# EXERCISES AND SUPPLEMENTAL TOPICS FOR LECTURE 5

## 1. Exercises on Hensel's lemma

(1) Prove the uniqueness part of Hensel's lemma. That is, if $f(x) \in \mathbb{Z}_p[x]$ and $\alpha \in \mathbb{Z}_p$ is such that $|f(\alpha)|_p < 1$ but $|f'(\alpha)_p| = 1$, then there exists a *unique* $\beta \in \mathbb{Z}_p$ such that $|\alpha - \beta|_p < 1$ and $f(\beta) = 0$. Existence follows from Newton's method (as in the lecture).

(2) One can also prove Hensel's lemma (both existence and uniqueness) using the *contraction mapping principle.* If $(X, d)$ is a complete metric space and $g : X \to X$ is a function with $d(g(x), g(y)) \leq cd(x, y)$ for some $c < 1$, then $g$ has a unique fixed point. (How to find this fixed point: start with any $x_0 \in X$. Then consider the sequence $x_0, g(x_0), g(g(x_0)), \dots$ and take its limit.)

Let $f(x) \in \mathbb{Z}_p[x]$ and $\alpha \in \mathbb{Z}_p$ be as in the statement of Hensel's lemma. Let $X = \{x \in \mathbb{Z}_p : |x - \alpha|_p < 1\}$, which is a complete metric space (why?). Let $g : X \to X$ be the map given by $g(x) = x - \frac{f(x)}{f'(\alpha)}$. Check that $g$ is a contraction and deduce Hensel's lemma. There is a nice discussion of Hensel's lemma and the various methods of proving it in K. Conrad's notes: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf`.

(3) Let $p > 2$. Show that if $\mathbb{Q}_p$ contains a primitive $r$th root of unity, then $r \mid p - 1$.

(4) A more general form of Hensel's lemma (there are also generalizations involving factorizations of polynomial). Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial. Let $\alpha \in \mathbb{Z}_p$ be such that $|f(\alpha)|_p < |f'(\alpha)|_p^2$. Then show that one can find a root $\beta$ of $f$ with $|\beta - \alpha|_p < 1$.

## 2. Exercises on quadratic forms over $\mathbb{Q}_p$

(1) Let $p > 2$. Let $u \in \mathbb{Z}_p^\times$ be an element such that $\overline{u} \in \mathbb{F}_p^\times$ is not a square. Show that the form $\langle 1, -u, p, -pu \rangle$ is anisotropic over $\mathbb{Q}_p$. More generally, you should show the following: let $\langle u_1, \dots, u_r \rangle \oplus \langle pv_1, \dots, pv_s \rangle$ be a quadratic form over $\mathbb{Q}_p$, with $u_i, v_i \in \mathbb{Z}_p^\times$. Then this form is isotropic if and only if *either* of the quadratic forms $\langle \overline{u_1}, \dots, \overline{u_r} \rangle$ *or* $\langle \overline{v_1}, \dots, \overline{v_s} \rangle$ is isotropic.

(2) Let $K$ be any field of characteristic $\neq 2$. Generalizing the argument in lecture (and the above exercise) to show that $u(\mathbb{Q}_p) = 4$, show that $u(K((t))) = 2u(K)$ (here the parameter $t$ replaces $p$). In particular, construct fields of $u$-invariant any power of 2. (It is an open problem exactly which integers occur as $u$-invariants.) Also prove (another case of Springer's theorem) that there is an isomorphism of abelian groups

$$W(K((t))) \simeq W(K) \oplus W(K).$$

Unlike the case in lecture (of $\mathbb{Q}_p$ and $\mathbb{F}_p$), there is an inclusion of fields $K \subset K((t))$.

---

*Date*: July 16, 2021.

## 3. Exercises on squares in $\mathbb{Q}_2$

(1) Show that any element $x \in \mathbb{Z}_2$ (for example, $-7$) with $x \equiv 1 \bmod 8$ is a square. The square root is of the form $1 + 2y$, so one needs to solve $(1 + 2y)^2 = x$.
(2) Show that the group $\mathbb{Q}_2^\times / \mathbb{Q}_2^\times \simeq (\mathbb{Z}/2)^3$. Generators of this group can be taken to be the classes of $2, -1, 5$.
(3) Let $p > 2$. Show that an element of $\mathbb{Z}_p^\times$ which is a $p$th power in $(\mathbb{Z}/p^2)^\times$ is a $p$th power in $\mathbb{Z}_p^\times$. You can prove this either using Hensel's lemma or the $p$-adic logarithm and exponential functions.