# On Čebotarev Sets

By

Moshe Jarden*)

The aim of this note is to give a positive answer to a question raised by W. Jehne in a talk.

I am indebted to Professor Jehne for letting me use his notes from this talk.

Let $P$ be the set of the rational primes. Let $K$ be a finite normal extension of $\mathbb{Q}$. Then, the set $R(K) = \{p \in P \mid p \text{ is ramified in } K\}$ is finite. For every $p \in P - R(K)$ the Artin symbol $\left(\frac{K/\mathbb{Q}}{p}\right)$ is a conjugacy class in the Galois group $\mathcal{G}(K/\mathbb{Q})$.

Let now $\mathfrak{C}$ be a non empty conjugacy class in $\mathcal{G}(K/\mathbb{Q})$. Put

$$A(\mathfrak{C}) = \left\{p \in P - R(K) \,\Big|\, \left(\frac{K/\mathbb{Q}}{p}\right) = \mathfrak{C}\right\}.$$

$A(\mathfrak{C})$ is called a *Čebotarev set.* Čebotarev density theorem assures us that $A(\mathfrak{C})$ has a positive Dirichlet density and in particular that it is an infinite set.

If $L$ is a finite normal extension of $\mathbb{Q}$ which contains $K$ and

$$\mathfrak{C}' = \{\sigma \in \mathcal{G}(L/\mathbb{Q}) \mid \sigma | K \in \mathfrak{C}\}$$

then $\mathfrak{C}'$ can be decomposed into a disjoint union of conjugacy classes,

$$\mathfrak{C}' = \bigcup_{i=1}^{n} \mathfrak{C}'_i, \quad \text{and} \quad A(\mathfrak{C}) - R(L) = \bigcup_{i=1}^{n} A(\mathfrak{C}'_i).$$

Conversely, if $J$ is a finite normal extension of $\mathbb{Q}$ which is contained in $K$ and

$$\overline{\mathfrak{C}} = \{\sigma | J \mid \sigma \in \mathfrak{C}\}$$

then $\overline{\mathfrak{C}}$ is a conjugacy class in $\mathcal{G}(J/\mathbb{Q})$ and $A(\mathfrak{C}) \subseteqq A(\overline{\mathfrak{C}})$. The Theorem which we prove here shows that the lattice of all Čebotarev sets is small compared with the lattice of all subsets of $P$.

**Theorem.** *There exists a subset $A$ of $P$ such that $A \cap C$ and $(P - A) \cap C$ are infinite sets for every Čebotarev set $C$.*

---

*) This paper was written while the author attended the University of Heidelberg.

Proof. Let $\mathbb{Q} = K_1 \subset K_2 \subset K_3 \subset \dots$ be an increasing sequence of finite normal extensions of $\mathbb{Q}$ such that $\tilde{\mathbb{Q}} = \bigcup_{n=1}^{\infty} K_n$. For every $n \geqq 1$ let

$$\mathcal{G}(K_n/\mathbb{Q}) = \bigcup_{i \in I(n)} \mathfrak{C}_{n,i}$$

be the disjoint decomposition of $\mathcal{G}(K_n/\mathbb{Q})$ into conjugacy classes and let $C_{n,i} = A(\mathfrak{C}_{n,i})$ be the corresponding Čebotarev sets. For every $n$ and for every $i \in I(n)$ there exists a unique subset $J \subseteqq I(n+1)$ such that

$$C_{n,i} - R(K_{n+1}) = \bigcup_{j \in J} C_{n+1,j}. \tag{1}$$

We define now for every $n$ and for every $i \in I(n)$ finite subsets $A_{n,i}$, $B_{n,i}$ of $P$ such that:

a) $A_{n,i}, B_{n,i} \subseteqq C_{n,i}$,

b) $A_{n,i} \cap B_{n,i} = \emptyset$,

c) $|A_{n,i}|, |B_{n,i}| \geqq n$,

d) If $J$ is the subset of $I(n+1)$ such that (1) holds then

$$A_{n,i} \cap C_{n+1,j} \subseteqq A_{n+1,j}$$

and

$$B_{n,i} \cap C_{n+1,j} \subseteqq B_{n+1,j} \quad \text{for every } j \in J.$$

We proceed by induction on $n$. For $n = 1$ $I(1) = \{1\}$ and $C_{1,1} = P$. Define

$$A_{1,1} = \{2\} \quad \text{and} \quad B_{1,1} = \{3\}.$$

Assume that $A_{m,i}$ and $B_{m,i}$ have already been defined for every $m \leqq n$ and for every $i \in I(m)$ and that they satisfy (a)—(d). Let $i \in I(n)$ and let $J$ be the subset of $I(n+1)$ for which (1) holds.

For every $j \in J$ $A_{n,i} \cap C_{n+1,j}$ and $B_{n,i} \cap C_{n+1,j}$ are certainly finite sets, wheras $C_{n+1,j}$ is infinite, since it is a Čebotarev set. We can therefore choose $2(n+1)$ distinct primes $p_1, \dots, p_{n+1}, q_1, \dots, q_{n+1}$ in $C_{n+1,j}$ which do not belong neither to $A_{n,i} \cap C_{n+1,j}$ nor to $B_{n,i} \cap C_{n+1,j}$. Define

$$A_{n+1,j} = (A_{n,i} \cap C_{n+1,j}) \cup \{p_1, \dots, p_{n+1}\},$$
$$B_{n+1,j} = (B_{n,i} \cap C_{n+1,j}) \cup \{q_1, \dots, q_{n+1}\}.$$

It is clear that the conditions (a)—(d) are still satisfied. Put now

$$A = \bigcup_{n=1}^{\infty} \bigcup_{i \in I(n)} A_{n,i}, \quad B = \bigcup_{n=1}^{\infty} \bigcup_{i \in I(n)} B_{n,i}.$$

Then $A \cap B = \emptyset$. Indeed assume that there exists a $p \in A \cap B$. Then there exists an $n$, an $i \in I(n)$, an $m$ and a $k \in I(m)$ such that $p \in A_{n,i} \cap B_{m,k}$. Without loss of generality assume that $n \leqq m$. Then $p \notin R(K_m)$ since $B_{m,k} \subseteqq C_{m,k}$.

If $m > n$, then $p \notin R(K_{n+1})$, since $K_{n+1} \subseteqq K_m$. Let $J$ be as in (1). Then there exists a $j \in J$ such that $p \in C_{n+1,j}$. It follows by (d) that $p \in A_{n+1,j}$. Proceeding in this way we see that one can assume that $m = n$. It follows that $p \in C_{n,i} \cap C_{n,k}$. Hence $i = k$, since otherwise $C_{n,i} \cap C_{n,k} = \emptyset$. But this means that $A_{n,i} \cap B_{n,i} \neq \emptyset$ which contradicts (b).

Secondly we claim that $A \cap C_{n,i}$ and $B \cap C_{n,i}$ are infinite sets for every $n$ and $i \in I(n)$. We prove it for example for $A \cap C_{n,i}$. Let $J \subseteq I(n+1)$ as in (1). Then $A_{n+1,j} \subseteq A \cap C_{n,i}$ for every $j \in J$. Proceeding inductively one can find for every $m \geqq n$ a $k \in I(m)$ such that $A_{m,j} \subseteq A \cap C_{n,i}$. Hence, by (c), $|A \cap C_{n,i}| \geqq m$ for every $m \geqq n$, i.e. $A \cap C_{n,i}$ is an infinite set.

Let now $C$ be an arbitrary Čebotarev set. Then there exists a finite normal extension $K$ of $\mathbb{Q}$ and there exists a conjugacy class $\mathfrak{C}$ in $\mathscr{G}(K/\mathbb{Q})$ such that $C = A(\mathfrak{C})$. Take an $n$ such that $K \subseteq K_n$, then there exists an $i \in I(n)$ such that $C_{n,i} \subseteq C$. Hence $A \cap C$ and $B \cap C$ are infinite sets. Since $B \subseteq P - A$, $(P - A) \cap C$ is also an infinite set.

**Corollary.** *There exists a subset $A$ of $P$ such that for every filter base $\mathfrak{B}$ which consists of Čebotarev sets only* (i.e. $\mathfrak{B}$ is a collection of Čebotarev sets such that $B_1 \cap B_2 \cap \cap \cdots \cap B_n$ is an infinite set for every $B_1, B_2, \ldots, B_n \in \mathfrak{B}$) *there exist two non principal ultra filter $\mathfrak{D}$, $\mathfrak{D}'$ of $P$ which contain $\mathfrak{B}$ such that $A \in \mathfrak{D}$ and $P - A \in \mathfrak{D}'$.*

Eingegangen am 8. 2. 1974

Anschrift des Autors:

M. Jarden
Department of Mathematical Sciences
Tel-Aviv University
Ramat-Aviv, Tel-Aviv, Israel