Discussion of 18.786 (Spring 2016) homework set #1

Darij Grinberg, Sam Raskin

March 15, 2016

1. Solution to problem 1

Let π be a uniformizer for $\mathcal{O}_K$; thus, $\mathfrak{p} = \pi\mathcal{O}_K$.

(a) Let $M = 2v_{\mathfrak{p}}(2) + 1$. We claim that every element of $1 + \mathfrak{p}^M$ is a square.

In fact, let $N = v_{\mathfrak{p}}(2) + 1$. Then we claim that the squaring map $x \mapsto x^2$ takes $1 + \mathfrak{p}^N$ to $1 + \mathfrak{p}^M$, and is an isomorphism between these two groups.

Indeed, for $x \in \mathfrak{p}^N$, we have:

$$(1 + x)^2 = 1 + 2x + x^2$$

and we observe that:

$$2x \in \mathfrak{p}^{N + v_{\mathfrak{p}}(2)} = \mathfrak{p}^M$$

while $x^2 \in \mathfrak{p}^{2N} \subset \mathfrak{p}^M$.

To see that the induced map is an isomorphism, we filter both sides, and will show that the map is an isomorphism on associated graded.

Namely, filter both sides via the subgroups $1 + \mathfrak{p}^{N+i}$ and $1 + \mathfrak{p}^{M+i}$ ($i \geq 0$) respectively. Clearly these filtrations are complete. Moreover, the above calculation shows that squaring takes $1 + \mathfrak{p}^{N+i}$ to $1 + \mathfrak{p}^{M+i}$ for all $i \geq 0$, so our map preserves the filtrations.

To calculate what happens at the associated graded level, take π a uniformizer. Then for $x \in \mathcal{O}_K$, the squaring map sends $1 + \pi^{N+i}x$ to $1 + 2\pi^{N+i}x + \pi^{2N+2i}x^2$. Modulo $1 + \mathfrak{p}^{M+i+1}$, the last summand is zero (since $2N \geq M + 1$). To project to k, which is the ith associated graded term of our filtration on $1 + \mathfrak{p}$, we should divide by π^{M+i} and then project modulo $\mathfrak{p}$: therefore, we obtain $2\pi^{N-M}x \bmod \mathfrak{p}$

as the result. Note that $2\pi^{N-M} = 2\pi^{-v_{\mathfrak{p}}(2)}$ is a unit, so the conclusion is that the map $k \to k$ given by the ith associated graded map is multiplication by the reduction of the unit $2\pi^{-v_{\mathfrak{p}}(2)}$.

Clearly this an isomorphism for every i, so we obtain the claim.

(b) It is clear that $\left(K^{\times}\right)^2$ is a subgroup of $K^{\times}$ (since $K^{\times}$ is abelian). It remains to prove that $\left[K^{\times} : \left(K^{\times}\right)^2\right] = 4\left|k\right|^{v_{\mathfrak{p}}(2)}$.

We first recall that

$$K^{\times} \to \mathbb{Z} \times \mathcal{O}_K^{\times}, \qquad a \mapsto \left(v_{\mathfrak{p}}\left(a\right), \frac{a}{\pi^{v_{\mathfrak{p}}(a)}}\right) \tag{1}$$

is a group isomorphism (with inverse $\mathbb{Z} \times \mathcal{O}_K^{\times} \to K^{\times},\ (n,b) \mapsto \pi^n b$). Thus,

$$\begin{aligned}\left[K^{\times} : \left(K^{\times}\right)^2\right] &= \left[\mathbb{Z} \times \mathcal{O}_K^{\times} : \left(\mathbb{Z} \times \mathcal{O}_K^{\times}\right)^2\right] \\ &= \underbrace{\left[\mathbb{Z} : \underbrace{\mathbb{Z}^2}_{\text{this means } 2\mathbb{Z}}\right]}_{=2} \cdot \left[\mathcal{O}_K^{\times} : \left(\mathcal{O}_K^{\times}\right)^2\right] = 2\left[\mathcal{O}_K^{\times} : \left(\mathcal{O}_K^{\times}\right)^2\right].\end{aligned}$$

Hence, it remains to prove that $\left[\mathcal{O}_K^{\times} : \left(\mathcal{O}_K^{\times}\right)^2\right] = 2\left|k\right|^{v_{\mathfrak{p}}(2)}$.

There are many ways to do this; here is a particularly slick one. We shall use the following fact:

Proposition 1.1. Let

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of abelian groups. Assume that both of its rows are exact sequences. Assume also that the groups $\operatorname{Ker} f$, $\operatorname{Ker} g$, $\operatorname{Ker} h$, $\operatorname{Coker} f$ and $\operatorname{Coker} h$ are finite. Then, the group $\operatorname{Coker} g$ is finite, and satisfies

$$\left|\operatorname{Coker} f\right| \cdot \left|\operatorname{Ker} g\right| \cdot \left|\operatorname{Coker} h\right| = \left|\operatorname{Ker} f\right| \cdot \left|\operatorname{Coker} g\right| \cdot \left|\operatorname{Ker} h\right|.$$

Proof of Proposition 1.1. The snake lemma yields an exact sequence

$$0 \longrightarrow \operatorname{Ker} f \longrightarrow \operatorname{Ker} g \longrightarrow \operatorname{Ker} h \longrightarrow \operatorname{Coker} f \longrightarrow \operatorname{Coker} g \longrightarrow \operatorname{Coker} h \longrightarrow 0.$$

The proposition follows easily from this (details left to the reader). □

The next lemma is even easier, and wholly left to the reader:

Lemma 1.2. Let A and B be two finite abelian groups. Let $f : A \to B$ be a group homomorphism. Then, $\dfrac{|\operatorname{Coker} f|}{|\operatorname{Ker} f|} = \dfrac{|B|}{|A|}$.

Now, let M and N be as in the first part, and let Sq_1 denote the map

$$\begin{aligned} \mathrm{Sq}_1 : 1 + \mathfrak{p}^N &\to 1 + \mathfrak{p}^M, \\ a &\mapsto a^2, \end{aligned}$$

which we saw is a group isomorphism in the first part.

Also, define a map

$$\begin{aligned} \mathrm{Sq}_2 : \mathcal{O}_K^\times &\to \mathcal{O}_K^\times, \\ a &\mapsto a^2. \end{aligned}$$

Clearly, this Sq_2 is a group homomorphism, and the previously defined map $\mathrm{Sq}_1 : 1 + \mathfrak{p}^N \to 1 + \mathfrak{p}^{N+v_\mathfrak{p}(2)}$ is a restriction of Sq_1. Furthermore, $\operatorname{Ker}(\mathrm{Sq}_2) = \{1, -1\}$ and thus $|\operatorname{Ker}(\mathrm{Sq}_2)| = 2$.

Our two maps Sq_1 and Sq_2 fit into a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 1+\mathfrak{p}^N & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & \left(\mathcal{O}_K/\mathfrak{p}^N\right)^\times & \longrightarrow & 0\,, \\ & & \cong\downarrow \mathrm{Sq}_1 & & \downarrow \mathrm{Sq}_2 & & & & \\ 0 & \longrightarrow & 1+\mathfrak{p}^{N+v_\mathfrak{p}(2)} & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & \left(\mathcal{O}_K/\mathfrak{p}^{N+v_\mathfrak{p}(2)}\right)^\times & \longrightarrow & 0 \end{array}$$

where the horizontal arrows are given by the canonical inclusions and projections. The two rows of this diagram are exact sequences, and thus there is a unique group homomorphism $\mathrm{Sq}_3 : \left(\mathcal{O}_K/\mathfrak{p}^N\right)^\times \to \left(\mathcal{O}_K/\mathfrak{p}^{N+v_\mathfrak{p}(2)}\right)^\times$ which makes the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 1+\mathfrak{p}^N & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & \left(\mathcal{O}_K/\mathfrak{p}^N\right)^\times & \longrightarrow & 0 \\ & & \cong\downarrow \mathrm{Sq}_1 & & \downarrow \mathrm{Sq}_2 & & \downarrow \mathrm{Sq}_3 & & \\ 0 & \longrightarrow & 1+\mathfrak{p}^{N+v_\mathfrak{p}(2)} & \longrightarrow & \mathcal{O}_K^\times & \longrightarrow & \left(\mathcal{O}_K/\mathfrak{p}^{N+v_\mathfrak{p}(2)}\right)^\times & \longrightarrow & 0 \end{array} \tag{2}$$

commute. Call this map Sq_3.

Since Sq_1 is an isomorphism, we have $\operatorname{Ker}(\mathrm{Sq}_1) = 1$ and $\operatorname{Coker}(\mathrm{Sq}_1) = 1$ (where we use 1 to denote the trivial group). As we already know, $|\operatorname{Ker}(\mathrm{Sq}_2)| = 2$. In particular, $\operatorname{Ker}(\mathrm{Sq}_1)$, $\operatorname{Coker}(\mathrm{Sq}_1)$ and $\operatorname{Ker}(\mathrm{Sq}_2)$ are finite groups.

Also, $\operatorname{Ker}\left(\mathrm{Sq}_3\right)$ and $\operatorname{Coker}\left(\mathrm{Sq}_3\right)$ are finite groups (since Sq_3 is a morphism between finite groups). Therefore, Proposition 1.1 (applied to the diagram (2)) shows that

$$|\operatorname{Coker}(\mathrm{Sq}_1)| \cdot |\operatorname{Ker}(\mathrm{Sq}_2)| \cdot \left|\operatorname{Coker}\left(\mathrm{Sq}_3\right)\right| = |\operatorname{Ker}(\mathrm{Sq}_1)| \cdot |\operatorname{Coker}(\mathrm{Sq}_2)| \cdot \left|\operatorname{Ker}\left(\mathrm{Sq}_3\right)\right|.$$

Plugging in the orders we have already calculated, we obtain:

$$2 \cdot \left|\operatorname{Coker}\left(\mathrm{Sq}_3\right)\right| = \left|\operatorname{Coker}\left(\mathrm{Sq}_2\right)\right| \cdot \left|\operatorname{Ker}\left(\mathrm{Sq}_3\right)\right|.$$

We are trying to solve for $\left|\operatorname{Coker}\left(\mathrm{Sq}_2\right)\right|$, so it remains to calculate $\frac{\left|\operatorname{Coker}\left(\mathrm{Sq}_3\right)\right|}{\left|\operatorname{Ker}\left(\mathrm{Sq}_3\right)\right|}$. By Lemma 1.2, this is $\frac{\left|\left(\mathcal{O}_K/\mathfrak{p}^M\right)^\times\right|}{\left|\left(\mathcal{O}_K/\mathfrak{p}^N\right)^\times\right|}$. Filtering the unit group in the usual way (or explicitly calculating the orders), we find this quotient to be $|k|^{M-N} = |k|^{v_\mathfrak{p}(2)}$.

Plugging this in for our earlier calculation, we obtain:

$$2 \cdot |k|^{v_\mathfrak{p}(2)} = \left|\operatorname{Coker}\left(\mathrm{Sq}_2\right)\right| \tag{3}$$

as desired.

(c) First, we shall characterize $\left(\mathbb{Z}_2^\times\right)^2$.

Set $p = 2$ and $K = \mathbb{Q}_2$; thus, $\mathcal{O}_K = \mathbb{Z}_2$, $\mathfrak{p} = 2\mathbb{Z}_2$, $k = \mathbb{F}_2$ and $v_\mathfrak{p} = v_2$. Thus, (3) rewrites as follows: $2\left|\mathbb{F}_2\right|^{v_2(2)} = \left|\operatorname{Coker}\left(\mathrm{Sq}_2\right)\right| = \left[\mathbb{Z}_2^\times : \left(\mathbb{Z}_2^\times\right)^2\right]$. Hence,

$$\left[\mathbb{Z}_2^\times : \left(\mathbb{Z}_2^\times\right)^2\right] = 2\underbrace{\left|\mathbb{F}_2\right|^{v_2(2)}}_{=2^1=2} = 4.$$

It is easy to see that $\left(\mathbb{Z}_2^\times\right)^2 \subseteq 1 + 8\mathbb{Z}_2$ (in fact, the canonical projection $\mathbb{Z}_2 \to \mathbb{Z}_2/8\mathbb{Z}_2 \cong \mathbb{Z}/8\mathbb{Z}$ sends $\left(\mathbb{Z}_2^\times\right)^2$ to $\left(\left(\mathbb{Z}/8\mathbb{Z}\right)^\times\right)^2$, which is the trivial subgroup of $\left(\mathbb{Z}/8\mathbb{Z}\right)^\times$). But the canonical projection $\mathbb{Z}_2 \to \mathbb{Z}_2/8\mathbb{Z}_2 \cong \mathbb{Z}/8\mathbb{Z}$ restricts to a surjection $\mathbb{Z}_2^\times \to \left(\mathbb{Z}/8\mathbb{Z}\right)^\times$, whose kernel is $1 + 8\mathbb{Z}_2$. Hence, the index of the subgroup $1 + 8\mathbb{Z}_2$ in $\mathbb{Z}_2^\times$ must equal the size $\left|\left(\mathbb{Z}/8\mathbb{Z}\right)^\times\right|$ of the image of this surjection. In other words, $\left[\mathbb{Z}_2^\times : \left(1 + 8\mathbb{Z}_2\right)\right] = \left|\left(\mathbb{Z}/8\mathbb{Z}\right)^\times\right| = 4$. Comparing this with $\left[\mathbb{Z}_2^\times : \left(\mathbb{Z}_2^\times\right)^2\right] = 4$, we conclude that the two subgroups $\left(\mathbb{Z}_2^\times\right)^2$ and $1 + 8\mathbb{Z}_2$ of $\mathbb{Z}_2^\times$ have the same (finite) index in $\mathbb{Z}_2^\times$. Since one of these two subgroups is contained in the other (because $\left(\mathbb{Z}_2^\times\right)^2 \subseteq 1 + 8\mathbb{Z}_2$), this yields that these two subgroups are identical. In other words, $\left(\mathbb{Z}_2^\times\right)^2 = 1 + 8\mathbb{Z}_2$.

But in our setting, the group isomorphism (1) takes the form

$$\mathbb{Q}_2^\times \to \mathbb{Z} \times \mathbb{Z}_2^\times, \qquad a \mapsto \left(v_2\left(a\right), \frac{a}{2^{v_2(a)}}\right)$$

(where we choose 2 as our uniformizer π). Thus, this isomorphism takes the subgroup $\left(\mathbb{Q}_2^\times\right)^2$ of $\mathbb{Q}_2^\times$ to the subgroup $\left(\mathbb{Z} \times \mathbb{Z}_2^\times\right)^2 = 2\mathbb{Z} \times \underbrace{\left(\mathbb{Z}_2^\times\right)^2}_{=1+8\mathbb{Z}_2} = 2\mathbb{Z} \times \left(1 + 8\mathbb{Z}_2\right)$ of $\mathbb{Z} \times \mathbb{Z}_2^\times$. This means that an element x of $\mathbb{Q}_2^\times$ is a square (in $\mathbb{Q}_2^\times$) if and only if $v_2\left(x\right)$ belongs to the subgroup $2\mathbb{Z}$ of $\mathbb{Z}$, and $\frac{x}{2^{v_2(x)}}$ belongs to the subgroup $1 + 8\mathbb{Z}_2$ of $\mathbb{Z}_2^\times$. This is exactly what the problem asked us to prove.

2. Solution to problem 3

If V is a subgroup of an abelian group U, and if $p \in U$, then we shall use the notation $[p]_V$ for the projection of p on U/V.

(a) Let $x \in A$ and $n \geq 0$. We need to show that the map

$$F_nA/F_{n+1}A \to F_nB/F_{n+1}B, \qquad [y]_{F_{n+1}A} \mapsto [f(x+y) - f(x)]_{F_{n+1}B}$$

is well-defined. In other words, we need to show two statements:

Statement 1: If $y \in F_nA$, then $f(x+y) - f(x) \in F_nB$.

Statement 2: If y and y' are two elements of F_nA satisfying $y \equiv y' \bmod F_{n+1}A$, then $f(x+y) - f(x) \equiv f(x+y') - f(x) \bmod F_{n+1}B$.

Proof of Statement 1: Let $y \in F_nA$. Then, $x + y \in x + F_nA$. But f preserves the filtration; thus, f maps $x + F_nA$ to $f(x) + F_nB$. In other words, $f(x + F_nA) \subseteq f(x) + F_nB$. Hence, $f\left(\underbrace{x+y}_{\in x+F_nA}\right) \in f(x + F_nA) \subseteq f(x) + F_nB$. In other words, $f(x+y) - f(x) \in F_nB$. This proves Statement 1.

Proof of Statement 2: Let y and y' be two elements of F_nA satisfying $y \equiv y' \bmod F_{n+1}A$. Thus, $y \in y' + F_{n+1}A$, so that $x + y \in x + y' + F_{n+1}A$. But f preserves the filtration; thus, f maps $x + y' + F_{n+1}A$ to $f(x+y') + F_{n+1}B$. In other words, $f(x + y' + F_{n+1}A) \subseteq f(x+y') + F_{n+1}B$. Hence, $f\left(\underbrace{x+y}_{\in x+y'+F_{n+1}A}\right) \in f(x + y' + F_{n+1}A) \subseteq f(x+y') + F_{n+1}B$. In other words, $f(x+y) \equiv f(x+y') \bmod F_{n+1}B$. Hence, $f(x+y) - f(x) \equiv f(x+y') - f(x) \bmod F_{n+1}B$. This proves Statement 2.

Thus, part **(a)** of the problem is solved.

(b) Let $b \in B$. We will find some $a \in A$ satisfying $f(a) = b$.

We shall construct a sequence $(a_0, a_1, a_2, \ldots) \in A^\infty$ of elements of A such that every $n \geq 1$ satisfies

$$a_n \equiv a_{n-1} \bmod F_{n-1}A \tag{4}$$

and every $n \geq 0$ satisfies

$$f(a_n) \equiv b \bmod F_nB. \tag{5}$$

We shall construct this sequence $(a_0, a_1, a_2, \ldots)$ recursively: We start by setting $a_0 = 0$; thus, (5) is clearly satisfied for $n = 0$. Now, let k be a nonnegative integer, and assume that we have defined $a_k \in A$ such that (5) is satisfied for $n = k$. We shall then define an $a_{k+1} \in A$ such that both (4) and (5) are satisfied for $n = k+1$.

Indeed, we have $f(a_k) \equiv b \bmod F_kB$ (since (5) is satisfied for $n = k$). Thus, $b - f(a_k) \in F_kB$. Hence, $[b - f(a_k)]_{F_{k+1}B} \in F_kB/F_{k+1}B$ is well-defined.

But by assumption, the symbol map

$$F_kA/F_{k+1}A \to F_kB/F_{k+1}B, \qquad [y]_{F_{k+1}A} \mapsto [f(x+y) - f(x)]_{F_{k+1}B}$$

is surjective for every $x \in A$. Applying this to $x = a_k$, we see that the symbol map

$$F_k A / F_{k+1} A \to F_k B / F_{k+1} B, \qquad [y]_{F_{k+1}A} \mapsto [f(a_k + y) - f(a_k)]_{F_{k+1}B}$$

is surjective. Thus, there exists some $y \in F_k A$ such that

$$[f(a_k + y) - f(a_k)]_{F_{k+1}B} = [b - f(a_k)]_{F_{k+1}B}. \tag{6}$$

Consider this y. From (6), we obtain $f(a_k + y) - f(a_k) \equiv b - f(a_k) \bmod F_{k+1}B$, so that $f(a_k + y) \equiv b \bmod F_{k+1}B$.

Now, set $a_{k+1} = a_k + y$. Thus, $a_{k+1} = a_k + \underbrace{y}_{\in F_k A} \in a_k + F_k A$, so that $a_{k+1} \equiv a_k \bmod F_k A$. In other words, (4) holds for $n = k+1$. Moreover, $f\left(\underbrace{a_{k+1}}_{=a_k+y}\right) = f(a_k + y) \equiv b \bmod F_{k+1}B$. In other words, (5) holds for $n = k+1$. Thus, we have defined an $a_{k+1} \in A$ such that both (4) and (5) are satisfied for $n = k+1$. This completes our recursive construction of the sequence $(a_0, a_1, a_2, \ldots)$.

Now, the sequence $(a_0, a_1, a_2, \ldots) \in A^\infty$ is Cauchy (because of (4)). Hence, it has a limit $a \in A$. Consider this a. We claim that $f(a) = b$.

Indeed, let $n \geq 0$ be an integer. Then, $a_n \equiv a \bmod F_n A$ (because (4) shows that the sequence $(a_0, a_1, a_2, \ldots)$ stabilizes modulo $F_n A$ at its term a_n). In other words, $a \in a_n + F_n A$. But from (5), we obtain $f(a_n) \equiv b \bmod F_n B$.

The map f preserves the filtration, and thus maps $a_n + F_n A$ to $f(a_n) + F_n B$. In other words, $f(a_n + F_n A) \subseteq f(a_n) + F_n B$. Hence, $f\left(\underbrace{a}_{\in a_n + F_n A}\right) \in f(a_n + F_n A) \subseteq f(a_n) + F_n B$. Thus, $f(a) \equiv f(a_n) \equiv b \bmod F_n B$, so that $f(a) - b \in F_n B$.

Now, forget that we fixed n. We thus have shown that $f(a) - b \in F_n B$ for every $n \geq 0$. Hence, $f(a) - b \in \bigcap_{n \geq 0} (F_n B) = 0$ (since the topology on B is complete and thus Hausdorff). In other words, $f(a) = b$.

Now, let us forget that we fixed b. Thus, for every $b \in B$, we have constructed an $a \in A$ such that $f(a) = b$. Hence, the map f is surjective. Part **(b)** of the problem is solved.

(c) We shall prove two versions of Hensel's lemma:

Theorem 2.1. Let $f(t) \in \mathcal{O}_K[t]$ be a polynomial with $f(\mathfrak{p}) \subseteq \mathfrak{p}$ and $f'(\mathfrak{p}) \subseteq \mathcal{O}_K^\times$. Then, f has a zero in $\mathfrak{p}$.

Theorem 2.2. Let $f(t) \in \mathcal{O}_K[t]$ be a polynomial. Let proj be the canonical projection $\mathcal{O}_K \to k$. Let $\overline{f}(t) \in k[t]$ be the image of $f(t)$ under the projection $\operatorname{proj}[t] : \mathcal{O}_K[t] \to k[t]$. Let $\overline{x}$ be a root of $\overline{f}(t)$ in k such that $\overline{f}'(\overline{x}) \neq 0$. Then, there exists a root x of f in $\mathcal{O}_K$ such that $\overline{x} = \operatorname{proj} x$.

(Both of these theorems can be amended to include uniqueness statements, but we shall not need these.)

Proof of Theorem 2.1. Let $A = \mathfrak{p}$ and $B = \mathfrak{p}$, equipped with filtrations given by $F_n A = \mathfrak{p}^{n+1}$ and $F_n B = \mathfrak{p}^{n+1}$. Clearly, both of these filtered groups A and B are complete. The polynomial f gives rise to a map $\mathfrak{p} \to \mathfrak{p}$, $a \mapsto f(a)$ (since $f(\mathfrak{p}) \subseteq \mathfrak{p}$), which we shall also denote by f (by abuse of notation). This map f preserves the filtration (in the sense of this exercise)[1]. Thus, part **(a)** of this exercise shows that the symbol map

$$\mathfrak{p}^{n+1}/\mathfrak{p}^{n+2} \to \mathfrak{p}^{n+1}/\mathfrak{p}^{n+2}, \qquad [y]_{\mathfrak{p}^{n+2}} \mapsto [f(x+y) - f(x)]_{\mathfrak{p}^{n+2}}$$

is well-defined for every $n \geq 0$ and every $x \in \mathfrak{p}$. Moreover, this symbol map is surjective[2]. Hence, part **(b)** of this exercise shows that the map $f : \mathfrak{p} \to \mathfrak{p}$ is surjective. Hence, there exists some $a \in \mathfrak{p}$ such that $f(a) = 0$. In other words, f has a zero in $\mathfrak{p}$. This proves Theorem 2.1. $\square$

[1] This is a particular case of the following general fact: If R is a commutative ring, if $g \in R[t]$ is any polynomial, if $x \in R$, and if I is any ideal of R, then g maps $x + I$ to $g(x) + I$. (This, in turn follows from the fact that $x - y \mid g(x) - g(y)$ for any $g \in R[t]$ and any $x, y \in R$.)

[2] *Proof.* Fix $n \geq 0$ and $x \in \mathfrak{p}$. Let $b \in \mathfrak{p}^{n+1}/\mathfrak{p}^{n+2}$. We need to show that there exists some $y \in \mathfrak{p}^{n+1}$ such that $[f(x+y) - f(x)]_{\mathfrak{p}^{n+2}} = b$.

Write b as $[c]_{\mathfrak{p}^{n+2}}$ for some $c \in \mathfrak{p}^{n+1}$. Fix a uniformizer π of $\mathfrak{p}$. Notice that $\left(\pi^{n+1}\right)^2 = \pi^{2(n+1)} \in \mathfrak{p}^{2(n+1)} \subseteq \mathfrak{p}^{n+2}$ (since $2(n+1) \geq n+2$). Also, $\dfrac{c}{\pi^{n+1}} \in \mathcal{O}_K$ (since $c \in \mathfrak{p}^{n+1}$).

Fix $\lambda \in \mathcal{O}_K$. It is well-known that $f(t+s) \equiv f(t) + sf'(t) \bmod s^2$ in the polynomial ring $\mathcal{O}_K[t,s]$ (this is the algebraic version of the difference-limit definition $f'(t) = \lim\limits_{s \to 0} \dfrac{f(t+s) - f(t)}{s}$ of the derivative). Evaluating this congruence at $t = x$ and $s = \lambda\pi^{n+1}$, we obtain

$$f\left(x + \lambda\pi^{n+1}\right) \equiv f(x) + \lambda\pi^{n+1} f'(x) \bmod \left(\pi^{n+1}\right)^2.$$

Thus,

$$f\left(x + \lambda\pi^{n+1}\right) \equiv f(x) + \lambda\pi^{n+1} f'(x) \bmod \mathfrak{p}^{n+2} \tag{7}$$

(because $\left(\pi^{n+1}\right)^2 \in \mathfrak{p}^{n+2}$).

Let us now forget that we fixed λ. We thus have proven (7) for every $\lambda \in \mathcal{O}_K$. Now, recall that $x \in \mathfrak{p}$ and thus $f'(x) \in f'(\mathfrak{p}) \subseteq \mathcal{O}_K^\times$. Hence, there exists a $\lambda \in \mathcal{O}_K$ such that $\lambda\pi^{n+1} f'(x) = c$ (namely, $\lambda = \dfrac{c}{\pi^{n+1}} / f'(x)$; this is allowed because $\dfrac{c}{\pi^{n+1}} \in \mathcal{O}_K$). Consider this λ. From (7), we obtain

$$f\left(x + \lambda\pi^{n+1}\right) \equiv f(x) + \underbrace{\lambda\pi^{n+1} f'(x)}_{=c} = f(x) + c \bmod \mathfrak{p}^{n+2},$$

so that $f\left(x + \lambda\pi^{n+1}\right) - f(x) \equiv c \bmod \mathfrak{p}^{n+2}$ and thus $\left[f\left(x + \lambda\pi^{n+1}\right) - f(x)\right]_{\mathfrak{p}^{n+2}} = [c]_{\mathfrak{p}^{n+2}} = b$.

Moreover, $\underbrace{\lambda}_{\in \mathcal{O}_K} \underbrace{\pi^{n+1}}_{\in \mathfrak{p}^{n+1}} \in \mathfrak{p}^{n+1}$. Hence, there exists some $y \in \mathfrak{p}^{n+1}$ such that $[f(x+y) - f(x)]_{\mathfrak{p}^{n+2}} = b$ (namely, $y = \lambda\pi^{n+1}$). This completes our proof.

Proof of Theorem 2.2. There clearly exists some $z \in \mathcal{O}_K$ such that $\overline{x} = \operatorname{proj} z$. Fix such a z.

Define a polynomial $g \in \mathcal{O}_K[t]$ by $g(t) = f(t-z)$. Then, show that $g(\mathfrak{p}) \subseteq \mathfrak{p}$ and argue the rest by applying Theorem 2.1 to g instead of f. (Or read the proof in [Murfet05, Corollary 2].) □

Showing that -1 is a square in $\mathbb{Q}_5$ can easily be done using Theorem 2.2 (applied to $K = \mathbb{Q}_5$, $\mathcal{O}_K = \mathbb{Z}_5$, $p = 5$, $f(t) = t^2 + 1$ and $x = [2]_{5\mathcal{O}_K}$).

3. Solution sketch to problem 2

(a) Let $a, b \in K^\times$. Then,

$$v_\mathfrak{p}\left(\frac{a^{v_\mathfrak{p}(b)}}{b^{v_\mathfrak{p}(a)}}\right) = \underbrace{v_\mathfrak{p}\left(a^{v_\mathfrak{p}(b)}\right)}_{=v_\mathfrak{p}(b)v_\mathfrak{p}(a)} - \underbrace{v_\mathfrak{p}\left(b^{v_\mathfrak{p}(a)}\right)}_{=v_\mathfrak{p}(a)v_\mathfrak{p}(b)} = v_\mathfrak{p}(b)\,v_\mathfrak{p}(a) - v_\mathfrak{p}(a)\,v_\mathfrak{p}(b) = 0,$$

so that $\dfrac{a^{v_\mathfrak{p}(b)}}{b^{v_\mathfrak{p}(a)}} \in \mathcal{O}_K^\times$.

(b) The field k is a finite field, and thus its multiplicative group $k^\times$ is cyclic. Hence, the unique non-trivial character $k^\times \to \{1, -1\}$ is the map which sends every square in $k^\times$ to 1 and every non-square to -1. Let us denote this character by $\mathcal{L}$. Thus, $\mathcal{L}(a)$ (for some $a \in k^\times$) is the analogue of the Legendre symbol $\left(\dfrac{\overline{a}}{p}\right)$ for finite fields.

The rest of the solution is a (mostly literal) translation of [Raskin15, Proposition 3.16.2] with the following changes (no guarantee of completeness):

- Replace $\left(\dfrac{a}{p}\right)$ by $\mathcal{L}(a)$.
- Replace $\mathbb{F}_p$ by k.
- Replace $(a,b)_p$ by (a,b).
- Replace each remaining p by $\mathfrak{p}$, π (the uniformizer of $\mathfrak{p}$) or $|k|$ (depending on the context).
- Replace Hensel's lemma by Theorem 2.2.
- Replace Corollary 3.10.4 by the fact that $x \in \mathcal{O}_K^\times$ is a square if and only if $x \bmod \mathfrak{p}$ is a square in $k^\times$. (This is proven using Theorem 2.2, just as Corollary 3.10.4 is proven using Hensel's lemma.)

(c) See [Raskin15, Proposition 3.16.3].
(d) See [Raskin15, Proposition 3.16.3].

4. Solution sketch to problem 4

Follow the proof of [Raskin15, Proposition 3.15.1] with the obvious generalizations.

5. Solution sketch to problem 5

(a) I give two proofs in [Grinbe15].

(b) See [Conrad15, Theorem 4.21] (and, more directly, [Conrad15, Theorem 4.25], but that one is left as an exercise).

References

[Conrad15] Keith Conrad, *Quaternion algebras*, version 10 May 2015.

[Grinbe15] Darij Grinberg, *Why quaternion algebras have rank* 4, version 27 February 2016.

[Murfet05] Daniel Murfet, *Hensel's lemma*, version 8 April 2005.

[Raskin15] Sam Raskin, *Introduction to the arithmetic theory of quadratic forms*, version 28 March 2015.

18.786 Number Theory II: Class Field Theory

Spring 2016