Notes on the proof of the theorem of Hasse–Arf

We reformulate the proof of the theorem of Hasse–Arf [1, Chap. V §7 Théorème 1], under the assumption that the residue field F of K is perfect and L is a totally ramified cyclic extension of K. In fact, the perfectness assumption is redundant but we omit the proof.

The author thanks Takumi Watanabe for careful reading and numerous comments and Shigenao Tsuboi for pointing out an error in an earlier version.

Lemma 1. *Let K be a discrete valuation field and let L be a totally ramified cyclic extension of K of Galois group G. Define a subgroup A of $B = \mathcal{O}_L^\times$ by $A = \{s(u)/u \mid s \in G, u \in \mathcal{O}_L^\times\}$ and let $\mathrm{N}_{L/K}\colon B \to C = \mathcal{O}_K^\times$ denote the norm. Then, the morphism*

$$G \to H = \mathrm{Ker}(\mathrm{N}_{L/K}\colon B \to C)/A \tag{1}$$

sending s to $s(\pi)/\pi$ for a uniformizer π of L is an isomorphism independent of π.

Proof. Let $\sigma \in G$ be a generator and identify H with the Galois cohomology $\mathrm{H}^1(G, B) = \mathrm{Ker}(\mathrm{N}_{L/K}\colon \mathcal{O}_L^\times \to \mathcal{O}_K^\times)/(\sigma - 1)\mathcal{O}_L^\times$. Since L is totally ramified, the order of the cyclic group G equals the ramification index $e = e_{L/K}$. Since $\mathrm{H}^1(G, L^\times) = 0$ by Hilbert 90, the exact sequence $0 \to \mathcal{O}_L^\times \to L^\times \to \mathbf{Z} \to 0$ induces an isomorphism $\mathbf{Z}/e\mathbf{Z} \to H$ sending 1 to the class of $\sigma(\pi)/\pi$ independent of the choice of uniformizer π. Identifying $G = \langle\sigma\rangle$ with $\mathbf{Z}/e\mathbf{Z}$ by the generator σ, we obtain an isomorphism $G \to H$ sending σ^i to $(\sigma(\pi)/\pi)^i \equiv \sigma^i(\pi)/\pi$. □

We consider the filtration $B_m = 1 + \mathfrak{m}_L^m \subset B = \mathcal{O}_L^\times$ indexed by integers $m \geqq 1$ and the induced filtration $A_m = A \cap B_m$. For $m \geqq 1$, let $n \geqq 1$ be the largest integer such that $\mathrm{N}_{L/K}(B_m) \subset 1 + \mathfrak{m}_K^n$ and set $C_m = 1 + \mathfrak{m}_K^n$. For $X = A, B, C$, we also set $X_0 = X$ and define $\mathrm{Gr}_m X = X_m/X_{m+1}$ for $m \geqq 0$. We consider subcomplexes

$$A_m \to B_m \to C_m$$

of $A \to B \to C$ and the graded quotients

$$\mathrm{Gr}_m A \to \mathrm{Gr}_m B \to \mathrm{Gr}_m C.$$

The canonical morphism $\mathrm{Gr}_m A \to \mathrm{Gr}_m B$ is an injection. We define subgroups $H_m \subset H$ by $H_m = \mathrm{Ker}(\mathrm{N}\colon B_m \to C_m)/A_m$ and set $\mathrm{Gr}_m H = H_m/H_{m+1}$. We have $H_m = 0$ for m sufficiently large by [1, Chap. V §7 Lemme 9]).

Lemma 2. *Let $m \geqq 0$ be an integer.*

1. *The injection $H_m \to B_m/A_m$ induces an injection*

$$\mathrm{Gr}_m H \to \mathrm{Ker}(\mathrm{N}\colon \mathrm{Gr}_m B \to \mathrm{Gr}_m C)/\mathrm{Gr}_m A. \tag{2}$$

This is an isomorphism if K is complete and if the residue field F is algebraically closed.

2 ([1, Chap. V §6 Proposition 9]). *Assume that K is complete, that F is algebraically closed and that $\varphi(m)$ is an integer. Then, we have an isomorphism*

$$\mathrm{Gr}_m G \to \mathrm{Ker}(\mathrm{N}\colon \mathrm{Gr}_m B \to \mathrm{Gr}_m C). \tag{3}$$

Proof. 1. Since $H_m = \mathrm{Ker}(B_m/A_m \to C_m)$, by the commutative diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & B_{m+1}/A_{m+1} & \longrightarrow & B_m/A_m & \longrightarrow & \mathrm{Gr}_m B/\mathrm{Gr}_m A & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C_{m+1} & \longrightarrow & C_m & \longrightarrow & \mathrm{Gr}_m C & \longrightarrow & 0
\end{array} \tag{4}
$$

of exact sequences, we obtain an injection $\mathrm{Gr}_m H \to \mathrm{Ker}(\mathrm{Gr}_m B/\mathrm{Gr}_m A \to \mathrm{Gr}_m C)$. If K is complete and F is algebraically closed, the vertical arrows in (4) are surjections by [1, Chap. V §6 Corollaire 4]. □

Proposition 3. *Let K be a discrete valuation field and L be a totally ramified cyclic extension of K. We consider the following conditions on integer $m \geqq 0$:*

(1) $\mathrm{Gr}_m H \neq 0$.

(2) *The injection $\mathrm{Gr}_m A \to \mathrm{Gr}_m B$ is not an isomorphism.*

(3) $\mathrm{Gr}_m A = 0$.

(4) $\mathrm{Gr}_m C \neq 0$.

(5) $\varphi(m)$ *is an integer.*

1. *Assume $m \geqq 1$. Then, we have (1)⇒(2)⇔(3). If K is complete and if the residue field F is algebraically closed, the conditions (2), (3), (4) and (5) are equivalent to each other.*

2. *Assume $m = 0$. Then, the conditions (2), (3) and (4) hold, except possibly for (4) in the case $F = \mathbf{F}_2$. If K is complete, then (5) also holds.*

Proof. 1. (1)⇒(2): The assertion follows from the injection $\mathrm{Gr}_m H \to \mathrm{Gr}_m B/\mathrm{Gr}_m A$ in Lemma 2.1.

(2)⇒(3) [1, Chap. V §7 Lemme 11]: We show the contraposition. Suppose $\sigma(1+x)/(1+x) \equiv 1 + (\sigma(x) - x) \in \mathrm{Gr}_m A$ is a non-trivial element for $x \in \mathfrak{m}_L$. Then, for $a \in \mathcal{O}_K$, we have $\sigma(1+ax)/(1+ax) \equiv 1 + a(\sigma(x) - x) \in \mathrm{Gr}_m B$ and $\mathrm{Gr}_m A \to \mathrm{Gr}_m B$ is a surjection.

(3)⇒(2): Since $\mathrm{Gr}_m B \neq 0$, the condition (3) implies (2).

(3)⇒(4): By the assumptions $\mathrm{Gr}_m A = 0$, that K is complete and that the residue field F is algebraically closed, we have an injection $\mathrm{Gr}_m B/\mathrm{Gr}_m H \to \mathrm{Gr}_m C$ by Lemma 2.1. Since $\mathrm{Gr}_m H$ is cyclic and $\mathrm{Gr}_m B$ is not, we have $\mathrm{Gr}_m C \neq 0$.

(4)⇒(5): Let $n \geqq 1$ be the integer such that $C_m = 1 + \mathfrak{m}_K^n$. By the definition of n, we have $1 + \mathfrak{m}_K^{n+1} \not\supset \mathrm{N}(1 + \mathfrak{m}_L^m) \subset 1 + \mathfrak{m}_K^n$. If $\mathrm{Gr}_m C \neq 0$, we have $\mathrm{N}(1 + \mathfrak{m}_L^{m+1}) \subset 1 + \mathfrak{m}_K^{n+1}$. For $m' = \psi(n)$, by the assumption that K is complete and F is algebraically closed, we have $\mathrm{N}(1 + \mathfrak{m}_L^{m'}) = 1 + \mathfrak{m}_K^n$ and $\mathrm{N}(1 + \mathfrak{m}_L^{m'+1}) = 1 + \mathfrak{m}_K^{n+1}$ by [1, Chap. V §6 Corollaire 3].

From $\mathrm{N}(1+\mathfrak{m}_L^{m'+1}) = 1+\mathfrak{m}_K^{n+1} \not\supset \mathrm{N}(1+\mathfrak{m}_L^m)$, we obtain $m'+1 > m$. From $\mathrm{N}(1+\mathfrak{m}_L^{m+1}) \subset 1+\mathfrak{m}_K^{n+1} \subsetneqq 1+\mathfrak{m}_K^n = \mathrm{N}(1+\mathfrak{m}_L^{m'})$, we obtain $m+1 > m'$ conversely. Thus, $m = m' = \psi(n)$ and $n = \varphi(m)$ is an integer.

(5)⇒(2): Assume that K is complete and the residue field F is algebraically closed. By Lemma 2.2, the condition (5) implies that the kernel $\mathrm{Ker}(\mathrm{N}\colon \mathrm{Gr}_m B \to \mathrm{Gr}_m C)$ is finite. Hence $\mathrm{Gr}_m A \subset \mathrm{Ker}(\mathrm{N}\colon \mathrm{Gr}_m B \to \mathrm{Gr}_m C)$ is also finite. Since $\mathrm{Gr}_m B$ is infinite, this implies (2).

2. Since G acts trivially on the residue field $E = F$ of L, we have $A_0 = A_0 \cap B_1 = A_1$ and (3) holds. As in 1, (3) implies (2) and the condition (2) also holds. We have $\mathrm{Gr}_0 C = \mathcal{O}_K^\times/1 + \mathfrak{m}_K^n \neq 0$ for some integer $n \geqq 1$ and (4) holds. Since $\varphi(0) = 0$, the condition (5) also holds. □

Corollary 4. *Assume that K is complete and that the residue field F is algebraically closed. Then, the morphism $G \to H$ (1) induces an isomorphism $\mathrm{Gr}_m G \to \mathrm{Gr}_m H$ for every $m \geqq 0$.*

Proof. We define an isomorphism assuming that $\mathrm{Gr}_m H \neq 0$. By Lemma 2.1, we have an isomorphism $\mathrm{Gr}_m H \to \mathrm{Ker}(\mathrm{N}\colon \mathrm{Gr}_m B/\mathrm{Gr}_m A \to \mathrm{Gr}_m C)$ (2). By Proposition 3 (1)⇒(5) and Lemma 2.2, we have an isomorphism $\mathrm{Gr}_m G \to \mathrm{Ker}(\mathrm{N}\colon \mathrm{Gr}_m B \to \mathrm{Gr}_m C)$ (3). By Proposition 3 (1)⇒(3), we have $\mathrm{Gr}_m A = 0$ and we obtain an isomorphism $\mathrm{Gr}_m G \to \mathrm{Gr}_m H$. The isomorphism is induced by $G \to H$ (1).

By the isomorphisms, we have either $\#\mathrm{Gr}_m H = \#\mathrm{Gr}_m G$ or $\mathrm{Gr}_m H = 0$ for each $m \geqq 0$. Hence, we obtain $\#H = \prod_{m \geqq 0} \#\mathrm{Gr}_m H \leqq \prod_{m \geqq 0} \#\mathrm{Gr}_m G = \#G$ and the equality is equivalent to $\#\mathrm{Gr}_m H = \#\mathrm{Gr}_m G$ for every $m \geqq 0$. Since the equality holds by Lemma 1, we have $\#\mathrm{Gr}_m H = \#\mathrm{Gr}_m G$ for every $m \geqq 0$. □

Theorem 5. *Let K be a complete discrete valuation field and L be a totally ramified cyclic extension of K. If $\mathrm{Gr}_m G \neq 0$, then $\varphi(m)$ is an integer.*

Proof. By replacing K by the completion $\widehat{K}_{\mathrm{ur}}$ of a maximal unramified extension and L by the composition field $\widehat{L}_{\mathrm{ur}} = L\widehat{K}_{\mathrm{ur}}$, we may assume that F is algebraically closed. Then the assertion follows from Corollary 4 and Proposition 3 (1)⇒(5). □

References

[1] Jean-Pierre Serre, Corps locaux, Hermann, Paris.