p$ sont les $p-1$ solutions de l'équation $X^{p-1} - 1$.*

1 (1) Rappelons que tout $v \in \mathbb{Q}_p^\times$ s'écrit de manière unique sous la forme $v = p^r u$ avec $r \in \mathbb{Z}$ et $u \in \mathbb{Z}_p^\times$. Si $v = w^2$ on a alors $r \equiv 0 \mod 2$ et u est un carré de $\mathbb{Z}_p^\times$ de sorte que son image modulo p est aussi un carré.

Réciproquement si u est un carré modulo p alors, d'après le lemme de Hensel, u est un carré dans $\mathbb{Z}_p^\times$ et donc $p^{2r}u$ est un carré.

(2) Le premier facteur correspond à l'image de r modulo 2 et le deuxième à celle de $u \in \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2} \simeq \mathbb{Z}/2\mathbb{Z}$.

(3) Une extension quadratique de $\mathbb{Q}_p$ s'écrit $\mathbb{Q}_p[X]/(aX^2+bX+c) = \mathbb{Q}_p[\sqrt{d}]$ où $d = b^2-4ac$. D'après la question précédente, il y a donc exactement 3 extensions quadratiques. Pour $p \equiv 1 \mod 4$, on trouve $\mathbb{Q}_p[\sqrt{-1}]$, $\mathbb{Q}_p[\sqrt{p}]$ et $\mathbb{Q}_p[\sqrt{-p}]$.

2 (1) Comme α et $\sigma(\alpha)$ ont le même polynôme minimal, ils ont la même norme et engendrent des corps isomorphes ; ils ont donc la même valuation.

(2) Supposons $\alpha_1 \notin \mathbb{Q}_p(\beta)$ et soit $\sigma : \mathbb{Q}_p(\alpha_1, \beta) \longrightarrow \overline{\mathbb{Q}}_p$ qui fixe $\mathbb{Q}_p(\beta)$ mais pas α_1. On a alors $\bar{v}_p(\beta - \alpha_1) = \bar{v}_p(\sigma(\beta - \alpha_1)) = \bar{v}_p(\beta - \alpha_i)$ avec $i \geq 2$. Or $\bar{v}_p(\alpha_1 - \alpha_i) = \bar{v}_p((\alpha_1 - \beta) + (\beta - \alpha_i)) \geq \min\{\bar{v}_p(\alpha_1 - \beta), \bar{v}_p(\beta - \alpha_i)\} = \bar{v}_p(\alpha_1 - \beta)$ ce qui contredit notre hypothèse.

(3) C'est clair si $f(X) = X^n$. Sinon $||f||_1 > 1$. Pour $|\alpha_i| \leq 1$, il n'y a rien à faire et pour $|\alpha_i| > 1$, de $|\alpha_i|^n = |a_1\alpha_i^{n-1}+\cdots+a_{n-1}\alpha_i+a_n|$ et donc $|\alpha_i| \leq \max\{|a_1\alpha_i^{n-1}|, \cdots, |a_{n-1}\alpha_i|, |a_n|\}$. Pour j tel que $a_j \neq 0$, on a ainsi $|\alpha_i| \leq |\alpha_i^{n-j}| \leq |a_j| \leq ||f||_1$.

(4) Soit $\epsilon = \min\{1, \min_{i\neq j}\{|\alpha_i - \alpha_j|\}\}$ puis $\delta = (\frac{\epsilon}{2(||f||_1+1)})^n < 1$. Notons que $g \in \mathbb{Q}_p[X]$ unitaire, l'inégalité $||f - g||_1 < \delta$, impose $\deg f = \deg g$. On écrit $g(X) = X^n + b_1X^{n-1} + \cdots + b_1X + b_0$ avec $||g||_1 \leq ||f||_1 + ||g - f||_1 < ||f||_1 + \delta$. Pour β une racine de $g(X)$, on a

$$\begin{aligned} |f(\beta)| &= |f(\beta) - g(\beta)| \leq \textstyle\sum_{i=0}^n |a_i - b_i|.|\beta|^i < \sum_{i=0}^n |a_i - b_i|.||g||_1^i \\ &\leq ||f - g||_1.||g||_1^n < \delta(||f||_1 + \delta)^n < \delta(||f||_1 + 1)^n = (\tfrac{\epsilon}{2})^n. \end{aligned}$$

Par ailleurs on a $f(\beta) = \prod_{i=1}^n |\beta - \alpha_i|$ de sorte qu'il existe α_j tel que $|\beta - \alpha_j| < \epsilon/2$. D'après la définition de ϵ, on a $|\alpha_j - \beta| < |\alpha_j - \alpha_i|$ pour tout $j \neq i$. D'après le lemme de Krasner, on a $\mathbb{Q}_p(\alpha_j) \subset \mathbb{Q}_p(\beta)$. Comme en outre $n = [\mathbb{Q}_p(\alpha_j) : \mathbb{Q}_p] \leq [\mathbb{Q}_p(\beta) : \mathbb{Q}_p] \leq n$ et donc $\mathbb{Q}_p(\alpha_j) = \mathbb{Q}_p(\beta)$. En particulier β est séparable et g est le polnynôme minimal de β qui est donc irréductible.

3 Si $x^n = 1$ alors $|x|_p^n = 1$ soit $|x|_p = 1$ et donc $x \in \mathbb{Z}_p^\times$. Pour m premier avec p, d'après le lemme de Hensel si $x \equiv y \mod p$ sont deux solutions de $X^m - 1$ alors $x = y$. Comme $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, alors m doit être un diviseur de $p-1$. Réciproquement le lemme de Hensel fournit des racines de $X^{p-1} - 1$.

Enfin pour $f(X) = X^p - 1$, pour appliquer la version forte du lemme de Hensel **??**, en notant que $|f'(x)|_p = |px^{p-1}|_p = 1/p$, il suffit de montrer que $x \equiv 1 \mod p^2\mathbb{Z}_p$. On écrit $x = 1 + py$ avec $1 = (1 + py)^p \equiv 1 + p^2y \mod p^3$ et donc $y \equiv 0 \mod p$. Le lemme de Hensel donne alors $x = 1$ et donc la seule racine de $X^p - 1$ est $x = 1$.