Local Galois groups and decomposition groups

Peter Koymans
Max Planck Institute for Mathematics

Anabelian Geometry Seminar

06 November 2020

The goal for today

Our aim is to prove the following theorem. Write $\overline{k}$ for the separable closure of a field k, write G_k for the Galois group $\mathrm{Gal}(\overline{k}/k)$ and write $D_{\mathfrak{q}/\mathfrak{p}}$ for the decomposition group.

The goal for today

Our aim is to prove the following theorem. Write $\overline{k}$ for the separable closure of a field k, write G_k for the Galois group $\mathrm{Gal}(\overline{k}/k)$ and write $D_{\mathfrak{q}/\mathfrak{p}}$ for the decomposition group.

Theorem 1 (NSW 12.1.9)

Let k be a global field, κ a nonarchimedean local field, and assume that G_k has a closed subgroup $H \cong G_\kappa$. Then there exists a unique prime $\mathfrak{p}$ in k and a unique extension $\mathfrak{P}$ of $\mathfrak{p}$ to $\overline{k}$ such that $H \subseteq D_{\mathfrak{P}/\mathfrak{p}}$.

Algebraic number theory background

We will use the following two results from algebraic number theory.

Lemma 2 (Weak approximation)

Let K be a global field and let $|\cdot|_1, \ldots, |\cdot|_N$ be inequivalent non-trivial absolute values. Then given $\epsilon > 0$ and elements $a_1, \ldots, a_N \in K$, there exists $b \in K$ such that

$$|a_i - b|_i < \epsilon \text{ for all } 1 \leq i \leq N.$$

Lemma 3 (NSW 12.1.1)

Let k be a field complete with respect to a rank 1 valuation. Let $f_1 = a_{0,1} + a_{1,1}X + \cdots + a_{d,1}X^d \in k[X]$ be a separable polynomial. Then there exists $\epsilon > 0$ such that for every polynomial $f_2 = a_{0,2} + a_{1,2}X + \cdots + a_{d,2}X^d \in k[X]$ with $|f_1 - f_2| < \epsilon$, we have $\mathrm{Spl}(f_1) = \mathrm{Spl}(f_2)$.

Proof.

This is a variant of Krasner's lemma. □

The key proposition

We say that a prime $\mathfrak{p}$ of K is indecomposable in L/K if there is exactly one prime $\mathfrak{P}$ of L above $\mathfrak{p}$.

The key proposition

We say that a prime $\mathfrak{p}$ of K is indecomposable in L/K if there is exactly one prime $\mathfrak{P}$ of L above $\mathfrak{p}$.

Proposition 1 (Key proposition)

Let k be a global field and let $K \subsetneq \overline{k}$. Then there exists at most one prime of K that is indecomposable in $\overline{k}$.

The key proposition

We say that a prime $\mathfrak{p}$ of K is indecomposable in L/K if there is exactly one prime $\mathfrak{P}$ of L above $\mathfrak{p}$.

Proposition 1 (Key proposition)

Let k be a global field and let $K \subsetneq \overline{k}$. Then there exists at most one prime of K that is indecomposable in $\overline{k}$.

Suppose that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are two indecomposable primes of K. Let $f_1, f_2 \in K[X]$ be two separable polynomials of the same degree d.

The key proposition

We say that a prime $\mathfrak{p}$ of K is indecomposable in L/K if there is exactly one prime $\mathfrak{P}$ of L above $\mathfrak{p}$.

Proposition 1 (Key proposition)

Let k be a global field and let $K \subsetneq \overline{k}$. Then there exists at most one prime of K that is indecomposable in $\overline{k}$.

Suppose that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are two indecomposable primes of K. Let $f_1, f_2 \in K[X]$ be two separable polynomials of the same degree d.

We claim that $\mathrm{Spl}(f_1) = \mathrm{Spl}(f_2)$. The claim implies $K = \overline{k}$ contrary to our assumptions, so it suffices to establish the claim.

Proof of key proposition

By weak approximation there exists for all $\epsilon > 0$ a polynomial $f \in K[X]$ such that

$$|f - f_1|_{\mathfrak{p}_1} < \epsilon \text{ and } |f - f_2|_{\mathfrak{p}_2} < \epsilon.$$

By taking ϵ sufficiently small in terms of f_1 and f_2, we deduce from Krasner's lemma that $\mathrm{Spl}(f_1) = \mathrm{Spl}(f)$ over $K_{\mathfrak{p}_1}$, and similarly for f_2.

Proof of key proposition

By weak approximation there exists for all $\epsilon > 0$ a polynomial $f \in K[X]$ such that

$$|f - f_1|_{\mathfrak{p}_1} < \epsilon \text{ and } |f - f_2|_{\mathfrak{p}_2} < \epsilon.$$

By taking ϵ sufficiently small in terms of f_1 and f_2, we deduce from Krasner's lemma that $\mathrm{Spl}(f_1) = \mathrm{Spl}(f)$ over $K_{\mathfrak{p}_1}$, and similarly for f_2.

Since $\mathfrak{p}_1$ is indecomposable, we see that

$$\mathrm{Gal}(K_{\mathfrak{p}_1}\mathrm{Spl}(f_1)\mathrm{Spl}(f)/K_{\mathfrak{p}_1}) \cong \mathrm{Gal}(\mathrm{Spl}(f_1)\mathrm{Spl}(f)/K).$$

Since $\mathrm{Spl}(f_1) = \mathrm{Spl}(f)$ over $K_{\mathfrak{p}_1}$, this implies $\mathrm{Spl}(f_1) = \mathrm{Spl}(f)$ over K.

Proof of key proposition

By weak approximation there exists for all $\epsilon > 0$ a polynomial $f \in K[X]$ such that

$$|f - f_1|_{\mathfrak{p}_1} < \epsilon \text{ and } |f - f_2|_{\mathfrak{p}_2} < \epsilon.$$

By taking ϵ sufficiently small in terms of f_1 and f_2, we deduce from Krasner's lemma that $\mathrm{Spl}(f_1) = \mathrm{Spl}(f)$ over $K_{\mathfrak{p}_1}$, and similarly for f_2.

Since $\mathfrak{p}_1$ is indecomposable, we see that

$$\mathrm{Gal}(K_{\mathfrak{p}_1}\mathrm{Spl}(f_1)\mathrm{Spl}(f)/K_{\mathfrak{p}_1}) \cong \mathrm{Gal}(\mathrm{Spl}(f_1)\mathrm{Spl}(f)/K).$$

Since $\mathrm{Spl}(f_1) = \mathrm{Spl}(f)$ over $K_{\mathfrak{p}_1}$, this implies $\mathrm{Spl}(f_1) = \mathrm{Spl}(f)$ over K.

Repeating this argument, we conclude that $\mathrm{Spl}(f_1) = \mathrm{Spl}(f_2)$ as claimed.

A corollary from the key proposition

We immediately deduce the following corollary.

Corollary 4 (NSW 12.1.3)

Let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be two distinct primes of the separable closure $\overline{k}$ of a global field k lying over $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Then $D_{\mathfrak{P}_1/\mathfrak{p}_1} \cap D_{\mathfrak{P}_2/\mathfrak{p}_2} = 1$.

A corollary from the key proposition

We immediately deduce the following corollary.

Corollary 4 (NSW 12.1.3)

Let $\mathfrak{P}_1$ *and* $\mathfrak{P}_2$ *be two distinct primes of the separable closure* $\overline{k}$ *of a global field* k *lying over* $\mathfrak{p}_1$ *and* $\mathfrak{p}_2$*. Then* $D_{\mathfrak{P}_1/\mathfrak{p}_1} \cap D_{\mathfrak{P}_2/\mathfrak{p}_2} = 1$*.*

Proof.

Use the Proposition and the fact that decomposition groups are closed subgroups of G_k. □

This immediately establishes the uniqueness part of the main theorem.

A corollary from the key proposition

We immediately deduce the following corollary.

Corollary 4 (NSW 12.1.3)

Let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be two distinct primes of the separable closure $\overline{k}$ of a global field k lying over $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Then $D_{\mathfrak{P}_1/\mathfrak{p}_1} \cap D_{\mathfrak{P}_2/\mathfrak{p}_2} = 1$.

Proof.

Use the Proposition and the fact that decomposition groups are closed subgroups of G_k. □

This immediately establishes the uniqueness part of the main theorem.

Before we can prove the rest of the main theorem, we need the following lemma that allows us to reduce to the case that k contains appropriate roots of unity.

A reduction step

Lemma 5 (NSW 12.1.10)

Let k be a global field, $\mathfrak{P}$ a prime of $\overline{k}$ lying above $\mathfrak{p}$ and H an infinite closed subgroup in G_k such that $[H : H \cap D_{\mathfrak{P}/\mathfrak{p}}] < \infty$. Then $H \subseteq D_{\mathfrak{P}/\mathfrak{p}}$.

A reduction step

Lemma 5 (NSW 12.1.10)

Let k be a global field, $\mathfrak{P}$ a prime of $\overline{k}$ lying above $\mathfrak{p}$ and H an infinite closed subgroup in G_k such that $[H : H \cap D_{\mathfrak{P}/\mathfrak{p}}] < \infty$. Then $H \subseteq D_{\mathfrak{P}/\mathfrak{p}}$.

Proof.

Take some open subgroup U of $H \cap D_{\mathfrak{P}/\mathfrak{p}}$ such that U is normal in H. Denote by K the fixed field of H and by L the fixed field of U. Then $[L : K] < \infty$ and $\mathfrak{P} \cap L$ is indecomposable in $\overline{k}/L$. Since L/K is Galois, all extensions of $\mathfrak{P} \cap K$ to L are indecomposable in $\overline{k}/L$.

A reduction step

Lemma 5 (NSW 12.1.10)

Let k be a global field, $\mathfrak{P}$ a prime of $\overline{k}$ lying above $\mathfrak{p}$ and H an infinite closed subgroup in G_k such that $[H : H \cap D_{\mathfrak{P}/\mathfrak{p}}] < \infty$. Then $H \subseteq D_{\mathfrak{P}/\mathfrak{p}}$.

Proof.

Take some open subgroup U of $H \cap D_{\mathfrak{P}/\mathfrak{p}}$ such that U is normal in H. Denote by K the fixed field of H and by L the fixed field of U. Then $[L : K] < \infty$ and $\mathfrak{P} \cap L$ is indecomposable in $\overline{k}/L$. Since L/K is Galois, all extensions of $\mathfrak{P} \cap K$ to L are indecomposable in $\overline{k}/L$.

Since H is infinite, we see that $L \neq \overline{k}$. Hence the key proposition shows that $\mathfrak{P} \cap L$ is the only extension of $\mathfrak{P} \cap K$, and $\mathfrak{P} \cap K$ is indecomposable in $\overline{k}/K$. Therefore $H \subseteq D_{\mathfrak{P}/\mathfrak{p}}$. □

A reduction step

Lemma 5 (NSW 12.1.10)

Let k be a global field, $\mathfrak{P}$ a prime of $\overline{k}$ lying above $\mathfrak{p}$ and H an infinite closed subgroup in G_k such that $[H : H \cap D_{\mathfrak{P}/\mathfrak{p}}] < \infty$. Then $H \subseteq D_{\mathfrak{P}/\mathfrak{p}}$.

Proof.

Take some open subgroup U of $H \cap D_{\mathfrak{P}/\mathfrak{p}}$ such that U is normal in H. Denote by K the fixed field of H and by L the fixed field of U. Then $[L : K] < \infty$ and $\mathfrak{P} \cap L$ is indecomposable in $\overline{k}/L$. Since L/K is Galois, all extensions of $\mathfrak{P} \cap K$ to L are indecomposable in $\overline{k}/L$.

Since H is infinite, we see that $L \neq \overline{k}$. Hence the key proposition shows that $\mathfrak{P} \cap L$ is the only extension of $\mathfrak{P} \cap K$, and $\mathfrak{P} \cap K$ is indecomposable in $\overline{k}/K$. Therefore $H \subseteq D_{\mathfrak{P}/\mathfrak{p}}$. □

By this lemma, it suffices to prove the main theorem in case μ_ℓ is contained in k and κ, where ℓ is a fixed odd prime.

Proof of main theorem

Recall that we aim to prove the following:

Theorem 6 (NSW 12.1.9)

Let k be a global field, κ a nonarchimedean local field, and assume that G_k has a closed subgroup $H \cong G_\kappa$. Then there exists a unique prime $\mathfrak{p}$ in k and a unique extension $\mathfrak{P}$ of $\mathfrak{p}$ to $\overline{k}$ such that $H \subseteq D_{\mathfrak{P}/\mathfrak{p}}$.

Proof of main theorem

Recall that we aim to prove the following:

Theorem 6 (NSW 12.1.9)

Let k be a global field, κ a nonarchimedean local field, and assume that G_k has a closed subgroup $H \cong G_\kappa$. Then there exists a unique prime $\mathfrak{p}$ in k and a unique extension $\mathfrak{P}$ of $\mathfrak{p}$ to $\overline{k}$ such that $H \subseteq D_{\mathfrak{P}/\mathfrak{p}}$.

We have already established uniqueness, and we have also reduced to the case that k and κ contain μ_ℓ for some fixed odd prime ℓ coprime with the characteristic of k.

Proof of main theorem

Recall that we aim to prove the following:

Theorem 6 (NSW 12.1.9)

Let k be a global field, κ a nonarchimedean local field, and assume that G_k has a closed subgroup $H \cong G_\kappa$. Then there exists a unique prime $\mathfrak{p}$ in k and a unique extension $\mathfrak{P}$ of $\mathfrak{p}$ to $\overline{k}$ such that $H \subseteq D_{\mathfrak{P}/\mathfrak{p}}$.

We have already established uniqueness, and we have also reduced to the case that k and κ contain μ_ℓ for some fixed odd prime ℓ coprime with the characteristic of k.

We need to understand the cohomology of local fields better.

Blackbox: cohomology of local fields

The following theorem gives us the needed machinery for the cohomology of local fields.

Theorem 7 (NSW 7.1.8)

Let k be a nonarchimedean local field. Let for now ℓ be a prime number coprime to $\mathrm{char}(k)$*. Then*

$$H^2(G_k, \mu_\ell) = \mathbb{Z}/\ell\mathbb{Z}.$$

Blackbox: cohomology of local fields

The following theorem gives us the needed machinery for the cohomology of local fields.

Theorem 7 (NSW 7.1.8)

Let k be a nonarchimedian local field. Let for now ℓ be a prime number coprime to $\mathrm{char}(k)$*. Then*

$$H^2(G_k, \mu_\ell) = \mathbb{Z}/\ell\mathbb{Z}.$$

Furthermore, for $k \subseteq L \subseteq \overline{k}$, we have

$$H^2(G_L, \mathbb{F}_\ell) = 0$$

if the degree $[L : k]$ is divisible by ℓ^∞ or if $\mathrm{char}(k) = \ell$*.*

Proof of main theorem: I

Set K to be the fixed field of H. Since $H \cong G_\kappa$ with κ a nonarchimedian local field, it follows from the cohomology of local fields that

$$H^2(U, \mu_\ell) \cong \mathbb{Z}/\ell\mathbb{Z}$$

for every open subgroup U of H.

Proof of main theorem: I

Set K to be the fixed field of H. Since $H \cong G_\kappa$ with κ a nonarchimedian local field, it follows from the cohomology of local fields that

$$H^2(U, \mu_\ell) \cong \mathbb{Z}/\ell\mathbb{Z}$$

for every open subgroup U of H.

Blackbox: from class field theory, we have for every global field k an injection

$$H^2(G_k, \mu_\ell) \to \bigoplus_{\mathfrak{p}} H^2(G_{k_\mathfrak{p}}, \mu_\ell).$$

Proof of main theorem: I

Set K to be the fixed field of H. Since $H \cong G_\kappa$ with κ a nonarchimedian local field, it follows from the cohomology of local fields that

$$H^2(U, \mu_\ell) \cong \mathbb{Z}/\ell\mathbb{Z}$$

for every open subgroup U of H.

Blackbox: from class field theory, we have for every global field k an injection

$$H^2(G_k, \mu_\ell) \to \bigoplus_{\mathfrak{p}} H^2(G_{k_\mathfrak{p}}, \mu_\ell).$$

Passing to the limit (blackbox NSW 1.5.1) we get an injection

$$H^2(G_K, \mu_\ell) \to \bigoplus_{\mathfrak{P}} H^2(G_{K_\mathfrak{P}}, \mu_\ell).$$

Since $H^2(G_K, \mu_\ell) \cong \mathbb{Z}/\ell\mathbb{Z}$, we see that there is a prime $\mathfrak{P}$ such that $H^2(G_{K_\mathfrak{P}}, \mu_\ell) \neq 0$. Since ℓ is odd, $\mathfrak{P}$ is nonarchimedian.

Proof of main theorem: II

We claim that $\mathfrak{P}$ is indecomposable in $\overline{k}/K$. Take an arbitrary finite separable extension L of K, which corresponds to an open subgroup U of H. Then recall that

$$H^2(G_L, \mu_\ell) \cong \mathbb{Z}/\ell\mathbb{Z}.$$

Proof of main theorem: II

We claim that $\mathfrak{P}$ is indecomposable in $\overline{k}/K$. Take an arbitrary finite separable extension L of K, which corresponds to an open subgroup U of H. Then recall that

$$H^2(G_L, \mu_\ell) \cong \mathbb{Z}/\ell\mathbb{Z}.$$

Blackbox: there is a surjection

$$\mathbb{Z}/\ell\mathbb{Z} \cong H^2(G_L, \mu_\ell) \to \bigoplus_{\mathfrak{P}' \text{ above } \mathfrak{P}} H^2(G_{L_{\mathfrak{P}'}}, \mu_\ell).$$

Proof of main theorem: II

We claim that $\mathfrak{P}$ is indecomposable in $\overline{k}/K$. Take an arbitrary finite separable extension L of K, which corresponds to an open subgroup U of H. Then recall that

$$H^2(G_L, \mu_\ell) \cong \mathbb{Z}/\ell\mathbb{Z}.$$

Blackbox: there is a surjection

$$\mathbb{Z}/\ell\mathbb{Z} \cong H^2(G_L, \mu_\ell) \to \bigoplus_{\mathfrak{P}' \text{ above } \mathfrak{P}} H^2(G_{L_{\mathfrak{P}'}}, \mu_\ell).$$

Recall that $\mathfrak{P}$ was chosen such that $H^2(G_{K_{\mathfrak{P}}}, \mu_\ell) \neq 0$. By the cohomology of local fields, then also $H^2(G_{L_{\mathfrak{P}'}}, \mu_\ell) \neq 0$.

Proof of main theorem: II

We claim that $\mathfrak{P}$ is indecomposable in $\overline{k}/K$. Take an arbitrary finite separable extension L of K, which corresponds to an open subgroup U of H. Then recall that

$$H^2(G_L, \mu_\ell) \cong \mathbb{Z}/\ell\mathbb{Z}.$$

Blackbox: there is a surjection

$$\mathbb{Z}/\ell\mathbb{Z} \cong H^2(G_L, \mu_\ell) \to \bigoplus_{\mathfrak{P}' \text{ above } \mathfrak{P}} H^2(G_{L_{\mathfrak{P}'}}, \mu_\ell).$$

Recall that $\mathfrak{P}$ was chosen such that $H^2(G_{K_{\mathfrak{P}}}, \mu_\ell) \neq 0$. By the cohomology of local fields, then also $H^2(G_{L_{\mathfrak{P}'}}, \mu_\ell) \neq 0$.

This implies that there can be at most one $\mathfrak{P}'$ above $\mathfrak{P}$. Since L was arbitrary, we conclude that $\mathfrak{P}$ is indecomposable in $\overline{k}/K$ and hence $H = G_{K_{\mathfrak{P}}}$.

Proof of main theorem: III

Denote by $\mathfrak{P}$ the unique extension of $\mathfrak{P}$ to K. Then we have the inclusion

$$H = G_{K_{\mathfrak{P}}} \subseteq D_{\mathfrak{P}/\mathfrak{p}},$$

where $\mathfrak{p}$ is the prime of k below $\mathfrak{P}$. This finishes the proof of the main theorem.

Theorem 8 (NSW 12.1.9)

Let k be a global field, κ a nonarchimedean local field, and assume that G_k has a closed subgroup $H \cong G_\kappa$. Then there exists a unique prime $\mathfrak{p}$ in k and a unique extension $\mathfrak{P}$ of $\mathfrak{p}$ to $\overline{k}$ such that $H \subseteq D_{\mathfrak{P}/\mathfrak{p}}$.

Proof of main theorem: III

Denote by $\mathfrak{P}$ the unique extension of $\mathfrak{P}$ to K. Then we have the inclusion

$$H = G_{K_{\mathfrak{P}}} \subseteq D_{\mathfrak{P}/\mathfrak{p}},$$

where $\mathfrak{p}$ is the prime of k below $\mathfrak{P}$. This finishes the proof of the main theorem.

Theorem 8 (NSW 12.1.9)

Let k be a global field, κ a nonarchimedean local field, and assume that G_k has a closed subgroup $H \cong G_\kappa$. Then there exists a unique prime $\mathfrak{p}$ in k and a unique extension $\mathfrak{P}$ of $\mathfrak{p}$ to $\overline{k}$ such that $H \subseteq D_{\mathfrak{P}/\mathfrak{p}}$.

Bonus part: furthermore, if κ is a finite extension of $\mathbb{Q}_p$, then k is a number field and $[D_{\mathfrak{P}/\mathfrak{p}} : H] < \infty$. Also $\mathfrak{p} \mid p$ and $[\kappa : \mathbb{Q}_p] \geq [k_{\mathfrak{p}} : \mathbb{Q}_p]$.

Proof of bonus part

If κ is a finite extension of $\mathbb{Q}_p$, then $H^2(G_\kappa, \mathbb{F}_\ell)$ is non-zero for all prime numbers ℓ. Hence k must be a number field.

Proof of bonus part

If κ is a finite extension of $\mathbb{Q}_p$, then $H^2(G_\kappa, \mathbb{F}_\ell)$ is non-zero for all prime numbers ℓ. Hence k must be a number field.

Furthermore, $D_{\mathfrak{P}/\mathfrak{p}} \supseteq H \cong G_\kappa$ contains closed subgroups which are pro-p-groups of rank greater than 2, so $\mathfrak{p} \mid p$.

Proof of bonus part

If κ is a finite extension of $\mathbb{Q}_p$, then $H^2(G_\kappa, \mathbb{F}_\ell)$ is non-zero for all prime numbers ℓ. Hence k must be a number field.

Furthermore, $D_{\mathfrak{P}/\mathfrak{p}} \supseteq H \cong G_\kappa$ contains closed subgroups which are pro-p-groups of rank greater than 2, so $\mathfrak{p} \mid p$.

To show that $[D_{\mathfrak{P}/\mathfrak{p}} : H] < \infty$, we may assume that κ contains μ_p. Then $G_{K_{\mathfrak{P}}} \cong G_\kappa$ implies that $p^\infty \nmid [D_{\mathfrak{P}/\mathfrak{p}} : H]$ by the cohomology of local fields.

Proof of bonus part

If κ is a finite extension of $\mathbb{Q}_p$, then $H^2(G_\kappa, \mathbb{F}_\ell)$ is non-zero for all prime numbers ℓ. Hence k must be a number field.

Furthermore, $D_{\mathfrak{P}/\mathfrak{p}} \supseteq H \cong G_\kappa$ contains closed subgroups which are pro-p-groups of rank greater than 2, so $\mathfrak{p} \mid p$.

To show that $[D_{\mathfrak{P}/\mathfrak{p}} : H] < \infty$, we may assume that κ contains μ_p. Then $G_{K_\mathfrak{P}} \cong G_\kappa$ implies that $p^\infty \nmid [D_{\mathfrak{P}/\mathfrak{p}} : H]$ by the cohomology of local fields.

For open subgroups V in $D_{\mathfrak{P}/\mathfrak{p}}$ containing H with $p \nmid [V : H]$, the restriction map $H^1(V, \mathbb{F}_p) \to H^1(H, \mathbb{F}_p)$ is injective.

Proof of bonus part

If κ is a finite extension of $\mathbb{Q}_p$, then $H^2(G_\kappa, \mathbb{F}_\ell)$ is non-zero for all prime numbers ℓ. Hence k must be a number field.

Furthermore, $D_{\mathfrak{P}/\mathfrak{p}} \supseteq H \cong G_\kappa$ contains closed subgroups which are pro-p-groups of rank greater than 2, so $\mathfrak{p} \mid p$.

To show that $[D_{\mathfrak{P}/\mathfrak{p}} : H] < \infty$, we may assume that κ contains μ_p. Then $G_{K_\mathfrak{P}} \cong G_\kappa$ implies that $p^\infty \nmid [D_{\mathfrak{P}/\mathfrak{p}} : H]$ by the cohomology of local fields.

For open subgroups V in $D_{\mathfrak{P}/\mathfrak{p}}$ containing H with $p \nmid [V : H]$, the restriction map $H^1(V, \mathbb{F}_p) \to H^1(H, \mathbb{F}_p)$ is injective.

But $H^1(H, \mathbb{F}_p)$ is finite, while $|H^1(V, \mathbb{F}_p)|$ becomes arbitrarily large as $[D_{\mathfrak{P}/\mathfrak{p}} : V]$ tends to infinity. Hence $[D_{\mathfrak{P}/\mathfrak{p}} : H] < \infty$. For the final part, look at the dimension of several $H^1(-,-)$ (blackbox: NSW 7.3.9).