Some Remarks on the Hasse-Arf Theorem

Arnaldo Garcia* and Henning Stichtenoth

Abstract: We give a very simple proof of Hasse-Arf theorem in the particular case where the extension is Galois with an elementary-abelian Galois group of exponent p. It just uses the transitivity of different exponents and Hilbert's different formula.

Let E/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(E/F)$. Let P be a place of F and let Q be a place of E lying above P. We assume that the corresponding valuations v_P (and hence also v_Q) are discrete valuations of rank 1, and that the residue field extension E_Q/F_P is separable. We want to study the sequence of ramification groups $G_i = G_i(Q|P)$, $i = 0, 1, 2, \ldots$. We have the inclusions

$$G \supseteq G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots .$$

Let p denote the characteristic of the residue field F_P. We will always assume that $p > 0$. It is well-known (see Serre [6]) that the order of G_0 is equal to the ramification index $e = e(Q|P)$, that G_1 is the unique p-Sylow subgroup of G_0 and that G_0/G_1 is cyclic of order prime to p. All groups G_i are normal subgroups of G_0, and for $i \geq 1$ the quotients G_i/G_{i+1} are elementary-abelian groups of exponent p.

For simplicity, we will assume from now on that $Q|P$ is totally ramified and that G is a p-group. Then we have

$$G = G_0 = G_1 \supseteq G_2 \supseteq G_3 \supseteq \ldots \tag{1}$$

and $G_m = \{1\}$ for m sufficiently large.

Definition. An integer $s \geq 1$ is called a *jump* of $Q|P$ if $G_s \supsetneq G_{s+1}$.

– 2000 Math. Subject Classification - 11S15, 11S20, 14H05 and 14H37.

* – A. Garcia was supported by CNPq-FAPERJ (PRONEX) and also by the grant from CNPq #307569/2006-3.

The Hasse-Arf theorem states

Theorem 1. *With notations as above, assume moreover that G is an abelian p-group. Let $s < t$ be two subsequent jumps of $Q|P$; i.e., we have*

$$G_s \supsetneqq G_{s+1} = \cdots = G_t \supsetneqq G_{t+1}.$$

Then it holds that

$$t \equiv s \mod (G : G_t).$$

Remark. Theorem 1 was firstly proved by Hasse for the case of finite residue fields (see [2] and [3]), and the general case is due to Arf [1]. A different proof of Theorem 1 was given by Serre [5]. See also [6], Chapter IV, §3 and [4], Chapter III, §8.

The aim of this note is to give a very simple group-theoretical proof of the Hasse-Arf theorem if the Galois group G is an elementary-abelian group of exponent p, see Theorem 2 below. Our method also yields some weaker results in the case of arbitrary (abelian or non-abelian) p-groups G, see Theorem 3 below. Other basic ingredients in the proofs below are the transitivity of different exponents and Hilbert's different formula.

Theorem 2. *With notations as above, assume moreover that G is an elementary-abelian group of exponent p. Let $s < t$ be subsequent jumps of $Q|P$. Then it holds that*

$$t \equiv s \mod (G : G_t).$$

Remark. The idea of the proof of Theorem 2 becomes very transparent if we consider the special case of an elementary-abelian group G of order p^2. Then for two subsequent jumps $s < t$ of $Q|P$ we must have

$$G = G_0 = G_1 = \cdots = G_s \supsetneqq G_{s+1} = \cdots = G_t \supsetneqq G_{t+1} = \{1\},$$

and $(G : G_t) = \text{ord } G_t = p$. The assertion of Theorem 2 in this special case is then:

$$t \equiv s \mod p. \tag{2}$$

In order to prove (2), we choose a subgroup $K \subseteq G$ such that $\text{ord}(K) = p$ and $K \cap G_t = \{1\}$. Note that such a subgroup K of G exists, since the Galois group G is not cyclic. Let E^K denote the fixed field of K and let Q_1 denote the restriction of Q to E^K. For all $i \geq 0$, the i-th ramification group of $Q|Q_1$ (denoted by $G_i(Q|Q_1)$) satisfies

$$G_i(Q|Q_1) = G_i(Q|P) \cap K = \begin{cases} K, & \text{for } i \leq s, \\ \{1\}, & \text{for } i \geq s+1. \end{cases}$$

This follows immediately from the definition of ramification groups. By Hilbert's different formula (cf. Serre [6], Chapter IV, §1), the different exponents for $Q|P$ and for $Q|Q_1$ are given by

$$d(Q|P) = \sum_{i=0}^{\infty} (\text{ord } G_i - 1) = (s+1)(p^2-1) + (t-s)(p-1),$$

and

$$d(Q|Q_1) = \sum_{i=0}^{\infty} (\text{ord } G_i(Q|Q_1) - 1) = (s+1)(p-1).$$

By the transitivity of different exponents, we also have

$$d(Q|P) = d(Q|Q_1) + p \cdot d(Q_1|P)$$

and hence $d(Q|P) \equiv d(Q|Q_1) \bmod p$. Therefore we obtain

$$(s+1)(p^2-1) + (t-s)(p-1) \equiv (s+1)(p-1) \mod p.$$

The congruence (2) now follows immediately. □

We are now going to prove Theorem 2. Hence the Galois group G is an arbitrary elementary-abelian group of exponent p. Let $s_1, s_2, \dots, s_m$ denote the ordered sequence of all jumps of $Q|P$. We also define $s_0 := 0$, so

$$0 = s_0 < s_1 < s_2 < \cdots < s_m$$

and $G_i = \{1\}$ for all $i > s_m$. We have to show that

$$s_n \equiv s_{n-1} \mod (G : G_{s_n}) \tag{3}$$

holds for all n with $1 \leq n \leq m$. We proceed by induction on n.

The case $n = 1$ is trivial since $G_{s_1} = G$. Assume now that $1 \leq n \leq m-1$ and that (3) holds for all j with $1 \leq j \leq n$; i.e., it holds that $s_j \equiv s_{j-1} \bmod (G : G_{s_j})$. We will show that (3) also holds for $n+1$. To simplify notation, we set $s := s_n$ and $t := s_{n+1}$ and we have to show that $t \equiv s \bmod (G : G_t)$. We have that

$$G = G_0 \supseteq \cdots \supseteq G_s \supsetneqq G_{s+1} = \cdots = G_t \supsetneqq G_{t+1} \supseteq \dots \tag{4}$$

Since the Galois group G is assumed to be elementary-abelian of exponent p, the factor group G/G_{t+1} is also elementary-abelian of exponent p. Then there exists a subgroup $K \subseteq G$ with the following properties

$$G_{t+1} \subseteq K \subseteq G\ ; \quad K \cap G_t = G_{t+1}\ ; \quad (K : G_{t+1}) = (G : G_t). \tag{5}$$

Let E^K denote the fixed field of K and let Q_1 denote the restriction of Q to E^K. The i-th ramification group of $Q|Q_1$ is then $K \cap G_i$, and Hilbert's different formula for the different exponents of $Q|P$ and of $Q|Q_1$ gives

$$\begin{aligned} d(Q|P) = \text{ord } G_0 - 1 &+ \sum_{j=1}^{n} (s_j - s_{j-1})(\text{ord } G_{s_j} - 1) \\ &+ (t-s)(\text{ord } G_t - 1) + \sum_{\ell > t} (\text{ord } G_\ell - 1), \end{aligned} \tag{6}$$

and

$$\begin{aligned} d(Q|Q_1) = \text{ord } K - 1 &+ \sum_{j=1}^{n} (s_j - s_{j-1})(\text{ord } K \cap G_{s_j} - 1) \\ &+ (t-s)(\text{ord } G_{t+1} - 1) + \sum_{\ell > t} (\text{ord } G_\ell - 1). \end{aligned} \tag{7}$$

Since $d(Q|P) = d(Q|Q_1) + \mathrm{ord}(K) \cdot d(Q_1|P)$, we obtain by subtracting Equations (6) and (7):

$$(s-t)(\mathrm{ord}\ G_t - \mathrm{ord}\ G_{t+1}) \equiv \sum_{j=1}^{n} (s_j - s_{j-1})(\mathrm{ord}\ G_{s_j} - \mathrm{ord}(K \cap G_{s_j})) \quad \mathrm{mod}(\mathrm{ord}\ K). \tag{8}$$

Now we use the induction hypothesis which implies that there exist integers $c_j \geq 1$ such that

$$s_j - s_{j-1} = c_j \cdot (G : G_{s_j}), \qquad \text{for } j = 1, 2, \ldots, n.$$

It follows that

$$\begin{aligned}(s_j - s_{j-1}) \cdot\ \mathrm{ord}\ G_{s_j} &= c_j \cdot (G : G_{s_j}) \cdot\ \mathrm{ord}\ G_{s_j} \\ &= c_j \cdot\ \mathrm{ord}\ G \quad \equiv 0 \quad \mathrm{mod}(\mathrm{ord}\ K)\end{aligned}$$

and

$$\begin{aligned}(s_j - s_{j-1}) \cdot\ \mathrm{ord}(K \cap G_{s_j}) &= c_j \cdot (G : G_{s_j}) \cdot\ \mathrm{ord}(K \cap G_{s_j}) \\ &= c_j \cdot (G : G_{s_j}) \cdot \frac{\mathrm{ord}\ K \cdot\ \mathrm{ord}\ G_{s_j}}{\mathrm{ord}(K \cdot G_{s_j})} \\ &= c_j \cdot \frac{\mathrm{ord}(G)}{\mathrm{ord}(K \cdot G_{s_j})} \cdot\ \mathrm{ord}\ K \quad \equiv 0 \quad \mathrm{mod}(\mathrm{ord}\ K).\end{aligned}$$

It now follows from Equation (8) above that

$$(t-s) \cdot\ \mathrm{ord}\ G_{t+1} \cdot ((G_t : G_{t+1}) - 1) \quad \equiv 0 \quad \mathrm{mod}(\mathrm{ord}\ K). \tag{9}$$

Since $(K : G_{t+1}) = (G : G_t)$ holds by (5), we have

$$\mathrm{ord}(K) = \mathrm{ord}\ G_{t+1} \cdot (G : G_t),$$

and we then conclude from (9) that

$$(t-s) \cdot ((G_t : G_{t+1}) - 1) \equiv 0 \quad \mathrm{mod}(G : G_t).$$

Since $(G_t : G_{t+1}) - 1$ is relatively prime to the characteristic p and $(G : G_t)$ is a power of p, we get

$$t - s \equiv 0 \quad \mathrm{mod}\ (G : G_t).$$

This finishes the proof of Theorem 2. □

We can apply the method of the proof of Theorem 2 to obtain a congruence condition for subsequent jumps, for arbitrary p-groups G. This congruence is slightly weaker than the one in the Hasse-Arf Theorem.

Theorem 3. *Let E/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(E/F)$. Suppose that $Q|P$ is totally ramified in E/F and that G is a p-group, where p is the characteristic of the residue field of the place P. Suppose that $s < t$ are subsequent jumps of $Q|P$ and assume one of the following two conditions:*

(i) $(G_t : G_{t+1}) \geq p^2$.

(ii) $(G_t : G_{t+1}) = p$ *and* G_s/G_{t+1} *contains at least two distinct subgroups of order* p.

Then it holds that

$$t \equiv s \mod p.$$

Proof: We first show that there exists a subgroup $K \subseteq G$ with the following properties:

$$G_{t+1} \subseteq K \subseteq G_s \ ; \quad G_t \cap K \subsetneqq G_t \ ; \quad G_t \cap K \subsetneqq K. \tag{10}$$

If condition (ii) holds, this is clear: one chooses $K \subseteq G_s$ such that $\mathrm{ord}(K/G_{t+1}) = p$ and $K/G_{t+1} \neq G_t/G_{t+1}$. If condition (i) holds, we take $a \in G_s \setminus G_t$ and we set $K := \langle G_{t+1}, a\rangle$. Since K/G_{t+1} is cyclic and G_t/G_{t+1} is elementary-abelian of order at least p^2, it follows that G_t is not contained in K and hence the subgroup K satisfies all conditions of (10).

Now we proceed as in the proof of Theorem 2: Let E^K be the fixed field of K and let Q_1 be the restriction of Q to E^K. We have

$$d(Q|P) = \sum_{i=0}^{s}(\mathrm{ord}\ G_i - 1) + (t-s)(\mathrm{ord}\ G_t - 1) + \sum_{i>t}(\mathrm{ord}\ G_i - 1),$$

and using (10), we have

$$d(Q|Q_1) = \sum_{i=0}^{s}(\mathrm{ord}\ K - 1) + (t-s)(\mathrm{ord}(K \cap G_t) - 1) + \sum_{i>t}(\mathrm{ord}\ G_i - 1).$$

Since $d(Q|P) = d(Q|Q_1) + \mathrm{ord}(K) \cdot d(Q_1|Q) \equiv d(Q|Q_1) \bmod(\mathrm{ord}\ K)$, we see that

$$(t-s)(\mathrm{ord}\ G_t - \mathrm{ord}(K \cap G_t)) \equiv 0 \mod(\mathrm{ord}\ K).$$

Observing that $K \cap G_t \subsetneqq K$ and $K \cap G_t \subsetneqq G_t$, we obtain that

$$t \equiv s \mod (K : K \cap G_t). \tag{11}$$

This finishes the proof of Theorem 3. □

Remark. Equation (11) can also be written as

$$t \equiv s \mod(K \cdot G_t : G_t).$$

The bigger is the order of the subgroup $K \cdot G_t$ of G_s, the finer is the information in the congruence relation above. We stress that the subgroup K is chosen satisfying Eq.(10). Assume that $(G_s : G_t) \geq p^2$ and we can ask the following question: Find general conditions on the factor group G_s/G_{t+1} implying that one can choose K satisfying Eq.(10) such that $K \cdot G_t = G_s$.

References

[1] C. Arf – *Untersuchungen über reinverzweigte Erweiterungen diskret bewerteter perfekter Körper*, J. Reine Angew. Math. **181** (1940), 1–44.

[2] H. Hasse – *Führer, Diskriminante und Verzweigunsgskörper relativ Abelscher Zahlkörper*, J. Reine Angew. Math. **162** (1930), 169–184.

[3] H. Hasse – *Normenresttheorie galoisscher Zahlkörper mit Anwendungen auf Führer und Diskriminante abelscher Zahlkörper*, J. Fac. Sci. Tokyo **2** (1934), 477–498.

[4] J. Neukirch – *Class Field Theory* – Grundlehren der Math. Wissenschaften **280**, Springer-Verlag, Berlin, 1986.

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

[6] J.-P. Serre – *Local Fields* – Graduate Texts in Math. **67**, Springer-Verlag, New York, 1979.

Arnaldo Garcia
IMPA
Estrada Dona Castorina 110
22460-320, Rio de Janeiro, Brazil
Email- garcia@impa.br

Henning Stichtenoth
Sabanci University
MDBF, Orhanli, 34956
Tuzla, Istanbul, Turkey
Email- henning@sabanciuniv.edu