Math. Res. Lett. **13** (2006), *no.* 2, 179–197

ON ČEBOTAREV SETS

Kay Wingberg

The aim of this paper is to define a topology with good properties on the set $\mathcal{P}_K$ of prime ideals of a number field K. The idea is, roughly speaking, that open sets are given by so-called Čebotarev sets, i.e. sets of the form

$$P_{L|K}(\sigma) = \{\mathfrak{p} \in \mathcal{P}_K \,|\, \mathfrak{p} \text{ is unramified in } L,\ \sigma = \Big(\frac{L|K}{\mathfrak{P}}\Big),\ \mathfrak{P}|\mathfrak{p}\},$$

where $L|K$ is a finite Galois extension with Galois group $G(L|K)$, $\sigma \in G(L|K)$ and $\left(\frac{L|K}{\mathfrak{P}}\right)$ denotes the Frobenius automorphism with respect to $\mathfrak{P}$, $\mathfrak{P}$ an arbitrary extension of $\mathfrak{p}$ to L. The precise definition of the topology $\mathcal{T}_K$ of $\mathcal{P}_K$ is slightly more complicated (see §2) since we want that the natural map

$$\varphi_{K'|K} : (\mathcal{P}_{K'}, \mathcal{T}_{K'}) \longrightarrow (\mathcal{P}_K, \mathcal{T}_K), \quad \mathfrak{P} \mapsto \mathfrak{P} \cap K,$$

is continuous if $K'|K$ is a finite extension. We will show that $(\mathcal{P}_K, \mathcal{T}_K)$ is a strongly zero-dimensional (and so totally disconnected) Hausdorff space with countable base, and so metrizable, hence normal and completely regular (and not discrete). In particular, every point of $(\mathcal{P}_K, \mathcal{T}_K)$ has a base of neighbourhoods consisting of both open and closed sets. Furthermore we will prove the following theorem (2.8)

Theorem: *Let K be a number field, then*

(a) *the isolated points of $(\mathcal{P}_K, \mathcal{T}_K)$ are prime ideals whose underlying prime numbers ramify in the extension $K|\mathbb{Q}$ (and so the set of isolated points is finite),*

(b) *every open neighbourhood of a prime ideal whose underlying prime number is completely decomposed in $K|\mathbb{Q}$ has positive density.*

In section 3 we consider uniform structures on $\mathcal{P}_K$ inducing the topology $\mathcal{T}_K$. If $\mathfrak{U}_K$ is the uniformity defined by finite partitions of $\mathcal{P}_K$ given by both open and closed sets, then the completion $(\hat{\mathcal{P}}_K, \hat{\mathfrak{U}}_K)$ of $(\mathcal{P}_K, \mathfrak{U}_K)$ is a profinite space, i.e. compact and totally disconnected. Finally we define in section 4 a metric on $\mathcal{P}_K$ (in the case $K = \mathbb{Q}$) inducing the topology $\mathcal{T}_K$.

The good properties of this topology are consequences of deep theorems in algebraic number theory. The Hausdorff property may illustrate this: it follows easily by considering certain number fields with suitable local behaviour. But the existence of these fields is a consequence of the theorem of Grunwald/Wang.

Received by the editors August 24, 2005.

1. Čebotarev Sets

Let K be a number field and let $\mathcal{P}_K$ be the set of all prime ideals $\mathfrak{p} \neq (0)$ of K. For a finite Galois extension $L|K$ with Galois group $G(L|K)$ we denote by

$U(L|K)$ the set of prime ideals of K which are unramified in L,
$D(L|K)$ the set of prime ideals of K which are completely decomposed in L,
$R(L|K)$ the set of prime ideals of K ramifying in L.

For an element $\sigma \in G(L|K)$ let

$$P_{L|K}(\sigma) = \{\mathfrak{p} \in U(L|K) \,|\, \sigma = \Big(\frac{L|K}{\mathfrak{P}}\Big) \text{ for a prime ideal } \mathfrak{P}|\mathfrak{p} \text{ of } L\},$$

where $\left(\frac{L|K}{\mathfrak{P}}\right)$ denotes the Frobenius automorphism with respect to $\mathfrak{P}$. Obviously, this set depends only on the conjugacy class $\langle\langle\sigma\rangle\rangle = \{\tau\sigma\tau^{-1} \,|\, \tau \in G(L|K)\}$ of σ. We have $P_{L|K}(\sigma) \cap P_{L|K}(\tau) = \varnothing$ if $\langle\langle\sigma\rangle\rangle \neq \langle\langle\tau\rangle\rangle$ and $P_{L|K}(1) = D(L|K)$. If $\delta(S) = \delta_K(S)$ denotes the Dirichlet density of a set S of primes of K, then by Čebotarev's density theorem

$$\delta(P_{L|K}(\sigma)) = \frac{\#\langle\langle\sigma\rangle\rangle}{\#G(L|K)}\,.$$

Observe that for a finite Galois extension $L|K$ and a set $S(K)$ of primes of K we have

$$\delta_L(S(L)) = \delta_K(S(K) \cap D(L|K))) \cdot [L:K],$$

where $S(L)$ denotes the set of all extensions of $S(K)$ to L. For sets S_1 and S_2 of primes we use the notation

$$S_1 \subsetneq S_2 :\Longleftrightarrow \delta(S_1 \backslash S_2) = 0,$$

i.e. S_1 is contained in S_2 up to a set of primes of density zero, and

$$S_1 \eqsim S_2 :\Longleftrightarrow S_1 \subsetneq S_2 \text{ and } S_2 \subsetneq S_1.$$

Definition 1.1. *A set S of prime ideals of K is called* **Čebotarev set** *if there exist a finite Galois extension L of K and an element $\sigma \in G(L|K)$ such that*

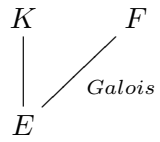
$$S = P_{L|K}(\sigma).$$

We set $\mathcal{C}_K = \{S \subseteq \mathcal{P}_K \text{ is a Čebotarev set}\}$.

For a finite extension $K'|K$ let

$$\varphi_{K'|K} : \mathcal{P}_{K'} \longrightarrow \mathcal{P}_K, \quad \mathfrak{P} \mapsto \mathfrak{p} = \mathfrak{P} \cap K,$$

and we also denote the corresponding map on the set of all subsets of $\mathcal{P}_{K'}$ by $\varphi_{K'|K}$. For a subfield $E \subseteq K$, a finite Galois extension $F|E$



and $\sigma \in G(F|E)$, let $U^K(F|E) = \varphi_{K|E}^{-1} U(F|E)$, $R^K(F|E) = \varphi_{K|E}^{-1} R(F|E)$ and

$$P_{F|E}^K(\sigma) = \varphi_{K|E}^{-1} P_{F|E}(\sigma).$$

In the next section we will consider the topology $\mathcal{T}_K$ on $\mathcal{P}_K$ defined by the subbase which consists of all sets of the form $P_{F|E}^K(\sigma)$. But first we have to prove some properties of the Čebotarev sets.

Proposition 1.2. *Let $N|K$ and $L|K$ be finite Galois extensions with $L \subseteq N$, and let $H = G(N|L)$ and $\bar{\sigma} \in G(L|K)$. Then*

$$U(N|K) \cap P_{L|K}(\bar{\sigma}) = \bigcup_{\langle\langle\tau\rangle\rangle \cap \sigma H \neq \varnothing}^{\cdot} P_{N|K}(\tau)\,,$$

where σ is a lifting of $\bar{\sigma}$ to $G(N|K)$; in particular

$$U(N|K) \cap D(L|K) = \bigcup_{\langle\langle\tau\rangle\rangle \cap H \neq \varnothing}^{\cdot} P_{N|K}(\tau)\,.$$

Proof: Let $\mathfrak{p}$ be a prime ideal of K which is unramified in $N|K$. Then $\mathfrak{p} \in P_{L|K}(\bar{\sigma})$ if and only if there exists a prime $\overline{\mathfrak{P}}|\mathfrak{p}$ of L such that $\bar{\sigma} = \left(\frac{L|K}{\overline{\mathfrak{P}}}\right)$, i.e. if there exists a prime $\mathfrak{P}|\mathfrak{p}$ of N such that $\sigma H = \left(\frac{N|K}{\mathfrak{P}}\right) H$. This is equivalent to the assertion that there exists an element in σH which is contained in the conjugacy class $\langle\langle\tau\rangle\rangle$ of $\tau = \left(\frac{N|K}{\mathfrak{P}}\right)$ for some prime ideal $\mathfrak{P}|\mathfrak{p}$ of N, i.e. if $\mathfrak{p} \in P_{N|K}(\tau)$ for some $\tau \in G(N|K)$ with $\langle\langle\tau\rangle\rangle \cap \sigma H \neq \varnothing$. □

Since $U(L_1|K) \cap U(L_2|K) = U(L_1L_2|K)$, we obtain

Corollary 1.3. *Let $L_1|K$ and $L_2|K$ be finite Galois extensions, H_i=$G(L_1L_2|L_i)$ and $\bar{\sigma}_i \in G(L_i|K)$, $i = 1, 2$. Then*

(i) $$P_{L_1|K}(\bar{\sigma}_1) \cap P_{L_2|K}(\bar{\sigma}_2) = \bigcup_{\substack{\langle\langle\tau\rangle\rangle \cap \sigma_1 H_1 \neq \varnothing \\ \langle\langle\tau\rangle\rangle \cap \sigma_2 H_2 \neq \varnothing}}^{\cdot} P_{L_1L_2|K}(\tau)\,,$$

(ii) $P_{L_1|K}(\bar\sigma_1) \cap P_{L_2|K}(\bar\sigma_2) \neq \varnothing$ *if and only if* $(\sigma_1)^{-1}(\sigma_2)^\rho \in G(L_1L_2|L_1 \cap L_2)$ *for some* $\rho \in G(L_1L_2|K)$ (*here* σ_i *is an arbitrary lifting of* $\bar\sigma_i$ *to* $G(L_1L_2|K)$).

If $\bar\sigma_1 = 1 = \bar\sigma_2$, then the corollary above is just the assertion $D(L_1L_2|K) = D(L_1|K) \cap D(L_2|K)$. From part (ii) of the proposition above it follows that all sets $P_{L_1|K}(\bar\sigma_1)$ and $P_{L_2|K}(\bar\sigma_2)$ have a non-trivial intersection, if L_1 and L_2 are linearly disjoint over K. For an element τ of a finite group G we denote the stabilizer of τ under conjugation by $\mathrm{St}_G(\tau)$.

Proposition 1.4. *Let* L_1 *and* L_2 *be finite Galois extensions of* K. *For an element* $\sigma_i \in G(L_i|K)$ *we denote its restriction to* $L_1 \cap L_2$ *by* $\overline{\sigma_i}$, $i = 1, 2$. *Then the following assertions are equivalent:*

(i) $P_{L_1|K}(\sigma_1) \subsetneq P_{L_2|K}(\sigma_2)$,

(ii) $\langle\langle\overline{\sigma_1}\rangle\rangle = \langle\langle\overline{\sigma_2}\rangle\rangle$ *and* $\#\mathrm{St}_{G(L_2|K)}(\sigma_2) = \#\mathrm{St}_{G(L_1\cap L_2|K)}(\overline{\sigma_2})$.

In particular, $P_{L_1|K}(\sigma_1) \dot\subsetneq P_{L_2|K}(\sigma_2)$ *if and only if* $\langle\langle\overline{\sigma_1}\rangle\rangle = \langle\langle\overline{\sigma_2}\rangle\rangle$ *and*

$$\#\mathrm{St}_{G(L_1|K)}(\sigma_1) = \#\mathrm{St}_{G(L_1\cap L_2|K)}(\overline{\sigma_1}) = \#\mathrm{St}_{G(L_2|K)}(\sigma_2).$$

Proof: Let $N = L_1L_2$, $H_i = G(N|L_i)$, $i = 1, 2$, and $H = G(L_2|L_1 \cap L_2) \cong H_1$. We lift σ_i to $G(N|K)$ and denote it again by σ_i. Assume that (i) holds, i.e.

$$P_{L_1|K}(\sigma_1) \dot\subsetneq \bigcup_{\langle\langle\tau\rangle\rangle\cap\sigma_1H_1\neq\varnothing}{\cdot} P_{N|K}(\tau) \subsetneq \bigcup_{\langle\langle\tau\rangle\rangle\cap\sigma_2H_2\neq\varnothing}{\cdot} P_{N|K}(\tau) \dot\subsetneq P_{L_2|K}(\sigma_2).$$

Since the sets $P_{N|K}(\tau)$ have positive density, it follows that for every $h_1 \in H_1$ there exist $h_2 \in H_2$ and $\rho \in G(N|K)$ such that $\sigma_1h_1 = (\sigma_2)^\rho h_2$, and so $\langle\langle\overline{\sigma_1}\rangle\rangle = \langle\langle\overline{\sigma_2}\rangle\rangle$.

If $h \in H$ is a fixed element and $\tilde h$ a lifting of h to $G(N|K)$, then it follows that for every $h_1 \in H_1$ there exist $h_2 \in H_2$ and $\rho \in G(N|K)$ such that $\sigma_1h_1 = (\sigma_2\tilde h)^\rho h_2$, and therefore

$$\bigcup_{\langle\langle\tau\rangle\rangle\cap\sigma_1H_1\neq\varnothing}{\cdot} P_{N|K}(\tau) \subsetneq \bigcup_{\langle\langle\tau\rangle\rangle\cap(\sigma_2\tilde h)H_2\neq\varnothing}{\cdot} P_{N|K}(\tau).$$

We obtain $P_{L_1|K}(\sigma_1) \subsetneq P_{L_2|K}(\sigma_2h)$ for $h \in H$, hence

$$P_{L_1|K}(\sigma_1) \subsetneq \bigcap_{h\in H} P_{L_2|K}(\sigma_2h).$$

Since

$$P_{L_2|K}(\sigma_2) \cap P_{L_2|K}(\sigma_2h) \neq \varnothing \text{ if and only if } \langle\langle\sigma_2\rangle\rangle = \langle\langle\sigma_2h\rangle\rangle,$$

it follows that

$$P_{L_1\cap L_2|K}(\sigma_2H) \dot\subsetneq \bigcup_{\langle\langle\sigma_2h\rangle\rangle,h\in H}{\cdot} P_{L_2|K}(\sigma_2h) = P_{L_2|K}(\sigma_2),$$

and therefore

$$\frac{\#\langle\langle \sigma_2 H\rangle\rangle_{G(L_1\cap L_2|K)}}{\#G(L_1\cap L_2|K)} = \frac{\#\langle\langle\sigma_2\rangle\rangle_{G(L_2|K)}}{\#G(L_2|K)}\,.$$

From this equation we get

$$\#\mathrm{St}_{G(L_2|K)}(\sigma_2) = \#\mathrm{St}_{G(L_1\cap L_2|K)}(\sigma_2 H).$$

Conversely, using the arguments above in the other direction, we obtain from the assertion (ii) that $P_{L_1\cap L_2|K}(\sigma_2 H) \doteq P_{L_2|K}(\sigma_2)$. Since $\langle\langle\overline{\sigma_1}\rangle\rangle = \langle\langle\overline{\sigma_2}\rangle\rangle$, we get $P_{L_1|K}(\sigma_1) \subsetneq P_{L_1\cap L_2|K}(\sigma_2 H)$ and so (i). This finishes the proof of the proposition. □

Corollary 1.5. *Let L_1 and L_2 be finite Galois extensions of K and let σ_i be an element of $G(L_i|K)$, $i = 1, 2$. Assume that σ_2 lies in the center of $G(L_2|K)$. Then the following assertions are equivalent:*

(i) $P_{L_1|K}(\sigma_1) \subsetneq P_{L_2|K}(\sigma_2)$,

(ii) $L_2 \subseteq L_1$ *and* $\langle\langle\sigma_2\rangle\rangle = \langle\langle\sigma_1 \bmod G(L_1|L_2)\rangle\rangle$.

In particular, if σ_i lies in the center of $G(L_i|K)$, $i = 1, 2$, then

$$P_{L_1|K}(\sigma_1) \doteq P_{L_2|K}(\sigma_2) \quad \textit{if and only if} \quad L_1 = L_2 \textit{ and } \langle\langle\sigma_1\rangle\rangle = \langle\langle\sigma_2\rangle\rangle.$$

Proof: By assumption σ_2 lies in the center of $G(L_2|K)$, and so

$$\#\mathrm{St}_{G(L_2|K)}(\sigma_2) = \#\mathrm{St}_{G(L_1\cap L_2|K)}(\overline{\sigma_2})$$

if and only if $G(L_2|L_1\cap L_2) = 1$, i.e. $L_2 \subseteq L_1$. Now the corollary follows from proposition 1.4. □

Taking $\sigma_1 = 1 = \sigma_2$ it follows that $D(L_1|K) \doteq D(L_2|K)$ if and only if $L_1 = L_2$. Thus the corollary above is a generalization of a theorem of M.Bauer (see [3], theorem (13.9)).

In the next section we will need the following two lemmas.

Lemma 1.6. *Let $K|\mathbb{Q}$ be a finite Galois extension and for $i = 1, \ldots, n$ let $E_i \subseteq K$ be subfields of K, $F_i|E_i$ finite Galois extensions and $\sigma_i \in G(F_i|E_i)$. Then*

$$P^K_{K|\mathbb{Q}}(1) \cap \bigcap_{i=1}^{n} P^K_{F_i|E_i}(\sigma_i)$$

is empty or has positive density.

Proof: Let $F|E$ be one of the extensions $F_i|E_i$. Then

$$\varphi_{K|\mathbb{Q}}^{-1}P_{K|\mathbb{Q}}(1)\cap\varphi_{K|E}^{-1}P_{F|E}(\sigma)=\varphi_{K|\mathbb{Q}}^{-1}P_{K|\mathbb{Q}}(1)\cap\bigcup_{\langle\langle\tau\rangle\rangle\cap\sigma H\neq\varnothing}P_{FK|K}(\tau),$$

where $H=G(FK|F)$. Indeed, let $\mathfrak{P}_K\in\varphi_{K|\mathbb{Q}}^{-1}P_{K|\mathbb{Q}}(1)\subseteq\mathcal{P}_K$ and let $\mathfrak{P}_F$ be an extension of $\mathfrak{p}=\mathfrak{P}_K\cap E$ to F and $\mathfrak{P}_{FK}$ an extension of $\mathfrak{P}_F$ to FK. Then $\mathfrak{P}'_K=\mathfrak{P}_{FK}\cap K$ is conjugated to $\mathfrak{P}_K$. Since $\mathfrak{P}_{FK}$ is unramified over K and the residue degree $f(\mathfrak{P}'_K|\mathfrak{p})=1$, we have $\left(\frac{FK|K}{\mathfrak{P}_{FK}}\right)_{|F}=\left(\frac{F|E}{\mathfrak{P}_F}\right)$. Now the equality stated above follows easily. Thus we obtain

$$\begin{aligned}
&P_{K|\mathbb{Q}}^{K}(1)\cap\bigcap_{i=1}^{n}P_{F_i|E_i}^{K}(\sigma_i)=\\
&\varphi_{K|\mathbb{Q}}^{-1}P_{K|\mathbb{Q}}(1)\cap\bigcap_{i=1}^{n}\bigcup_{\langle\langle\tau_i\rangle\rangle\cap\sigma_iH_i\neq\varnothing}P_{F_iK|K}(\tau_i)=\\
&\varphi_{K|\mathbb{Q}}^{-1}P_{K|\mathbb{Q}}(1)\cap\bigcup_{\langle\langle\tau_1\rangle\rangle\cap\sigma_1H_1\neq\varnothing}\cdots\bigcup_{\langle\langle\tau_n\rangle\rangle\cap\sigma_nH_n\neq\varnothing}\Big(P_{F_1K|K}(\tau_1)\cap\cdots\cap P_{F_nK|K}(\tau_n)\Big).
\end{aligned}$$

From corollary 1.3 (i) it follows that the sets $P_{F_1K|K}(\tau_1)\cap\cdots\cap P_{F_nK|K}(\tau_n)$ are empty or have positive density. Since the density of $\varphi_{K|\mathbb{Q}}^{-1}P_{K|\mathbb{Q}}(1)$ is equal to 1, we proved the lemma. □

Lemma 1.7. *Let K be a number field and for $i=1,\dots,n$ let $E_i\subseteq K$ be subfields of K, $F_i|E_i$ finite Galois extensions, $E=\bigcap_i E_i$ and $\sigma_i\in G(F_i|E_i)$. Then the set*

$$S=\varphi_{K|E}^{-1}U(K|E)\cap\bigcap_{i=1}^{n}P_{F_i|E_i}^{K}(\sigma_i)$$

is empty or infinite.

Proof: Considering the normal closure of $KF_1\cdots F_n$ over E we may assume that $K=F_1=\cdots=F_n$ and that $K|E$ is a Galois extension. For a set T of primes of K let $(T)_{G(K|E)}$ be the closure under conjugation by $G(K|E)$. Obviously, it is sufficient to show that $(S)_{G(K|E)}$ is empty or infinite.

Suppose that $\mathfrak{P}\in S$ and let $\mathfrak{p}=\mathfrak{P}\cap E$. Then $\mathfrak{P}_{E_i}=\mathfrak{P}\cap E_i\in P_{K|E_i}(\sigma_i)$, i.e. there exists an extension $\mathfrak{P}_K$ of $\mathfrak{P}_{E_i}$ in K such that $\sigma_i=\left(\frac{K|E_i}{\mathfrak{P}_K}\right)$. Since $\mathfrak{P}$ and $\mathfrak{P}_K$ are conjugated over E_i, it follows that there is an element $\rho_i\in G(K|E_i)$ such that $\sigma_i^{\rho_i}=\left(\frac{K|E_i}{\mathfrak{P}}\right)$ and we may assume that $\sigma_i=\left(\frac{K|E_i}{\mathfrak{P}}\right)$. Since $\mathfrak{P}\in$

$\varphi_{K|E}^{-1}U(K|E)$, we have the element $\sigma = \left(\frac{K|E}{\mathfrak{P}}\right) \in G(K|E)$ and it follows that

$$\sigma_i = \left(\frac{K|E_i}{\mathfrak{P}}\right) = \left(\frac{K|E}{\mathfrak{P}}\right)^{f(\mathfrak{P}_{E_i}|\mathfrak{p})} = \sigma^{f(\mathfrak{P}_{E_i}|\mathfrak{p})},$$

where $f(\mathfrak{P}_{E_i}|\mathfrak{p})$ is the inertia degree of $\mathfrak{P}_{E_i}$ over E. We claim that

$$\varphi_{K|E}^{-1}P_{K|E}(\sigma) \subseteq (S)_{G(K|E)}.$$

Indeed, let $\mathfrak{P}' \in \varphi_{K|E}^{-1}P_{K|E}(\left(\frac{K|E}{\mathfrak{P}}\right))$. Then there exists a prime $\mathfrak{P}''$ of K which is conjugated to $\mathfrak{P}'$ over E such that $\left(\frac{K|E}{\mathfrak{P}}\right) = \left(\frac{K|E}{\mathfrak{P}''}\right)$. Let $f(\mathfrak{P}''_{E_i}|\mathfrak{p})$ be the inertia degree of $\mathfrak{P}''_{E_i}$ over E. Since $G(K|E_i) \cap G_{\mathfrak{P}''}(K|E) = G_{\mathfrak{P}''}(K|E_i)$, we get

$$\left(\frac{K|E}{\mathfrak{P}''}\right)^{f(\mathfrak{P}_{E_i}|\mathfrak{p})} = \left(\frac{K|E}{\mathfrak{P}}\right)^{f(\mathfrak{P}_{E_i}|\mathfrak{p})} = \left(\frac{K|E_i}{\mathfrak{P}}\right) \in G_{\mathfrak{P}''}(K|E_i).$$

Since $G_{\mathfrak{P}''}(K|E_i)$ is generated by the element $\left(\frac{K|E_i}{\mathfrak{P}''}\right) = \left(\frac{K|E}{\mathfrak{P}''}\right)^{f(\mathfrak{P}''_{E_i}|\mathfrak{p})}$, $f(\mathfrak{P}''_{E_i}|\mathfrak{p})$ divides $f(\mathfrak{P}_{E_i}|\mathfrak{p})$. Analogously,

$$\left(\frac{K|E}{\mathfrak{P}}\right)^{f(\mathfrak{P}''_{E_i}|\mathfrak{p})} = \left(\frac{K|E}{\mathfrak{P}''}\right)^{f(\mathfrak{P}''_{E_i}|\mathfrak{p})} = \left(\frac{K|E_i}{\mathfrak{P}''}\right) \in G_{\mathfrak{P}}(K|E_i),$$

and so $f(\mathfrak{P}_{E_i}|\mathfrak{p})$ divides $f(\mathfrak{P}''_{E_i}|\mathfrak{p})$. Therefore we obtain

$$\left(\frac{K|E_i}{\mathfrak{P}''}\right) = \left(\frac{K|E}{\mathfrak{P}''}\right)^{f(\mathfrak{P}''_{E_i}|\mathfrak{p})} = \left(\frac{K|E}{\mathfrak{P}}\right)^{f(\mathfrak{P}_{E_i}|\mathfrak{p})} = \left(\frac{K|E_i}{\mathfrak{P}}\right) = \sigma_i.$$

It follows that $\mathfrak{P}'' \in \varphi_{K|E_i}^{-1}P_{K|E_i}(\sigma_i)$ for all $i = 1, \ldots, n$, i.e. $\mathfrak{P}'' \in S$, and so $\mathfrak{P}' \in (S)_{G(K|E)}$. This proves the claim. Since $\varphi_{K|E}^{-1}P_{K|E}(\sigma)$ is an infinite set, we proved the lemma. □

We finish this section with a slightly more general version of the theorem of Grunwald/Wang (see also [4], theorem (9.2.2)).

Let p be a prime number, K a number field and $S \supseteq T$ sets of primes of K, where S contains the set $S_p \cup S_\infty$ of archimedean primes and primes above p. Let K_S be the maximal extension of K which is unramified outside S. By μ_p we denote the group of all p-th roots of unity.

Theorem 1.8. *Let K be a number field and let $S \supseteq T$ be sets of primes of K, where $S \supseteq S_p \cup S_\infty$, T is finite and*

$$\delta(S \cap D(K(\mu_p)|K)) > \frac{1}{p\,[K(\mu_p) : K]}\,.$$

Then the canonical homomorphism

$$H^1(K_S|K, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \bigoplus_{\mathfrak{p}\in T} H^1(K_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z})$$

is surjective.

Proof: Using [4], lemma (9.2.1), it is enough to show that the canonical map

$$H^1(K_S|K,\mu_p) \longrightarrow \prod_{\mathfrak{p}\in(S\backslash T)(K)} H^1(K_\mathfrak{p},\mu_p)$$

is injective. Since $[K(\mu_p):K]$ is prime to p, it is sufficient to show the injectivity of the homomorphism

$$H^1(K_S|K(\mu_p),\mu_p) \longrightarrow \prod_{\mathfrak{P}\in(S\backslash T)(K(\mu_p))} H^1(K(\mu_p)_\mathfrak{P},\mu_p).$$

An element of the kernel corresponds to a Galois extension $L|K(\mu_p)$ of degree p which is unramified outside $S(K(\mu_p))$ and completely decomposed at $(S\backslash T)(K(\mu_p))$. Since

$$\begin{aligned}\delta_{K(\mu_p)}((S\backslash T)(K(\mu_p))) &= \delta_{K(\mu_p)}(S(K(\mu_p))\\ &= \delta_K(S(K)\cap D(K(\mu_p)|K))\cdot[K(\mu_p):K] > \tfrac{1}{p}\,,\end{aligned}$$

such an extension has to be trivial. □

2. Topology

In this section we define a topology on the set $\mathcal{P}_K$ of non-trivial prime ideals of a number field K.

Definition 2.1. *For a number field K let*

$$\mathcal{B}_K = \{P^K_{F|E}(\sigma)\,|\,E\subseteq K,\ F|E \text{ a finite Galois extension},\ \sigma\in G(F|E)\},$$

and let $\mathcal{T}_K$ be the topology on $\mathcal{P}_K$ having $\mathcal{B}_K$ as a subbase. Obviously, the topology $\mathcal{T}_K$ has a countable base.

Remarks: 1. From corollary 1.3 (i) it follows that $\mathcal{C}_\mathbb{Q}\cup\{\varnothing\}$ is a base of $\mathcal{T}_\mathbb{Q}$.
2. If $K'|K$ is a finite extension, then by definition of the topologies $\mathcal{T}_K$ and $\mathcal{T}_{K'}$ the map

$$\varphi_{K'|K} : (\mathcal{P}_{K'},\mathcal{T}_{K'}) \longrightarrow (\mathcal{P}_K,\mathcal{T}_K),\quad \mathfrak{P}\mapsto\mathfrak{P}\cap K,$$

is continuous.
3. Not quite obvious is that $\mathcal{T}_K$ is not the discrete topology on $\mathcal{P}_K$. In order to see this, suppose that $\mathcal{T}_K$ is discrete. Then for every point $\mathfrak{p}\in\mathcal{P}_K$ the set $\{\mathfrak{p}\}$ is open and therefore there exist finite Galois extensions $F_i|E_i$, $E_i\subseteq K$, and $\sigma_i\in G(F_i|E_i)$, $i=1,\dots,n$, such that

$$\{\mathfrak{p}\} = \bigcap_{i=1}^n P^K_{F_i|E_i}(\sigma_i).$$

But if $\mathfrak{p}$ is contained in $U^K(K|\mathbb{Q})$, then this equality contradicts lemma 1.7.

For a subset W of $\mathcal{P}_K$ we denote the closure of W by $\overline{W}$.

Proposition 2.2.

(i) *Let* $P^K_{F|E}(\sigma) \in \mathcal{B}_K$. *Then*

$$\mathcal{P}_K \backslash \Big(P^K_{F|E}(\sigma) \cup R^K(F|E) \Big) = \bigcup_{\langle\langle\tau\rangle\rangle \neq \langle\langle\sigma\rangle\rangle}^{\cdot} P^K_{F|E}(\tau),$$

and so $P^K_{F|E}(\sigma) \cup R^K(F|E)$ *is a closed set. In particular,* $\overline{P^K_{F|E}(\sigma)} \backslash P^K_{F|E}(\sigma)$ *is a finite set.*

(ii) *Let* $F|\mathbb{Q}$ *be a Galois extension of prime degree and let* $\sigma \in G(F|\mathbb{Q})$. *Then* $P_{F|\mathbb{Q}}(\sigma) \cup R(F|\mathbb{Q})$ *is the closure of* $P_{F|\mathbb{Q}}(\sigma)$.

Proof: Assertion (i) follows from the equation

$$\mathcal{P}_K = \bigcup_{\langle\langle\tau\rangle\rangle}^{\cdot} \varphi^{-1}_{K|E} P_{F|E}(\tau) \cup^{\cdot} \varphi^{-1}_{K|E} R(F|E).$$

In order to prove (ii), suppose the contrary is true. Then there exists a prime number $p \in R(F|\mathbb{Q})$ and an open neighbourhood $U = P_{L|\mathbb{Q}}(\tau)$ of p, $L|\mathbb{Q}$ a finite Galois extension, such that U does not meet $P_{F|\mathbb{Q}}(\sigma)$. From corollary 1.3 (ii) it follows that F and L are not linearly disjoint over $\mathbb{Q}$, and so $F \subseteq L$. But p is unramified in L and ramifies in F. This contradiction shows assertion (ii).

□

Remark: In general the set $P^K_{F|E}(\sigma) \cup R^K(F|E)$ is not necessarily the closure of $P^K_{F|E}(\sigma)$, since there may be isolated points in the set $R^K(F|E)$, see proposition 2.6, or there may exist subextensions of $F|E$ in which elements of $R^K(F|E)$ are unramified.

Proposition 2.3.

(i) *For every two different points* $\mathfrak{p}_1$ *and* $\mathfrak{p}_2$ *of* $(\mathcal{P}_K, \mathcal{T}_K)$ *there exists a both open and closed neighbourhood* W *of* $\mathfrak{p}_1$ *such that* $\mathfrak{p}_2 \notin W$.

(ii) *Let* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *be pairwise different points of* $(\mathcal{P}_K, \mathcal{T}_K)$. *Then there exist both open and closed neighbourhoods* $U(\mathfrak{p}_i)$ *of* $\mathfrak{p}_i$ *such that*

$$U(\mathfrak{p}_i) \cap U(\mathfrak{p}_j) = \varnothing \quad \text{for } i \neq j.$$

Proof: In order to prove (i) let $L|K$ be a cyclic extension of degree $m > 2$ such that $\mathfrak{p}_1$ is unramified in $L|K$ and let $\sigma \in G(L|K)$ with $\mathfrak{p}_1 \in P_{L|K}(\sigma)$. We denote the open neighbourhood $P_{L|K}(\sigma)$ of $\mathfrak{p}_1$ by U.

Let $N|K$ be a quadratic extension of K which is unramified at all primes of U, completely decomposed at $R(L|K) \cup \{\mathfrak{p}_2\}$ and inert at $\mathfrak{p}_1$; if $V = P_{N|K}(\tau)$, where τ is the non-trivial element of $G(N|K)$, then $\mathfrak{p}_1 \in V$ and $\mathfrak{p}_2 \notin V$. Such an extension exists. Indeed, let

$$T = S_2 \cup S_\infty \cup R(L|K) \cup \{\mathfrak{p}_1, \mathfrak{p}_2\} \quad \text{and} \quad S = (\mathcal{P}_K \backslash U) \cup T,$$

then

$$\delta_K(S) = 1 - \frac{1}{m} > \frac{1}{2},$$

and so we can apply theorem 1.8: there exists an element $\varphi \in H^1(K_S|K, \mathbb{Z}/2\mathbb{Z})$ such that

$$res_{\mathfrak{p}}(\varphi) = 0 \in H^1(K_{\mathfrak{p}}, \mathbb{Z}/2\mathbb{Z})) \quad \text{for } \mathfrak{p} \in T \backslash \{\mathfrak{p}_1\}$$

and

$$0 \neq res_{\mathfrak{p}_1}(\varphi) \in H^1_{nr}(K_{\mathfrak{p}_1}, \mathbb{Z}/2\mathbb{Z}) \subset H^1(K_{\mathfrak{p}_1}, \mathbb{Z}/2\mathbb{Z}).$$

If $\ker \varphi = G(K_S|N)$, then N is a quadratic extension of K with the desired properties.

Now $W = U \cap V$ is an open neighbourhood of $\mathfrak{p}_1$ and $\mathfrak{p}_2 \notin W$. It remains to show that W is closed. Let $\overline{W}$ be the closure of W. Using proposition 2.2(i), we get

$$\overline{U \cap V} \subseteq \overline{U} \cap \overline{V} \subseteq (U \cup R(L|K)) \cap (V \cup R(N|K)) = U \cap V,$$

and so $\overline{W} = W$. This finishes the proof of (i).

In order to prove (ii) we use induction with respect to n. Assume that we have found open and closed neighbourhoods $W(\mathfrak{p}_i)$ of $\mathfrak{p}_i$, $i = 1, \ldots, n-1$, which are pairwise disjoint. By (i) it follows that for every $i \in \{1, \ldots, n-1\}$ there exists an open and closed neighbourhood $W_i(\mathfrak{p}_n)$ of $\mathfrak{p}_n$ such that $\mathfrak{p}_i \notin W_i(\mathfrak{p}_n)$. Then

$$U(\mathfrak{p}_n) = \bigcap_{i=1}^{n-1} W_i(\mathfrak{p}_n)$$

is an open and closed neighbourhood of $\mathfrak{p}_n$ such that $\mathfrak{p}_i \notin U(\mathfrak{p}_n)$ for all $i = 1, \ldots, n-1$. Now the open and closed neighbourhoods $U(\mathfrak{p}_i) = W(\mathfrak{p}_i) \backslash U(\mathfrak{p}_n)$, $i = 1, \ldots, n-1$, and $U(\mathfrak{p}_n)$ have the desired property. □

Recall that a Hausdorff space X is called *zero-dimensional* if every point of X has a fundamental system of neighbourhoods which are both open and closed, and X is called *strongly zero-dimensional* if for every closed subset A of X and each neighbourhood U of A there is an open and closed neighbourhood of A contained in U.

Proposition 2.4. *The space $(\mathcal{P}_K, \mathcal{T}_K)$ has the following properties: it is*

(i) *a Hausdorff space,*

(ii) *strongly zero-dimensional (and so totally disconnected),*

(iii) *metrizable (and so normal and completely regular),*

(iv) *every point of $(\mathcal{P}_K, \mathcal{T}_K)$ has a base of neighbourhoods consisting of both open and closed sets.*

Proof: By proposition 2.3(i) there exists for every two different points x and y of $\mathcal{P}_K$ an open and closed neighbourhood W of x such that $y \notin W$. It follows that $\mathcal{P}_K \backslash W$ is an open neighbourhood of y being disjoint to W. Therefore $\mathcal{P}_K$ is a Hausdorff space.

Now we prove (iv). Let $\mathfrak{p} \in (\mathcal{P}_K, \mathcal{T}_K)$ and let $U = \bigcap_{i=1}^{n} P^K_{F_i|E_i}(\sigma_i)$ be an open neighbourhood of $\mathfrak{p}$. We have to find and open and closed neighbourhood of $\mathfrak{p}$ being contained in U. Obviously we may assume that $U = P^K_{F|E}(\sigma)$. By proposition 2.3(ii) there exist open und closed, pairwise disjoint neighbourhoods $U(\mathfrak{p}_i)$ of $\mathfrak{p}_i$ $i = 0, \ldots, n$, where $\{\mathfrak{p}_1 \ldots, \mathfrak{p}_n\} = R^K(F|E)$ and $\mathfrak{p}_0 = \mathfrak{p}$. Then

$$U_R = \bigcup_{i=1}^{n} \cdot\, U(\mathfrak{p}_i)$$

is an open and closed neighbourhood of $R^K(F|E)$ not containing $\mathfrak{p}$. Let $V = P^K_{F|E}(\sigma) \backslash U_R$, then V is open and contains $\mathfrak{p}$. But V is also closed, since we get for the closure $\overline{V}$ of V, using proposition 2.2(i),

$$\begin{aligned} \overline{P^K_{F|E}(\sigma) \backslash U_R} &= \overline{P^K_{F|E}(\sigma) \cap (\mathcal{P}_K \backslash U_R)} \\ &\subseteq \overline{P^K_{F|E}(\sigma)} \cap (\mathcal{P}_K \backslash U_R) \\ &\subseteq (P^K_{F|E}(\sigma) \cup R^K(F|E)) \cap (\mathcal{P}_K \backslash U_R) \\ &= P^K_{F|E}(\sigma) \backslash U_R. \end{aligned}$$

This finishes the proof of (iv). The other assertions follow from [2] IX.6 exercise 2(b) since the considered space has a countable base. □

Proposition 2.5.

(i) *Let $\mathfrak{p} \in (\mathcal{P}_K, \mathcal{T}_K)$ be a prime ideal of K such that $p = \mathfrak{p} \cap \mathbb{Q}$ is completely decomposed in K. Then every open neighbourhood of $\mathfrak{p}$ has positive density.*

(ii) *Let $\mathfrak{p} \in (\mathcal{P}_K, \mathcal{T}_K)$ be a prime ideal of K such that $p = \mathfrak{p} \cap \mathbb{Q}$ is unramified in K. Then every open neighbourhood of $\mathfrak{p}$ has infinitely many points.*

Proof: Let $\mathfrak{p} \in (\mathcal{P}_K, \mathcal{T}_K)$ such that $p = \mathfrak{p} \cap \mathbb{Q}$ is completely decomposed in K and let U be an open neighbourhood of $\mathfrak{p}$. The prime number p is also completely decomposed in the normal closure N of $K|\mathbb{Q}$. If $\mathfrak{P}$ is an extension of $\mathfrak{p}$ to N, then $V = \varphi^{-1}_{N|K}(U)$ is an open neighbourhood of $\mathfrak{P}$. Since every open neighbourhood of a point of $(\mathcal{P}_N, \mathcal{T}_N)$ contains a set which is a finite intersection of sets of $\mathcal{B}_N$, it follows from lemma 1.6 that V has positive density, and so U has. This proves assertion (i) and (ii) follows from lemma 1.7. □

Recall that a point x of a topological space X is called *isolated* if $\{x\}$ is an open set in X.

If $G(F|E)$ is the Galois group of a finite Galois extension $F|E$ and $\mathfrak{P}$ a prime of F, then we denote the decomposition group and the inertia subgroup of $G(F|E)$ with respect to $\mathfrak{P}$ by $G_{\mathfrak{P}} = G_{\mathfrak{P}}(F|E)$ and $T_{\mathfrak{P}} = T_{\mathfrak{P}}(F|E)$, respectively. If ℓ is a prime number, then $G(\ell)$ is a ℓ-Sylow group of a group G.

Proposition 2.6. *Let $K|\mathbb{Q}$ be a finite extension and let $\mathfrak{p} \in \varphi^{-1}_{K|\mathbb{Q}}(R(K|\mathbb{Q}))$.*

(i) *Assume that $K|\mathbb{Q}$ is normal and that $G_{\mathfrak{p}}(K|\mathbb{Q})$ has the following property:*

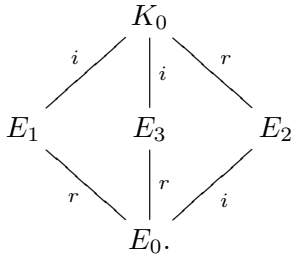
there exists a prime number ℓ such that $G_{\mathfrak{p}}(\ell)$ is not cyclic and the quotient $G_{\mathfrak{p}}(\ell)/T_{\mathfrak{p}}(\ell)$ is non-trivial. Then $\mathfrak{p}$ is an isolated point of $(\mathcal{P}_K, \mathcal{T}_K)$.

(ii) *For every prime ideal $\mathfrak{P}|\mathfrak{p}$ of the normal closure N of $K|\mathbb{Q}$ there exists a finite Galois extension $L|N$ such that $\mathfrak{P}$ and all $G(N|\mathbb{Q})$-conjugates of $\mathfrak{P}$ are inert in $L|N$ and their unique extensions to L are isolated in $(\mathcal{P}_L, \mathcal{T}_L)$.*

Proof: Let $K_0 \subseteq K$ be the fixed field of $[G_{\mathfrak{p}}(\ell), G_{\mathfrak{p}}(\ell)]$. From our assumptions it follows that K_0 has subfields E_i, $i = 0, 1, 2$, such that $K_0 = E_1E_2$, $E_0 = E_1 \cap E_2$ and

$$G(K_0|E_0) \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z},$$

and $\mathfrak{p} \cap E_1$ is inert and $\mathfrak{p} \cap E_2$ is ramified in K_0. Let E_3 be any extension of E_0 in K_0 of degree ℓ different to E_1 and E_2:



The letters i and r indicate whether $\mathfrak{p} \cap E_0$ resp. its unique extensions to the fields E_i, $i = 1, 2, 3$, are inert or ramify in the considered extensions. Now we consider the open set

$$U = P^{K_0}_{K_0|E_1}(\sigma) \cap P^{K_0}_{K_0|E_3}(\tau) = \varphi^{-1}_{K_0|E_1} P_{K_0|E_1}(\sigma) \cap \varphi^{-1}_{K_0|E_3} P_{K_0|E_3}(\tau)$$

of $(\mathcal{P}_{K_0}, \mathcal{T}_{K_0})$, where $\sigma = \left(\frac{K_0|E_1}{\mathfrak{p} \cap K_0}\right)$ and $\tau = \left(\frac{K_0|E_3}{\mathfrak{p} \cap K_0}\right)$. Observe that $\sigma \neq 1 \neq \tau$ and $\mathfrak{p}_0 = \mathfrak{p} \cap K_0 \in U$.

Let $\mathfrak{p}'$ be a prime ideal contained in U. Since $K_0|E_0$ is not cyclic and $\mathfrak{p}' \cap E_1$ is inert in $K_0|E_1$, $\mathfrak{p}' \cap E_0$ is completely decomposed or ramifies in $E_1|E_0$. In the first case its extensions to E_3 would also be completely decomposed in $K_0|E_3$, and so $\mathfrak{p}'$ can not be contained in $\varphi^{-1}_{K_0|E_3} P_{K_0|E_3}(\tau)$. It follows that

$U \subseteq \varphi^{-1}_{K_0|E_0} R(K_0|E_0)$, and so U is finite. Therefore $\{\mathfrak{p}_0\} \subseteq U$ is also open (the finite set $U\backslash\{\mathfrak{p}_0\}$ is closed as $(\mathcal{P}_{K_0}, \mathcal{T}_{K_0})$ is a Hausdorff space). Therefore $\mathfrak{p}_0$ is an isolated point of $(\mathcal{P}_{K_0}, \mathcal{T}_{K_0})$, and so $\mathfrak{p} = \varphi^{-1}_{K|K_0}(\mathfrak{p}_0)$ is an isolated point of $(\mathcal{P}_K, \mathcal{T}_K)$. This proves assertion (i).

In order to prove (ii) let $\mathfrak{P}$ be a prime ideal contained in $\varphi^{-1}_{N|\mathbb{Q}}(R(N|\mathbb{Q}))$ and let ℓ be any prime number dividing the order of the inertia subgroup $T_{\mathfrak{P}}$ of $G_{\mathfrak{P}} = G_{\mathfrak{P}}(N|\mathbb{Q})$. Let $L_0|\mathbb{Q}$ be a cyclic extension of ℓ-power degree such that $\mathfrak{P} \cap \mathbb{Q}$ is inert in $L_0|\mathbb{Q}$ and $L_0 \subsetneq N$. Let $L = NL_0$. Then all $G(N|\mathbb{Q})$-conjugates of $\mathfrak{P}$ are inert in $L|N$ and $G_{\mathfrak{P}_L}(L|\mathbb{Q})$ fulfills the condition of (i), where $\mathfrak{P}_L$ denotes the unique extension of $\mathfrak{P}$ to L. It follows that $\mathfrak{P}_L$ is isolated in $(\mathcal{P}_L, \mathcal{T}_L)$. □

Definition 2.7. *Let K be a number field and N the normal closure of $K|\mathbb{Q}$. A point $\mathfrak{p} \in (\mathcal{P}_K, \mathcal{T}_K)$ is called* **potentially isolated** *if for every $\mathfrak{P}|\mathfrak{p}$ of N there exists a finite Galois extension $L|N$ such that*

(i) *all $G(N|\mathbb{Q})$-conjugates of $\mathfrak{P}$ are unramified in $L|N$,*

(ii) *all points of $\varphi^{-1}_{L|N}(\mathfrak{P})$ are isolated in $(\mathcal{P}_L, \mathcal{T}_L)$.*

We denote the set of all isolated points and the set of all potentially isolated points of $(\mathcal{P}_K, \mathcal{T}_K)$ by $(\mathcal{P}_K)_{iso}$ and $(\mathcal{P}_K)_{p.iso}$, respectively.

Without condition (i) in the definition above, i.e. $\varphi^{-1}_{N|\mathbb{Q}}(\mathfrak{P} \cap \mathbb{Q}) \subseteq U(L|N)$, all points of $\mathcal{P}_K$ would be potentially isolated, since for every $\mathfrak{p} \in \mathcal{P}_K$ there exists a finite Galois extension $K'|K$ in which $\mathfrak{p}$ ramifies, and we can apply proposition 2.6(ii) to the field K'. Furthermore we would like to mention (although it is completely trivial) that $\mathcal{P}_{\mathbb{Q}}$ has no isolated points, since every open set of $\mathcal{P}_{\mathbb{Q}}$ has positive density. The following proposition considers the general case.

Theorem 2.8. *Let K be a number field. Then the following is true:*

(i) $$(\mathcal{P}_K)_{iso} \subseteq \varphi^{-1}_{K|\mathbb{Q}}(R(K|\mathbb{Q})) = (\mathcal{P}_K)_{p.iso},$$

(ii) $$\varphi^{-1}_{K|\mathbb{Q}}(U(K|\mathbb{Q})) \subseteq \{\mathfrak{p} \in \mathcal{P}_K \mid \begin{array}{l}\textit{every open neighbourhood of } \mathfrak{p} \\ \textit{has infinitely many points}\end{array}\},$$

(iii) $$\varphi^{-1}_{K|\mathbb{Q}}(D(K|\mathbb{Q})) \subseteq \{\mathfrak{p} \in \mathcal{P}_K \mid \begin{array}{l}\textit{every open neighbourhood of } \mathfrak{p} \\ \textit{has positive density}\end{array}\}.$$

If $K|\mathbb{Q}$ is a Galois extension, then we have equality in (iii).

Proof: Let N be the normal closure over K over $\mathbb{Q}$. The inclusion

$$\varphi_{K|\mathbb{Q}}^{-1}(R(K|\mathbb{Q})) \subseteq (\mathcal{P}_K)_{p.iso}$$

is just proposition 2.6(ii). In order to prove the other inclusion suppose that $\mathfrak{p} \in (\mathcal{P}_K)_{p.iso}$ is not contained in $\varphi_{K|\mathbb{Q}}^{-1}(R(K|\mathbb{Q}))$. Then the extensions $\mathfrak{P}$ of $\mathfrak{p}$ to N are contained in $\varphi_{N|\mathbb{Q}}^{-1}(U(N|\mathbb{Q}))$. Let $\mathfrak{P}_0$ be one of these extensions and let $L|N$ be a finite Galois extension such that all $G(N|\mathbb{Q})$-conjugates of $\mathfrak{P}_0$ are unramified in $L|N$ and all points $\mathfrak{P}_{0L} \in \varphi_{L|N}^{-1}(\mathfrak{P}_0)$ are isolated in $(\mathcal{P}_L, \mathcal{T}_L)$. Then $\mathfrak{P}_{0L} \in \varphi_{L|\mathbb{Q}}^{-1}(U(L|\mathbb{Q}))$. This contradicts proposition 2.5(ii) and therefore we proved the equality stated in (i). Assertions (ii) (and so the inclusion in (i)) and the inclusion (iii) follow from proposition 2.5(ii) and (i), respectively.

Now we show that for every point $\mathfrak{P} \in \varphi_{N|\mathbb{Q}}^{-1}(U(N|\mathbb{Q}))\backslash\varphi_{N|\mathbb{Q}}^{-1}(D(N|\mathbb{Q}))$ there exists an open neighbourhood of density equal to 0. Indeed, let $N_0 \subset N$ be its decomposition field and observe that by assumption $N \neq N_0$. Therefore $\tau = \left(\frac{N|N_0}{\mathfrak{P}}\right) \in G(N|N_0)$ is not equal to 1. Obviously, $\mathfrak{P} \in \varphi_{N|N_0}^{-1} P_{N|N_0}(\tau)$ and this open set has density equal to 0 since every prime ideal of $P_{N|N_0}(\tau)$ is inert in the extension $N|N_0$. So we get

$$\varphi_{N|\mathbb{Q}}^{-1}(D(N|\mathbb{Q})) = \{\mathfrak{P} \in \mathcal{P}_N \mid \begin{array}{l}\text{every open neighbourhood of } \mathfrak{P} \\ \text{has positive density}\end{array} \}$$

showing also the last assertion of the theorem. □

Remark: The inclusion in (ii) may be strict (even if $K|\mathbb{Q}$ is a Galois extension), i.e. there may exist ramified primes having only infinite open neighbourhoods, or with other words, it is possible that there are ramified points which are not isolated. But one can show that for a number field $K|\mathbb{Q}$ there exists a finite Galois extension $L|K$ such that $\varphi_{L|\mathbb{Q}}^{-1}(R(L|\mathbb{Q})) = (\mathcal{P}_L)_{iso}$.

3. Uniformity

In this section we consider uniformities on $\mathcal{P}_K$ which induce the topology $\mathcal{T}_K$. First we recall some facts concerning uniform structures on a normal topological space $(X, \mathcal{T})$:

The *uniformity* $\mathfrak{U}^{oc}$ *of finite partitions by open and closed subsets of* X is defined by the base

$$\mathfrak{V}^{oc} = \{ \bigcup_{i=1}^{n \cdot} (V_i \times V_i) \subseteq X \times X \mid V_i \subseteq (X, \mathcal{T}) \text{ open and closed}, \bigcup_{i=1}^{n \cdot} V_i = X\}.$$

We denote the completion of $(X, \mathfrak{U}^{oc})$ by $(\hat{X}, \hat{\mathfrak{U}}^{oc})$. The *uniformity* $\mathfrak{U}^o$ *of finite open coverings on* X is defined by the base

$$\mathfrak{V}^o = \{ \bigcup_{i=1}^{n} (U_i \times U_i) \subseteq X \times X \mid n \in \mathbb{N},\, U_i \in \mathcal{T},\, \bigcup_{i=1}^{n} U_i = X \}.$$

The *Stone-Čech compactification* βX of $(X, \mathcal{T})$ is the completion of X with respect to the coarsest uniformity $\mathfrak{U}^{S\check{C}}$ on X for which all continuous mappings of X into $[0, 1]$ are uniformly continuous. Concerning these three uniformities on X we have the

Proposition 3.1. *Let* $(X, \mathcal{T})$ *be a strongly zero-dimensional Hausdorff space. Then following is true.*

(i) *The uniform structures* $\mathfrak{U}^{oc}$, $\mathfrak{U}^o$ *and* $\mathfrak{U}^{S\check{C}}$ *on* X *are equal, now denoted by* $\mathfrak{U}$. *The topology induced by* $\mathfrak{U}$ *on* X *is equal to* $\mathcal{T}$.

(ii) *The completion* $(\hat{X}, \hat{\mathfrak{U}})$ *of* X *equipped with the uniformity* $\mathfrak{U} = \mathfrak{U}^{oc}$ *is a profinite space, i.e. it is compact and totally disconnected.*

Proof: Since $(X, \mathcal{T})$ is normal, the uniformity $\mathfrak{U}^o$ is equal to the uniformity $\mathfrak{U}_K^{S\check{C}}$ and $\mathfrak{U}^o = \mathfrak{U}^{S\check{C}}$ induces the topology $\mathcal{T}$ on X, see [2] IX.1 ex. 7, IX.4 ex. 17.

By definition $\mathfrak{U}^{oc}$ is coarser than $\mathfrak{U}^o$ and, since $(X, \mathcal{T})$ is strongly zero-dimensional, there exists for every open covering $\bigcup_{i=1}^{n} U_i$ of X a refinement $\bigcup\!\!\!\cdot\, {}_{i=1}^{n} V_i = X$ where $V_i \subseteq (X, \mathcal{T})$ is open and closed. Thus $\mathfrak{U}^{oc}$ is finer than $\mathfrak{U}^o$, and so they are equal. This proves (i).

From (i) it follows that $(\hat{X}, \hat{\mathfrak{U}}) = \beta(X, \mathcal{T})$ and the compact space $\beta(X, \mathcal{T})$ is totally disconnected, see [2] IX.6 ex. 1(b). This proves (ii). □

Proposition 3.2. *Let* X *be a strongly zero-dimensional Hausdorff space and let*

$$i : (X, \mathfrak{U}) \longrightarrow (\hat{X}, \hat{\mathfrak{U}})$$

be the canonical mapping $(\mathfrak{U} = \mathfrak{U}^{oc})$ *and we identify* X *with* $i(X)$. *Let* $\mathcal{OC}_X$ *and* $\mathcal{OC}_{\hat{X}}$ *be the set of both open and closed subsets of* X *and* $\hat{X}$, *respectively.*

(i) *The maps*

$$\mathcal{OC}_X \longrightarrow \mathcal{OC}_{\hat{X}}, \quad S \mapsto \overline{S}, \quad \textit{and} \quad \mathcal{OC}_{\hat{X}} \longrightarrow \mathcal{OC}_X, \quad \mathcal{S} \mapsto \mathcal{S} \cap X$$

are bijections, where $\overline{S}$ *is the closure of* S *in* $\hat{X}$.

(ii) *For the set of isolated points of* X *and* $\hat{X}$ *we have* $i(X_{iso}) = \hat{X}_{iso}$.

Proof: It is clear that the second map is well-defined. Let $S \in \mathcal{O}C_X$. Since S and $X\backslash S$ are closed sets of X, we get from $S \cup (X\backslash S) = X$ the partition $\overline{S} \cup \overline{X\backslash S} = \hat{X}$, see [2] IX.4 ex. 17(c), and so $\hat{X}\backslash\overline{S} = \overline{X\backslash S}$. Thus the closed set $\overline{S}$ is also open in $\hat{X}$, and so also the first map is well-defined.

If $S \in \mathcal{O}C_X$, then $S \subseteq \overline{S} \cap X$. Let $x \in \overline{S} \cap X$ and suppose that $x \in X\backslash S$. Then $x \in \overline{X\backslash S} = \hat{X}\backslash\overline{S}$ which is a contradiction, and it follows that $x \in S$. Therefore $S = \overline{S} \cap X$.

If $\mathcal{S} \in \mathcal{O}C_{\hat{X}}$, then $\overline{\mathcal{S} \cap X} \subseteq \mathcal{S}$, since $\mathcal{S}$ is closed. Since $\mathcal{S}$ is also open, $\mathcal{S} \cap X$ is dense in $\mathcal{S}$, and so $\overline{\mathcal{S} \cap X} = \mathcal{S}$. This proves that the considered maps are bijections.

In order to prove (ii) let $\hat{x} \in \hat{X}_{iso}$. Then $\{\hat{x}\}$ is open in $\hat{X}$. Since $i(X)$ is dense in $\hat{X}$, the set $\{\hat{x}\} \cap i(X)$ is not empty and so $\hat{x} \in i(X)$. Thus $\{\hat{x}\}$ is an open subset of $i(X)$.

Conversely, let $x \in X_{iso}$. Since the set $\{x\}$ is open and closed in X, the same is true, by (i), for its closure $\overline{\{x\}}$ in $\hat{X}$. Consider the open set $U = \overline{\{x\}}\backslash\{i(x)\} \subseteq \hat{X}$ (observe that $\{i(x)\}$ is closed in the Hausdorff space $\hat{X}$). Suppose that U is not empty. Then, using (i), we get the contradiction

$$\varnothing \neq U \cap i(X) = (\overline{\{x\}} \cap i(X))\backslash\{i(x)\} = \{i(x)\}\backslash\{i(x)\}.$$

Therefore U is empty, i.e. $\overline{\{x\}} = \{i(x)\}$, and so $\{i(x)\}$ is open in $\hat{X}$. □

Now let $(X, \mathcal{T}) = (\mathcal{P}_K, \mathcal{T}_K)$. This space is a strongly zero-dimensional Hausdorff space by proposition 2.4(ii). If $\mathfrak{U}_K = \mathfrak{U}_K^{oc}$ denotes the uniformity of finite partitions of $\mathcal{P}_K$ by both open and closed subsets of $(\mathcal{P}_K, \mathcal{T}_K)$, then we obtain

Theorem 3.3. *The Hausdorff uniform space $(\mathcal{P}_K, \mathfrak{U}_K)$ is pre-compact and strongly zero-dimensional, and its completion $(\hat{\mathcal{P}}_K, \hat{\mathfrak{U}}_K)$ is a profinite space. The canonical map*

$$i : (\mathcal{P}_K, \mathfrak{U}_K) \longrightarrow (\hat{\mathcal{P}}_K, \hat{\mathfrak{U}}_K)$$

induces an isomorphism of $(\mathcal{P}_K, \mathfrak{U}_K)$ onto a dense subspace of $(\hat{\mathcal{P}}_K, \hat{\mathfrak{U}}_K)$.

Furthermore the sets $(\mathcal{P}_K)_{iso}$ and $(\hat{\mathcal{P}}_K)_{iso}$ of isolated points are isomorphic and finite.

4. A metric for $\mathcal{P}_{\mathbb{Q}}$

In this section we will define a metric on $\mathcal{P}_{\mathbb{Q}}$ which induces the topology $\mathcal{T}_{\mathbb{Q}}$. The idea is that two points $x, y \in \mathcal{P}_{\mathbb{Q}}$ are *near*, if they induce in *many* fields with *large* discriminant the same Frobenius automorphism. We start by defining another uniformity on $\mathcal{P}_{\mathbb{Q}}$: *the uniformity of finite open coverings of $(\mathcal{P}_{\mathbb{Q}}, \mathcal{T}_{\mathbb{Q}})$ defined by the discriminant of finite Galois extensions $F|\mathbb{Q}$.*

Let $d \in \mathbb{N}$ and let

$$S_d = \{F|\mathbb{Q} \text{ a finite Galois extension, } |D(F|\mathbb{Q})| \leq d\},$$

where $D(F|\mathbb{Q})$ denotes the discriminant of F. The set S_d is finite by Hermite's theorem, see [3] III. (2.16). For $x \in \mathcal{P}_\mathbb{Q}$ let

$$S_{d,x} = \{F|\mathbb{Q} \text{ finite Galois }, x \in U(F|\mathbb{Q}), |D(F|\mathbb{Q})| \leq d\}$$

and

$$V_d(x) = \bigcap_{F|\mathbb{Q} \in S_{d,x}} P_{F|\mathbb{Q}}(\Big(\frac{F|\mathbb{Q}}{x_F}\Big)),$$

where x_F is an extension of x to F. Furthermore let

$$R_d = \bigcup_{F|\mathbb{Q} \in S_d} R(F|\mathbb{Q}), \qquad G_d = \prod_{F|\mathbb{Q} \in S_d} G(F|\mathbb{Q}), \qquad V_d(\tilde{\sigma}) = \bigcap_{F|\mathbb{Q} \in S_d} P_{F|\mathbb{Q}}(\sigma_{F|\mathbb{Q}})$$

for $\tilde{\sigma} = (\sigma_{F|\mathbb{Q}})_{F|\mathbb{Q}} \in G_d$. Observe that $V_d(\tilde{\sigma}) = V_d(x)$ for all $x \in V_d(\tilde{\sigma})$. We obtain a finite open covering

$$Cov^o(d): \qquad \mathcal{P}_\mathbb{Q} = \bigcup_{\tilde{\sigma} \in G_d} V_d(\tilde{\sigma}) \cup \bigcup_{\alpha \in R_d} V_d(\alpha)$$

of $\mathcal{P}_\mathbb{Q}$. Finally we define

$$V_d = \bigcup_{\tilde{\sigma} \in G_d} \Big(V_d(\tilde{\sigma}) \times V_d(\tilde{\sigma})\Big) \cup \bigcup_{\alpha \in R_d} \Big(V_d(\alpha) \times V_d(\alpha)\Big).$$

Obviously, we have $V_{d'} \subseteq V_d$ for $d \leq d'$.

Proposition 4.1. *The set $\mathfrak{V}_\mathbb{Q}^D = \{ V_d \,,\, d \in \mathbb{N}\}$ is a base for a uniform structure $\mathfrak{U}_\mathbb{Q}^D$ on $\mathcal{P}_\mathbb{Q}$ inducing the topology $\mathcal{T}_\mathbb{Q}$.*

Proof: Let $V_d \in \mathfrak{V}_\mathbb{Q}^D$. By proposition 2.3(ii) we find open (and closed) neighbourhoods $U(\alpha)$ of $\alpha \in R_d$ which are pairwise disjoint and defined by finitely many extensions of $\mathbb{Q}$ (see the proof of 2.3(ii)). Let $\tilde{V}_d(\alpha) = V_d(\alpha) \cap U(\alpha)$ and $\tilde{V}_d(\tilde{\sigma}) = V_d(\tilde{\sigma}) \backslash V(R_d)$, where $V(R_d) = \dot{\bigcup}_{\alpha \in R_d} \tilde{V}_d(\alpha)$ is an open and closed neighbourhood of the set R_d. Then

$$\widetilde{Cov}(d): \qquad \mathcal{P}_\mathbb{Q} = \dot{\bigcup_{\tilde{\sigma} \in G_d}} \tilde{V}_d(\tilde{\sigma}) \,\dot{\cup}\, \dot{\bigcup_{\alpha \in R_d}} \tilde{V}_d(\alpha)$$

is a partition of $\mathcal{P}_\mathbb{Q}$ by open sets which is a refinement of $Cov^o(d)$. Furthermore these open sets are defined by finitely many extensions of $\mathbb{Q}$. Let

$$d' = max_F\{|D(F|\mathbb{Q})|\},$$

where F runs through all extensions of $\mathbb{Q}$ which appear in a definition of the open sets in $\widetilde{Cov}(d)$. Then $Cov^o(d')$ is a refinement of $\widetilde{Cov}(d)$. Indeed, let $U \in Cov^o(d')$, i.e. $U = V_{d'}(\tilde{\sigma})$ for some $\tilde{\sigma} \in G_{d'}$ or $U = V_{d'}(\alpha)$ for some $\alpha \in R_{d'}$. Then $U = V_{d'}(x)$ for some $x \in \mathcal{P}_\mathbb{Q}$. Let $V \in \widetilde{Cov}(d)$ be the unique

open set containing x. It follows that $U \subseteq V$, since V is the (finite) union of open sets of the form $\bigcap_{i=1}^{r} P_{F_i|\mathbb{Q}}(\sigma_i)$, where $|D(F_i|\mathbb{Q})| \leq d'$ for all i, and at least one of these sets contains x.

Now we prove that the set $\mathfrak{V}_{\mathbb{Q}}^D = \{\, V_d \,,\, d \in \mathbb{N}\}$ is a base for a uniform structure on $\mathcal{P}_{\mathbb{Q}}$. The only axiom, which is not obvious, is the following: for $V_d \in \mathfrak{V}_{\mathbb{Q}}^D$ there exists a $V_{d'} \in \mathfrak{V}_{\mathbb{Q}}^D$ such that $\overset{2}{V}_{d'} \subseteq V_d$, where

$$\overset{2}{V}_{d'} = \{(x,y) \in \mathcal{P}_{\mathbb{Q}} \times \mathcal{P}_{\mathbb{Q}} \,|\, (x,z),(z,y) \in V_d \text{ for some } z \in \mathcal{P}_{\mathbb{Q}}\}.$$

But, taking d' as above, and let

$$W_d = \bigcup_{\tilde{\sigma} \in G_d}^{\cdot} \Big(\tilde{V}_d(\tilde{\sigma}) \times \tilde{V}_d(\tilde{\sigma})\Big) \cup \bigcup_{\alpha \in R_d}^{\cdot} \Big(\tilde{V}_d(\alpha) \times \tilde{V}_d(\alpha)\Big),$$

then it follows by the consideration above that $\overset{2}{V}_{d'} \subseteq \overset{2}{W}_d = W_d \subseteq V_d$.

Finally, the topology induced by $\mathfrak{U}_{\mathbb{Q}}^D$ is obviously coarser than $\mathcal{T}_{\mathbb{Q}}$. On the other hand, let $x \in \mathcal{P}_{\mathbb{Q}}$ and let $U(x) \in \mathcal{T}_{\mathbb{Q}}$ be an open neighbourhood of x. We may assume that $U(x) = \bigcap_{i=1}^{r} P_{F_i|\mathbb{Q}}(\sigma_i)$ for some finite Galois extensions $F_i|\mathbb{Q}$ and some $\sigma_i \in G(F_i|\mathbb{Q})$. Let $d = max\{|D(F_i|\mathbb{Q})|, i = 1, \ldots, r\}$ and let $V \in \widetilde{Cov}(d)$ be the unique open set containing x, and so $V \subseteq U(x)$. The neighbourhood of x induced by the entourage $V_{d'}$ with d' as above is

$$U_{d'}(x) = \begin{cases} V_{d'}(\tilde{\sigma}) \quad \cup \quad \displaystyle\bigcup_{\alpha \in R_{d'}(x)} V_{d'}(\alpha), & \text{if } x \text{ is unramified in all } F \in S_{d'}, \\ \displaystyle\bigcup_{\alpha \in R_{d'}(x)} V_{d'}(\alpha), & \text{otherwise.} \end{cases}$$

where $R_{d'}(x) = \{\alpha \in R_d \,|\, x \in V_{d'}(\alpha)\}$ and $\tilde{\sigma}$ is given by the condition that $x \in V_{d'}(\tilde{\sigma})$. Since the covering $Cov^{\,o}(d')$ is a refinement of $\widetilde{Cov}(d)$, we obtain that $U_{d'}(x) \subseteq V \subseteq U(x)$. Thus the topology induced by $\mathfrak{U}_{\mathbb{Q}}^D$ is finer than $\mathcal{T}_{\mathbb{Q}}$. This proves the proposition. □

Obviously, $\mathfrak{U}_{\mathbb{Q}}^D$ is coarser than $\mathfrak{U}_{\mathbb{Q}} = \mathfrak{U}_{\mathbb{Q}}^o$ (and it seems unlikely that they are equal), but this uniformity defines a nice metric on $\mathcal{P}_{\mathbb{Q}}$.

Theorem 4.2. *The map*

$$\delta : \mathcal{P}_{\mathbb{Q}} \times \mathcal{P}_{\mathbb{Q}} \longrightarrow [0,1]\,, \quad (x,y) \mapsto \delta(x,y) = \frac{1}{n}\,,$$

where

$$n = \sup\{\, d \,|\, (x,y) \in V_d\},$$

defines an ultra-metric on $\mathcal{P}_{\mathbb{Q}}$ which induces the uniformity $\mathfrak{U}_{\mathbb{Q}}^D$.

Corollary 4.3. *The completion $(\hat{\mathcal{P}}_{\mathbb{Q}}, \hat{\mathfrak{U}}_{\mathbb{Q}}^D)$ of $(\mathcal{P}_{\mathbb{Q}}, \mathfrak{U}_{\mathbb{Q}}^D)$ is a profinite space.*

Proof: Obviously, δ is symmetric, $\delta(x,x)=0$, $\delta(x,y)\le\max(\delta(x,z),\delta(z,y))$ for x, y, $z\in\mathcal{P}_{\mathbb{Q}}$ and the (quasi-)metric δ induces the uniformity $\mathfrak{U}_{\mathbb{Q}}^D$. Since $\mathcal{T}_{\mathbb{Q}}$ is a Hausdorff topology, δ is an (ultra-)metric.

Since $\mathfrak{U}_{\mathbb{Q}}^D$ is coarser than $\mathfrak{U}_{\mathbb{Q}}$, we get a surjection $(\hat{\mathcal{P}}_{\mathbb{Q}},\hat{\mathfrak{U}}_{\mathbb{Q}})\twoheadrightarrow(\hat{\mathcal{P}}_{\mathbb{Q}},\hat{\mathfrak{U}}_{\mathbb{Q}}^D)$ and so $(\hat{\mathcal{P}}_{\mathbb{Q}},\hat{\mathfrak{U}}_{\mathbb{Q}}^D)$ is compact. Furthermore, the extension of δ to $(\hat{\mathcal{P}}_{\mathbb{Q}},\hat{\mathfrak{U}}_{\mathbb{Q}}^D)$ is also an ultra-metric and so the completion is totally disconnected. □

Remarks: 1. Analogously one can define a uniformity $\mathfrak{U}_K^D$ on $(\mathcal{P}_K,\mathcal{T}_K)$ and a corresponding metric having the properties stated in 4.1, 4.2 and 4.3.

2. It is obvious that the metric δ is not easily to calculate (at least if $d>21$ when not only quadratic fields are involved). But we do some calculations for $d\le 5$. We have three non-trivial extensions $F|\mathbb{Q}$ with absolute discriminant $|D(F|\mathbb{Q})|\le 5$: $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{5})$. Now we use the notation $(a|\gamma)$ for $P_{\mathbb{Q}(\sqrt{a})|\mathbb{Q}}(\gamma)$, $\gamma\in G(\mathbb{Q}(\sqrt{a})|\mathbb{Q})$, and we denote the non-trivial element of $G(\mathbb{Q}(\sqrt{a})|\mathbb{Q})$ by -1. Then $V_3=\mathcal{P}_{\mathbb{Q}}\times\mathcal{P}_{\mathbb{Q}}$, for V_4 we have to use the covering $\Big((-3|-1)\cap(-1|\,1)\Big)\cup(-3|\,1)\cup(-1|-1)$ of $\mathcal{P}_{\mathbb{Q}}$ and for V_5 the covering

$$\begin{aligned}\mathcal{P}_{\mathbb{Q}} \;=\;& \Big((-3|\,1)\cap(-1|\,1)\cap(5|-1)\Big)\cup\Big((-3|-1)\cap(-1|-1)\cap(5|\,1)\Big)\\ &\cup\Big((-3|\,1)\cap(5|\,1)\Big)\cup\Big((-1|-1)\cap(5|-1)\Big)\cup\Big((-3|-1)\cap(-1|\,1)\Big).\end{aligned}$$

It follows that for prime numbers $x<y\le 19$

$$\begin{aligned}\delta(x,y) &= \tfrac{1}{4}\text{, if } (x,y)=(2,7),\,(2,13),\,(3,11),\,(3,19),\,(7,11),\,(7,13),\,(7,19),\\ &\qquad\qquad (11,19),\,(13,19),\\ \delta(x,y) &\le \tfrac{1}{5}\text{, if } (x,y)=(2,19),\,(3,7),\,(5,17),\end{aligned}$$

and for all other pairs we have $\delta(x,y)=\frac{1}{3}$.

References

[1] A. V. Arhangel'skii, General Topology III. Encyclopaedia of Math. Sciences Vol. 51, Springer 1995.
[2] N. Bourbaki, General Topology, Hermann 1966.
[3] J. Neukirch, Algebraic Number Theory, Springer 1999.
[4] J. Neukirch, A. Schmidt, and K. Wingberg, Cohomology of Number Fields, Springer 2000.

Mathematisches Institut, der Universität Heidelberg, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany
E-mail address: wingberg@mathi.uni-heidelberg.de