Lemme de Hensel

Dans toute la suite, p est un nombre premier.

Exercice 1. Montrer que le polynôme $X^3 - 4$ admet une unique racine dans $\mathbb{Q}_5$.

Exercice 2.(Lemme de Hensel) Soit $Q(X) \in \mathbb{Z}_p[X]$ et $k \geq 1$.

1. Soit $x \in \mathbb{Z}_p$ tel que $Q(x) \in Q'(x)^2 p^k \mathbb{Z}_p$ et $Q'(x) \neq 0$. On pose $y = x - \frac{Q(x)}{Q'(x)}$. Montrer que :
   (a) $Q(y) \in p^{k+1} Q'(x)^2 \mathbb{Z}_p$;
   (b) $y - x \in p^k Q'(x) \mathbb{Z}_p$;
   (c) $\mathrm{val}_p(Q'(y)) = \mathrm{val}_p(Q'(x))$;
   (d) $y \in \mathbb{Z}_p$.
2. Soit $a_0 \in \mathbb{Z}_p$ tel que $Q(a_0) \in Q'(a_0)^2 p^k \mathbb{Z}_p$. Montrer qu'il existe un unique $a \in \mathbb{Z}_p$ tel que $Q(a) = 0$ et $a - a_0 \in Q'(a_0) p^k \mathbb{Z}_p$.

Exercice 3. Dans cet exercice, on s'intéresse au cas $p = 2$.

1. Montrer qu'on a un isomorphisme de groupes naturel $\mathbb{Z}_2^\times \simeq \{\pm 1\} \times (1 + 4\mathbb{Z}_2)$.
2. Montrer que le sous-groupe $1 + 4\mathbb{Z}_2$ de $\mathbb{Z}_2^\times$ est sans torsion, c'est-à-dire que tous les éléments de $1 + 4\mathbb{Z}_2$ distincts de l'élément neutre sont d'ordre infini.
3. Soit $b \in \mathbb{Z}_2^\times$. Montrer que b est un carré de $\mathbb{Z}_2$ si, et seulement si, $b \in 1 + 8\mathbb{Z}_2$.
4. En déduire que le groupe $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2$ est d'ordre 8.

Exercice 4.(Isomorphismes de corps)

1. Soit l un nombre premier. Montrer que $\mathbb{Q}_l$ et $\mathbb{Q}_p$ sont isomorphes (en tant que corps) si, et seulement si, $l = p$.
2. Soit $a \in \mathbb{Q}_p^\times$. Montrer que $a \in \mathbb{Z}_p^\times$ si, et seulement si, il existe une infinité d'entiers $n \in \mathbb{N}$ tels que $\exists u \in \mathbb{Z}_p,\ a^{p-1} = u^n$.
3. Soit $\varphi : \mathbb{Q}_p \to \mathbb{Q}_p$ un morphisme d'anneaux non nul. Montrer que φ est une isométrie.
4. En déduire le groupe $\mathrm{Aut}(\mathbb{Q}_p)$ des automorphismes de corps de $\mathbb{Q}_p$.

Exercice 5. Notons $\mu(\mathbb{Q}_p)$ l'ensemble des racines de l'unité de $\mathbb{Q}_p^\times$.

1. On suppose $p \neq 2$. Soit $n \in \mathbb{N}^*$ et ζ une racine n-ème de l'unité.
   (a) On suppose que $\zeta \in 1 + p\mathbb{Z}_p$ et on écrit $\zeta = 1 + pt$. Montrer que $t = 0$ ou $p \mid n$.
   (b) On suppose que $n = p$. Montrer que $t = 0$.
   (c) Justifier que $\mu(\mathbb{Q}_p)$ est un sous-groupe de $\mathbb{Z}_p^\times$.
   (d) En déduire que $\mu(\mathbb{Q}_p) = \mu_{p-1}$ est cyclique d'ordre $p - 1$.
   Indication : on pourra considérer l'homomorphisme de groupes $\varphi : \mu(\mathbb{Q}_p) \to \mathbb{F}_p^\times$ obtenu par réduction modulo p.
2. On suppose désormais que $p = 2$. Montrer que $\mu(\mathbb{Q}_2) = \{\pm 1\}$.

Exercice 6. On suppose $p \neq 2$. Soit $b \in p\mathbb{Z}_p$.

1. Montrer qu'il existe un unique $c \in p\mathbb{Z}_p$ tel que $2c + c^2 = b$. Montrer que de plus, on a $\mathrm{val}_p(b) = \mathrm{val}_p(c)$.
2. Qu'advient-il si on suppose $p = 2$ ou $b \in \mathbb{Z}_p^\times$.

Exercice 7.(Critère d'irréductibilité d'Eisenstein)

Soit $f = \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}_p[X]$ tel que :
- $a_d \not\equiv 0 \mod p\mathbb{Z}_p$;
- $a_k \equiv 0 \mod p\mathbb{Z}_p$ pour tout $k \in [\![0, d-1]\!]$;
- $a_0 \not\equiv 0 \mod p^2\mathbb{Z}_p$.

Montrer que f est irréductible sur $\mathbb{Q}_p[X]$.