Construction algébrique de $\mathbb{Z}_p$; lemme de Hensel

Dans toute la suite, p est un nombre premier.

Exercice 1. En utilisant le lemme de Hensel, résoudre les équations modulaires suivantes :

1. $x^2 + 6 \equiv 0 \mod 5^4$;
2. $x^2 + x + 8 \equiv 0 \mod 7^4$;
3. $x^2 + x + 8 \equiv 0 \mod 9^4$.

Exercice 2. Montrer que le polynôme $X^3 - 4$ admet une unique racine dans $\mathbb{Q}_5$.

Exercice 3.(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) $y - x \in p^k Q'(x)\mathbb{Z}_p$ et $y \in \mathbb{Z}_p$;
   (b) $Q(y) \in p^{k+1} Q'(x)^2 \mathbb{Z}_p$;
   (c) $\mathrm{val}_p(Q'(y)) = \mathrm{val}_p(Q'(x))$.
2. Soit $a_0 \in \mathbb{Z}_p$ tel que $Q(a_0) \in Q'(a_0)^2 p^k \mathbb{Z}_p$.
   (a) On pose $a_{n+1} = a_n - \frac{Q(a_n)}{Q'(a_n)}$ pour tout $n \in \mathbb{N}^*$. Montrer que ceci définit bien une suite $(a_n)_n$ d'éléments de $\mathbb{Z}_p$ et que cette suite converge.
   (b) En déduire 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 4. 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, $b \in 1 + 8\mathbb{Z}_2$.
   Indication : on pourra utiliser le résultat de l'exercice précédent.
4. (Facultatif) Montrer que l'ensemble des carrés de $\mathbb{Q}_2^\times$ est un sous-groupe d'indice 8 de $\mathbb{Q}_2^\times$.

Exercice 5.(Relèvement de Teichmüller)
On note $\varepsilon : \mathbb{Z}_p \to \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le morphisme d'anneaux naturel.

1. Rappeler pourquoi pour tout $a \in \mathbb{Z}$, la suite $(a^{p^n})_n$ est de Cauchy dans $\mathbb{Z}$ pour la norme $|\cdot|_p$.

Notons $\ell(a)$ sa limite dans $\mathbb{Z}_p$.

2. Montrer que $a \mapsto \ell(a)$ induit une application $\tau : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_p$ telle que $\varepsilon \circ \tau$ est l'identité de $\mathbb{F}_p$ et que $\tau(x)^p = \tau(x)$ pour tout $x \in \mathbb{Z}/p\mathbb{Z}$.

L'application $\tau : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_p$ est appelée *relèvement de Teichmüller*.

3. Montrer que $\tau(0) = 0$, que $\tau(1) = 1$, que $\tau(-1) = -1$ et que $\tau(xy) = \tau(x)\tau(y)$ mais que, en général, $\tau(x + y) \neq \tau(x) + \tau(y)$.

Exercice 6. 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 7. Soit ℓ un nombre premier. Montrer que $\mathbb{Q}_\ell$ et $\mathbb{Q}_p$ sont isomorphes (en tant que corps) si, et seulement si, $\ell = p$.

Exercice 8.(Automorphismes de $\mathbb{Q}_p$)

1. Soit $a \in \mathbb{Q}_p^\times$.
   (a) Montrer que si $a \in 1 + p\mathbb{Z}_p$ et si $n \in \mathbb{N}$ est premier à p, alors l'équation $x^n = a$ a une solution dans $\mathbb{Q}_p$.
   (b) Réciproquement, montrer que, si pour tout $n \in \mathbb{N}$ premier à p l'équation $x^n = a$ a une solution dans $\mathbb{Q}_p$, alors $a \in 1 + p\mathbb{Z}_p$.
   (c) En déduire que $a \in \mathbb{Z}_p^\times$ si, et seulement si, il existe une infinité d'entiers $n \in \mathbb{N}$ tels que l'équation $x^n = a^{p-1}$ a une solution dans $\mathbb{Z}_p$.
2. Soit $\varphi : \mathbb{Q}_p \to \mathbb{Q}_p$ un morphisme d'anneaux non nul. Montrer que φ est une isométrie.
3. En déduire que le groupe des automorphismes de corps de $\mathbb{Q}_p$ est réduit à l'identité.

Exercice 9. 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 $b \in \mathbb{Z}_p^\times$.