Math. Nachrichten vol. 174 (1995), 81–87

HASSE–ARF PROPERTY AND ABELIAN EXTENSIONS

Ivan B. Fesenko

Let F be a complete (or Henselian) discrete valuation field with a perfect residue field of characteristic $p > 0$. For a finite Galois extension L/F let $h_{L/F}$ denote the Hasse-Herbrand function (it coincides with the inverse function to the function $\varphi_{L/F}$ in the ramification theory), see section 3 in Chapter III of [FV] or (3.2) of [F1].

The extension L/F is said *to satisfy Hasse–Arf property (HAP)*, if

$$\{v_L(\pi_L^{-1}\sigma\pi_L - 1) : \sigma \in \mathrm{Gal}(L/F)\} \subset h_{L/F}(\mathbb{N})$$

where π_L is a prime element in L and v_L is the discrete valuation on L, $v_L(\pi_L) = 1$.

Let $\overline{F}$ be the residue field of F and $\kappa = \dim_{\mathbb{F}_p} \overline{F}/\wp(\overline{F})$ where $\wp(X)$ is the polynomial $X^p - X$. Further we will assume that $\kappa \neq 0$ and apply local p-class field theory developed in [F2], the case $\kappa = 0$ when the field $\overline{F}$ is algebraically p-closed may be treated using the Serre geometric class field theory [S].

Let U_F be the group of units of the ring of integers of F and $U_{i,F}$ be the groups of higher principal units. The following assertion for totally ramified p-extensions is very well-known. We show how it easily follows from class field theory.

Theorem (Hasse–Arf). *Let L/F be a totally ramified abelian p-extension. Then L/F satisfies HAP.*

Proof. Let $\mathrm{Gal}(L/F)^*$ be the group of $\mathbb{Z}_p$-continuous homomorphisms from the Galois group of the maximal unramified abelian p-extension $\widetilde{F}/F$ to the discrete $\mathbb{Z}_p$-module $\mathrm{Gal}(L/F)$. Put as usually

$$\mathrm{Gal}(L/F)_i = \{\sigma \in \mathrm{Gal}(L/F) : \pi_L^{-1}\sigma\pi_L \in U_{i,L}\}.$$

The construction of the reciprocity map

$$\Psi_{L/F}\colon U_{1,F}/N_{L/F}U_{1,L} \to \mathrm{Gal}(L/F)^*$$

and the inverse isomorphism

$$\Upsilon_{L/F}\colon \mathrm{Gal}(L/F)^* \to U_{1,F}/N_{L/F}U_{1,L}$$

in section 1 of [F2] shows that $\Psi_{L/F}$ transforms $U_{i,L}N_{L/F}U_{1,L} - U_{i+1,L}N_{L/F}U_{1,L}$ onto $(\mathrm{Gal}(L/F)_{h_{L/F}(i)})^* - (\mathrm{Gal}(L/F)_{h_{L/F}(i)+1})^*$. Thus, each non-trivial automorphism $\sigma \in \mathrm{Gal}(L/F)$ belongs exactly to $\mathrm{Gal}(L/F)_{h_{L/F}(i)}$ for some integer i. $\square$

One can construct examples of non-abelian extensions (even totally ramified of degree a power of p) which satisfy HAP. Moreover, for every totally ramified non-abelian p-extension L/F (of degree a power of p) there exists a totally ramified p-extension E/F linearly disjoint with L/F and such that LE/E satisfies HAP, see Maus [M, Satz (3.7)]. Nevertheless, the following theorem provides a characterization of abelian totally ramified p-extensions in terms of HAP (the general case of totally ramified extensions see below in Remark 1).

Theorem. *Let L/F be a finite totally ramified Galois p-extension. Let M/F be the maximal abelian subextension in L/F. The following conditions are equivalent:*

(1) *L/F is abelian;*
(2) *for every totally ramified abelian p-extension E/F the extension LE/F satisfies HAP;*
(3) *for every totally ramified abelian p-extension E/F of M/F the extension LE/F satisfies HAP.*

Before starting the proof of the theorem we need to establish several auxiliary assertions. Every so often, we apply the description of the norm map on higher principal units (see (1.3) of [F2] or (3.1) of [F1]) and the properties of the Hasse-Herbrand function (see (3.2) of [F1] or section 3 in Chapter III of [FV]).

Lemma 1. *Let M/F be a totally ramified Galois p-extension. Let π_M be a prime element of M. Let an element $\alpha \in M^*$ be such that $v_M(\alpha-1) = r = h_{M/F}(r_0)$, $r_0 \in \mathbb{N}$ and $N_{M/F}(\alpha) \in U_{r_0+1,F}$. Then there is $\tau \in \mathrm{Gal}(M/F)$ such that $\alpha\pi_M\tau(\pi_M^{-1})$ belongs to $U_{r+1,M}$.*

Proof. This is Theorem (4.2) of section 4 in [FV]. For the sake of completeness we indicate the arguments.

One may proceed by induction on the degree of M/F.

If M/F is of degree p, then the conditions of the lemma imply first of all that $\alpha = \gamma^{-1}\sigma(\gamma)$ for some $\gamma \in M^*$ and a generator σ of $\mathrm{Gal}(M/F)$. Then the commutative diagrams of section (3.1) of [F1] show that $r = v_M(\pi_M^{-1}\sigma\pi_M - 1)$ and $\alpha\pi_M\sigma^i(\pi_M^{-1}) \in U_{r+1,M}$ for a suitable $0 < i < p$.

Let M_1/F be a Galois subextension in M/F such that M/M_1 is of degree p. If $\beta = N_{M/M_1}\alpha$ belongs to $U_{r_1+1,F}$ for $r_1 = h^{-1}_{M/M_1}(r)$, then $r_1 = r$ and α can be written in the required form. If $\beta \notin U_{r_1+1,F}$, then β satisfies the conditions of the lemma for the extension M_1/F, therefore $\beta\pi_{M_1}\tau_1(\pi_{M_1}^{-1})$ belongs to U_{r_1+1,M_1} for $\pi_{M_1} = N_{M/M_1}\pi_M$ and a suitable $\tau_1 \in \mathrm{Gal}(M_1/F)$. According to the Herbrand Theorem there is an automorphism $\tau \in \mathrm{Gal}(M/F)$ such that $\tau\big|_{M_1} = \tau_1$ and $\pi_M\tau(\pi_M^{-1}) \in U_{r,M}$. Then $N_{M/M_1}(\alpha\pi_M\tau(\pi_M^{-1})) \in U_{r_1+1,M_1}$ and $\alpha\pi_M\tau(\pi_M^{-1})$ can be written either as an element of $U_{r+1,M}$ or as $(\pi_M^{-1}\sigma\pi_M)\varepsilon$ with $\varepsilon \in U_{r+1,M}$ for a suitable $\sigma \in \mathrm{Gal}(M/M_1)$ and in this case $\alpha\pi_M\sigma\tau(\pi_M^{-1})$ belongs to $U_{r+1,M}$. $\square$

Lemma 2. *Let L/F be a totally ramified Galois p-extension, and $M = L \cap F^{\mathrm{ab}} \neq L$. Then there exists $\alpha \in U_{1,M}$ such that $N_{M/F}\alpha = 1$ and $\alpha \notin N_{L/M}U_{1,L}$.*

Proof. According to p-class field theory $N_{L/F}U_{1,L} = N_{M/F}U_{1,M}$ and $N_{L/M}U_{1,L} \neq U_{1,M}$. Let $\beta \in U_{1,M}, \beta \notin N_{L/M}U_{1,L}$. Then $N_{M/F}\beta = N_{L/F}\gamma$ for some $\gamma \in U_{1,L}$ and $\alpha = \beta N_{L/M}\gamma^{-1}$ is the required element. $\square$

Proof of Theorem. The Hasse–Arf Theorem means that (1) implies (2) and (3). We will verify that (3) implies (1). Assume that L/F is non-abelian and (3) holds. Our aim is to obtain a contradiction.

Put $M = L\cap F^{\mathrm{ab}}$. It is sufficient to verify the required assertion for the case L/M is of degree p. Indeed, let M_1/F be a Galois subextension in L/F such that M_1/M is of degree p. If there is a $\tau \in \mathrm{Gal}(M_1E/F)$ such that $v_{M_1E}(\pi_{M_1E}^{-1}\tau\pi_{M_1E} - 1) \notin h_{M_1E/F}(\mathbb{N})$, then by the Herbrand Theorem there is a $\sigma \in \mathrm{Gal}(ME/F)$ such that $v_{ME}(\pi_{ME}^{-1}\sigma\pi_{ME} - 1) \notin h_{ME/F}(\mathbb{N})$.

Thus, we may assume that L/M is of degree p. Assume that $U_{s,M} \not\subset N_{L/M}U_{1,L}$, $U_{s+1,M} \subset N_{L/M}U_{1,L}$. Let π_L be a prime element in L. For arriving at a contradiction, it suffices to find a normic subgroup $\mathcal{N}$ in $U_{1,L}$ (see section 3 of [F2], for simplicity one can treat the case of a finite residue field, then the word "normic" can be replaced by "open") with the following properties: $U_{1,L}/\mathcal{N} \simeq \oplus_\kappa G$ for a finite abelian p-group G, $\ker N_{L/F} \subset \mathcal{N}$, $U_{t,L} \not\subset \mathcal{N}U_{t+1,L}$ for some $t < s$ such that $t \notin h_{L/F}(\mathbb{N})$. Indeed, let, according to the Existence Theorem in local p-class field theory, $\mathcal{N} = N_{T/L}U_{1,T}$, $\pi_L \in N_{T/L}T^*$ for a totally ramified abelian p-extension T/L. Then the sequence

$$1 \longrightarrow U_{1,L}/N_{T/L}U_{1,T} \xrightarrow{N^*_{L/F}} U_{1,F}/N_{T/F}U_{1,T} \longrightarrow U_{1,F}/N_{L/F}U_{1,L} \longrightarrow 1$$

is exact, where $N^*_{L/F}$ is induced by the norm map $N_{L/F}$. As $\alpha^{\tau-1} \in \mathcal{N}$ for each $\alpha \in L^*$, $\tau \in \mathrm{Gal}(L/F)$, the same theorem shows that T/F is a Galois extension. Now $U_{1,F}/N_{T/F}U_{1,T} \simeq \oplus_\kappa G'$ for an abelian p-group G' of order equal to $|T : F|p^{-1}$. This means that $|T : E| = p$ for the maximal abelian subextension E/F in T/F. The conditions on $\mathcal{N}$ imply that there exists a $\tau \in \mathrm{Gal}(T/L)$ such that $v_T(\pi_T^{-1}\tau\pi_T - 1) = h_{T/L}(t)$ for a prime element π_T in T. Then LE/F doesn't satisfy HAP.

Now we construct the desired group $\mathcal{N}$. By Lemma 2 there exists

$$t = \max(v_M(\alpha - 1) : N_{M/F}\alpha = 1, \alpha \notin N_{L/M}U_{1,L}).$$

Since $\pi_M^{-1}\tau\pi_M \in N_{L/M}U_{1,L}$ for a prime element π_M in M and $\tau \in \mathrm{Gal}(M/F)$, Lemma 1 implies $t \notin h_{L/F}(\mathbb{N}), t < s$. If it were $U_{t,L} \subset U_{t+1,L}\ker N_{L/F}$, then we would get $U_{t,M} \subset U_{t+1,M}N_{L/M}(\ker N_{L/F})$ that contradicts the choice of t.

Therefore, there is a natural c such that $U_{t,L} \subset U_{t+1,L} \ker N_{L/F} U_{1,L}^{p^{c-1}}$, $U_{t,L} \not\subset U_{t+1,L} \ker N_{L/F} U_{1,L}^{p^c}$. Now one can take for the desired $\mathcal{N}$ every normic subgroup $\mathcal{N}$ in $U_{1,L}$ such that $\ker N_{L/F} U_{1,L}^{p^c} \subset \mathcal{N}, U_{t,L} \not\subset \mathcal{N} U_{t+1,L}$. $\square$

Remark 1. Let L/F be a finite totally ramified Galois extension, and M/F its maximal tamely ramified subextension. The extension M/F is a cyclic extension of degree prime to p. One can verify that L/F is abelian if and only if L/M is abelian and L/F satisfies HAP. Indeed, if L/F satisfies HAP and L/M is abelian, then all breaks in the upper numbering of the ramification subgroups of $\mathrm{Gal}(L/M)$ are divisible by $|M:F|$ and each $\alpha \in U_{1,M}$ can be written as $\prod (1+\theta_i \pi_F^{s_i}) \mod N_{L/M} U_{1,L}$ with $\theta_i \in U_F$ and a prime element π_F of F. Hence $\alpha^{\tau-1} \in N_{L/M} U_{1,L}$ for a $\tau \in \mathrm{Gal}(M/F)$. Furthermore, the extension L/F is abelian by the second commutative diagram in Proposition (1.8) of [F2]. Now it follows from the above-listed proof of the theorem that its assertions remain true if the words "p-extension" are replaced by "extension". Note that in the general case of a finite Galois extension with non-trivial unramified part there is no similar characterization of abelian extensions in terms of HAP.

Remark 2. Let notations be the same as in the proof of the theorem, and $|M:F| = p^n$. Elementary calculations demonstrate that $h_{L/F}^{-1}(s) \leqslant (n+p/(p-1))e_F$ if $\mathrm{char}(F) = 0$, where e_F is the absolute ramification index of F. Then in terms of the proof

$$c \leqslant 1 + n + \max_{1 \leqslant m \leqslant pe_F/(p-1)} v_{\mathbb{Q}_p}(m).$$

Thus, in the case of $\mathrm{char}(F) = 0$ for every extension E/M as in (3) of the theorem of sufficiently large degree the extension LE/F doesn't satisfy HAP.

On the other hand, using the proof of the theorem one can construct examples of totally ramified non-abelian p-extensions satisfying HAP. Let M/F be a totally ramified non-cyclic extension of degree p^2 with

$$s_2 = \max(v_M(\pi_M^{-1}\sigma\pi_M - 1) : \sigma \in \mathrm{Gal}(M/F), \sigma \neq 1) = v_M(\pi_M^{-1}\sigma\pi_M - 1),$$
$$s_1 = \max(v_M(\pi_M^{-1}\tau\pi_M - 1) < s_2 : \tau \in \mathrm{Gal}(M/F)) = v_M(\pi_M^{-1}\tau\pi_M - 1).$$

Let M_1 be the fixed field of σ. Assume that $s' = s_2 + p(s_1+1) \in h_{M/F}(\mathbb{N})$. Put $r = s_2 + p^{-1}(s' - s_2)$, then $r - s_1 - 1 = s_2$. There exists an element $\varepsilon \in U_{r-s_1-1,M_1}$ with the properties: $\varepsilon \notin N_{M/M_1} U_{1,M}, \varepsilon^{\tau-1} = N_{M/M_1}\beta, \beta \in U_{s'-p,M}$. If there are no non-trivial pth roots of unity in F, then β doesn't belong to the group $U_{1,M}^p A$, where A is the subgroup of elements of the form $\gamma^{\sigma-1}\delta^{\tau-1}$. Among normic subgroups $\mathcal{N}$ in $U_{1,M}$ satisfying the following properties:
$AU_{1,M}^p \subset \mathcal{N}$, $\beta \notin \mathcal{N}$, $U_{1,M}/\mathcal{N} \simeq \oplus_\kappa \mathbb{F}_p$, $U_{s+1,M} \subset \mathcal{N}$,
choose one with minimal s. Then, since $U_{j,M}A = U_{j+1,M}A$ for $s' - p < j \notin h_{M/F}(\mathbb{N})$, the choice of β implies that $s' \leqslant s \in h_{M/F}(\mathbb{N})$. Now, according to p-class field theory, the group $\mathcal{N}$ is the norm group of the extension L/M such that L/F

is a Galois extension of degree p^3. One can verify that $t = s' - p$ in terms of the proof of the theorem.

Now, if $s = h_{M/F}(q)$ and $U_{q,F} \subset U_{q+1,F} U_{1,F}^{p^{a+1}}$, then there exists an element $\gamma \in U_{s,M}, \gamma \notin N_{L/M} U_{1,L}$ such that $N_{M/F}\gamma = N_{L/F}\delta^{p^a}$ for some $\delta \in U_{1,L}$. Provided the residue field of F is of order p this implies that $U_{j,L} \subset U_{j+1,L} \ker N_{L/F}$ for $j \notin h_{L/F}(\mathbb{N}), j < s, j \neq t$ and $U_{t,L} \subset U_{t+1,L} \ker N_{L/F} U_{1,L}^{p^a}$. Therefore, in this case for every totally ramified abelian p-extension E/F with $M \subset E, |E : M| \leqslant p^a$, the extension LE/F satisfies HAP.

Now let L/F be a finite totally ramified Galois p-extension. Put $\widetilde{L} = L\widetilde{F}$ and let $V(L|F)$ be the subgroup in $U_{1,\widetilde{L}}$ generated by $\varepsilon^{\sigma-1}$ where $\varepsilon \in U_{1,\widetilde{L}}, \sigma \in \mathrm{Gal}(\widetilde{L}/\widetilde{F})$. There is a homomorphism $i\colon \mathrm{Gal}(L/F) \to U_{1,\widetilde{L}}/V(L|F)$ defined by the formula $i(\sigma) = \pi^{-1}\sigma\pi \mod V(L|F)$ where π is a fixed prime element in $\widetilde{L}$ (i doesn't depend on the choice of π). The kernel of i coincides with the commutator subgroup of $\mathrm{Gal}(L/F)$, see, for instance, (1.4) of [F2]. A connection of the Hasse–Arf property and the extension to be abelian is contained in the following assertion.

Proposition. *The following two conditions are equivalent:*

(1) *L/F is abelian;*
(2) *L/F satisfies HAP, and if $\varepsilon \in V(L|F)$, then $v_{\widetilde{L}}(\varepsilon - 1) \notin h_{L/F}(\mathbb{N})$.*

Proof. If HAP holds, then for $\sigma \neq 1$ we get $i(\sigma) \in (U_{r,\widetilde{L}} - U_{r+1,\widetilde{L}})V(L|F)$ for some $r \in h_{L/F}(\mathbb{N})$ and the second condition of (2) means L/F is abelian.

In order to show that the first condition implies the second one, we may proceed by induction on the degree of L/F. If L/F is of degree p, then this follows immediately. In the general case let M/F be a subextension in L/F such that L/M is of degree p. Let an integer s be determined by the conditions $U_{s,M} \not\subset N_{L/M}U_{1,L}$, $U_{s+1,M} \subset N_{L/M}U_{1,L}$. Let α be an element of $V(L|F)$ and $v_{\widetilde{L}}(\alpha - 1) = r = h_{L/F}(q)$, for some $q \in \mathbb{N}$. Then by the induction assumption $N_{\widetilde{L}/\widetilde{M}}\alpha \in U_{h_{M/F}(q)+1,\widetilde{M}}$, since $N_{\widetilde{L}/\widetilde{M}}V(L|F) = V(M|F)$. In this case Lemma 1 implies $r = s$ and $\alpha = \pi_L^{\tau-1}\varepsilon$ for a prime element π_L in L, a generator τ of $\mathrm{Gal}(L/M)$, and some $\varepsilon \in U_{s+1,\widetilde{M}}$. We will show that this is impossible and thus complete the proof.

Let $\alpha_1 \in V(L|F)$, $\varepsilon_1 \in U_{s+1,\widetilde{L}}$ be such that $\alpha = \alpha_1^{\varphi-1}$, $\varepsilon = \varepsilon_1^{\varphi-1}$ for an extension φ of an automorphism $\psi \neq 1$ in $\mathrm{Gal}(\widetilde{F}/F)$ (α_1 and ε_1 exist by Lemma in (1.4) of [F2]). Then $N_{\widetilde{L}/\widetilde{F}}(\alpha_1\varepsilon_1^{-1}) \in U_{q+1,F}$. One may assume without loss of generality that $s \geqslant \max\{v_L(\pi_L^{-1}\tau\pi_L - 1) : 1 \neq \tau \in \mathrm{Gal}(L/F)\}$. Then it follows from the description of the norm map in (3.1) of [F2] that $U_{q+1,F} \subset N_{L/F}U_{1,L}$ and $\beta = N_{\widetilde{L}/\widetilde{F}}(\alpha_1\varepsilon_1^{-1}) \in N_{L/F}U_{1,L}$. Now the construction of the reciprocity map $\Psi_{L/F}$ in section 1 of [F] implies that $\tau^{-1} = \Psi_{L/F}(\beta)(\varphi) = 1$, a contradiction. □

Remark. One can verify proceeding by induction on the degree of the extension L/F that $V(L|F)U_{r+1,\widetilde{L}} \cap U_{r,\widetilde{L}} = U_{r,\widetilde{L}}$ for each $r \notin h_{L/F}(\mathbb{N})$. In addition, $V(L|F)U_{r+1,\widetilde{L}} \cap U_{r,\widetilde{L}} = U_{r+1,\widetilde{L}}$ for all $r \in h_{L/F}(\mathbb{N})$ if the extension L/F is abelian.

Examples of non-abelian extensions satisfying HAP show that there exist totally ramified non-abelian p-extensions with

$$V(L|F)U_{r+1,\widetilde{L}} \cap U_{r,\widetilde{L}} \neq U_{r,\widetilde{L}} \quad \text{for } r \in h_{L/F}(\mathbb{N}).$$

References

[F1] Fesenko, I.B., *Local fields. Local class field theory. Higher local class field theory via algebraic K-theory*, Algebra i analiz **4, no.3** (1992), 1–41; English transl. in St. Petersburg Math. J. **4** (1993).

[F2] Fesenko, I., *Local class field theory: perfect residue field case*, Izvestija RAN. Ser. mat. **54, no.4** (1993), 72–91.

[FV] Fesenko, I. and Vostokov, S., *Local Fields and Their Extensions*, Amer. Math. Soc., Providence, R.I., 1993.

[M] Maus, E., *Existenz $\mathfrak{p}$-adischer Zahlkörper zu vorgegebenem verzweigungsverhalten*, Dissertation, Hamburg, 1965.

[S] J.-P. Serre, *Sur les corps locaux à corps résiduel algébriquement clos*, Bull. Soc. Math. France **89** (1961), 105–154.