Galois Groups of Local and Global Type

by Kay Wingberg at Heidelberg

In this article we are considering the structure of the Galois group

$$G_S = G(k_S(p)|k)$$

of the maximal p-extension $k_S(p)$ of an algebraic number field k which is unramified outside a finite set S of primes of k. Here p is a prime number and we assume that S contains the set $\Sigma = S_\infty \cup S_p$ of archimedean primes and primes above p. More precisely, we are interested in the arithmetical question about the relation between the group G_S and its decomposition groups

$$G_\mathfrak{p} = G((k_S(p))_\mathfrak{p}|k_\mathfrak{p}) \subseteq G_S$$

with respect to the non-archimedean primes $\mathfrak{p} \in S$. [*)] If $\mathcal{G}_\mathfrak{p} = G(k_\mathfrak{p}(p)|k_\mathfrak{p})$ denotes the Galois group of the maximal p-extension $k_\mathfrak{p}(p)$ of the local field $k_\mathfrak{p}$, then $G_\mathfrak{p}$ is obviously a quotient of $\mathcal{G}_\mathfrak{p}$. In some (rare) cases it can happen that there exists a prime $\mathfrak{p} \in S$ such that $G_\mathfrak{p}$ is almost equal to G_S.

Definition. *G_S is of* **local type**, *if there exists a prime $\mathfrak{p} \in S$ such that $G_\mathfrak{p} = G_S$. G_S is* **potentially of local type**, *if an open subgroup of G_S is of local type, and otherwise G_S is called of* **global type**.

Furthermore, we say that G_S is **(potentially)** *of* **maximal local type**, *if G_S is (potentially) of local type with respect to some prime $\mathfrak{p} \in S$ and the natural map $\mathcal{G}_\mathfrak{p} \twoheadrightarrow G_\mathfrak{p}$ is bijective.*

In the first paragraph we will characterize the cases where G_S is of (maximal) local type in terms of invariants of the base field k. In the following sections we deal with the question whether the group G_S is a free pro-p-group or a Demuškin group, i.e. a Poincaré group of dimension 2. If k contains the group μ_p of p-th roots of unity, we will see that this only can happen if G_S is potentially of local type. In contrast to this, if $\mu_p \notin k$, then there are number fields k such that G_Σ is a free pro-p-group of global type. But it is not known whether there are Galois groups of global type being Demuškin groups.

[*)] Actually one should denote this group by $G_\mathfrak{P}$ where $\mathfrak{P}$ is an extension of $\mathfrak{p}$ to $k_S(p)$.

1 The group G_S

Let p be a prime number and let μ_p be the group of p-th roots of unity. For an algebraic number field k and a finite set S of primes of k containing $\Sigma = S_\infty \cup S_p$ we introduce the following notations:

S^f	the set of finite primes in S,
$S_{\mathbb{R}}$, $S_{\mathbb{C}}$	the set of real and complex primes of k,
r_1, r_2	the number of real and complex primes of k,
$n_{\mathfrak{p}}$	the local degree $[k_{\mathfrak{p}} : \mathbb{Q}_\ell]$ of a non-archimedean prime $\mathfrak{p} \vert \ell$ of k,
$Cl_S(k)$	the S-ideal class group of k,
C_S	the S-idèle class group $C_S(k_S(p))$,
C_{S^f}	the S^f-idèle class group of $k_S(p)$,
G_S	the Galois group $G(k_S(p) \vert k)$ of the maximal p-extension $k_S(p)$ of k which is unramified outside S,
$G_{\mathfrak{p}}$	the decomposition group of G_S with respect to the prime $\mathfrak{p}$,
$T_{\mathfrak{p}}$	the inertia subgroup of $G_{\mathfrak{p}}$,
$\mathcal{G}_{\mathfrak{p}}$	the full local group $G(k_{\mathfrak{p}}(p) \vert k_{\mathfrak{p}})$,
$\mathcal{T}_{\mathfrak{p}}$	the inertia subgroup of $\mathcal{G}_{\mathfrak{p}}$,
$\mathrm{tor}_p A$	the p-torsion subgroup of an abelian group A.

Furthermore we set

$$\delta = \begin{cases} 1, & \mu_p \subseteq k, \\ 0, & \mu_p \nsubseteq k \end{cases} \qquad \text{and} \qquad \delta_{\mathfrak{p}} = \begin{cases} 1, & \mu_p \subseteq k_{\mathfrak{p}}, \\ 0, & \mu_p \nsubseteq k_{\mathfrak{p}}, \end{cases}$$

where $\mathfrak{p}$ is a prime of k. Assume that we are given a subset $S_0 \subseteq S$, then we put

$$V_{S_0}^S = \{a \in k^\times \mid a \in k_{\mathfrak{p}}^{\times p} \text{ for } \mathfrak{p} \in S_0;\ a \in U_{\mathfrak{p}} k_{\mathfrak{p}}^{\times p} \text{ for } \mathfrak{p} \notin S\}/k^{\times p},$$

where $U_{\mathfrak{p}}$ is the unit group of the local field $k_{\mathfrak{p}}$ (by convention $U_{\mathfrak{p}} = k_{\mathfrak{p}}^\times$ if $\mathfrak{p}$ is archimedean). The dual group is denoted by $\text{Б}_{S_0}^S = \mathrm{Hom}(V_{S_0}^S, \mathbb{Z}/p\mathbb{Z})$.

Observe that we have canonical inclusions

$$V_S^S \subseteq V_{S_0}^{S_0} \subseteq V_{S_0}^S$$

and that

$$V_{S_0}^S = \ker\left(H^1(k_S \vert k, \mu_p) \longrightarrow \prod_{\mathfrak{p} \in S_0} H^1(k_{\mathfrak{p}}, \mu_p)\right).$$

where k_S is the maximal extension of k which is unramified outside S.

First we will see that the question whether G_S is of local or global type depends (i.g.) only on the decomposition groups $G_{\mathfrak{p}}$ for $\mathfrak{p} \vert p$.

Proposition 1.1. *For $\mathfrak{p}_0 \in S \smallsetminus S_p$ the canonical homomorphism*

$$\mathcal{G}_{\mathfrak{p}_0} \longrightarrow G_S$$

is injective. The image is not open, i.e. of infinite index in G_S, except in the following cases:
k is totally real, p is odd, $\sum_{S^f\setminus\{\mathfrak{p}_0\}} \delta_{\mathfrak{p}} = 0$, $\text{Б}_\Sigma^\Sigma = 0$ and
either $\delta_{\mathfrak{p}_0} = 0$ (then $G_S \cong \mathbb{Z}_p$)
or $\delta_{\mathfrak{p}_0} = 1$ and $\mathfrak{p}_0$ does not split in the cyclotomic $\mathbb{Z}_p$-extension k_∞ of k
(then $\mathcal{G}_{\mathfrak{p}_0} = G_S$ is a Demuškin group of rank 2).

Proof: By [1] th. 10.6.1 the map is injective and if k is not totally real, then the image is of infinite index in G_S. If $p = 2$, then $G_S(k)$ is potentially of local type with respect to $\mathfrak{p}_0$ if and only if $G_S(k(i))$ has this property. But this is impossible by the cited theorem. Now let p be odd and k totally real.

If $\delta_{\mathfrak{p}_0} = 0$, then $\mathcal{G}_{\mathfrak{p}_0} \cong \mathbb{Z}_p$ is open in G_S if and only if $G_S = G(k_\infty|k)$. But the last assertion is equivalent to $\sum_{S^f} \delta_{\mathfrak{p}} = 0$ and $\text{Б}_\Sigma^\Sigma = 0$.

If $\delta_{\mathfrak{p}_0} = 1$, then $\mathcal{G}_{\mathfrak{p}_0}$ is a Demuškin group of rank 2 and this group is open in G_S if and only if G_S has the same structure. Assuming this, it follows that G_Σ is isomorphic to $\mathbb{Z}_p$, thus $\sum_{S_p} \delta_{\mathfrak{p}} = 0$, $\text{Б}_\Sigma^\Sigma = 0$ and $G_\Sigma = G(k_\infty|k)$. From [1] th. 10.5.1 we obtain the exact sequence

$$1 \longrightarrow \mathop{\ast}_{\mathfrak{p}\in S^f(k_\infty)} \mathcal{T}_{\mathfrak{p}} \longrightarrow G_S \longrightarrow G_\Sigma \longrightarrow 1\,.$$

It follows that $\sum_{S^f\setminus\{\mathfrak{p}_0\}} \delta_{\mathfrak{p}} = 0$ and $\mathfrak{p}_0$ does not split in $k_\infty|k$.

Conversely, from the conditions given in the theorem it follows that $G_\Sigma = G(k_\infty|k)$ and that we have the exact sequence

$$1 \longrightarrow \mathcal{T}_{\mathfrak{p}_0} \longrightarrow G_S \longrightarrow G(k_\infty|k) \longrightarrow 1\,,$$

which shows that G_S is equal to the Demuškin group $\mathcal{G}_{\mathfrak{p}_0}$, since $\mathfrak{p}_0$ does not split in $k_\infty|k$. This completes the proof of the theorem. □

Remark: $k = \mathbb{Q}$, $p = 3$, $S = \{3, 7, \infty\}$ gives an example for the exceptional case with $\delta_7 = 1$. In this situation we have $G_S = G_7$.

Furthermore we want to mention that in the case $p \neq 2$ and k totally imaginary G_S is potentially of local type if and only if it is of local type. More generally we have by [1] th. 10.6.2

Proposition 1.2. *Let k be totally imaginary and let $\mathfrak{p} \in S$. Suppose that $G_{\mathfrak{p}}$ is open in G_S. Then $\mathfrak{p} \in S_p$ and either*

$$G_{\mathfrak{p}} = G_S \quad \textit{or} \quad p = 2 \textit{ and } (G_S : G_{\mathfrak{p}}) = 2,\ \#S^f(k) = 1,\ S^f(k_S(2)) = 2.$$

If the base field k contains the group μ_p, then we have the following assertion concerning the structure of G_S, see [2] or [1] ch.X §7 and ch.III §4 for the notion of a (virtual) duality group.

Theorem 1.3. *If $\mu_p \subseteq k$, then the group G_S is of one of the following forms.*

(i) *If $\text{Б}^S_{\{\mathfrak{p}_0\}} = 0$ for a prime $\mathfrak{p}_0 \in S^f$, then G_S is of local type and it exists a finite set of primes $T \supseteq S$, such that the canonical homomorphism*

$$\mathop{\ast}_{\mathfrak{p}\in S\setminus\{\mathfrak{p}_0\}} \mathcal{G}_\mathfrak{p} \ast \mathop{\ast}_{\mathfrak{p}\in T\setminus S} \mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p} \longrightarrow G_S$$

is an isomorphism.

(ii) *Assume $\text{Б}^S_{\{\mathfrak{p}\}} \neq 0$ for all primes $\mathfrak{p} \in S^f$.*
If $p \neq 2$, then G_S is of global type and it is a duality group of dimension 2 with dualizing module $\mathrm{tor}_p C_{S^f}$.
For $p = 2$ the following cases occur:
If $\# S^f(k_S(2)) > 2$, then G_S is of global type and it is a virtual duality group of dimension 2 with dualizing module $\mathrm{tor}_2 C_{S^f}$.
If $\# S^f(k_S(2)) = 2$, then G_S is potentially of maximal local type and it is a virtual Poincaré group of dimension 2 with dualizing module μ_{2^∞}.

Remarks: 1. In (i) the prime $\mathfrak{p}_0$ is unique but the set T is not.
2. We use the opportunity here to mention that the corollary to theorem A in [2] is only correct if we assume that $\mu_{2p} \subseteq k$ (see below). Furthermore, there is a mistake in the subsequent paper to [2] which appeared in J. reine u. angew. Math. 416 (1991). The question whether G_S is a duality group in the case that $\mu_p \notin k$ remains open.

The theorem above gives us a complete characterization for G_S to be (potentially) of local or global type if $\mu_p \subseteq k$. Without this assumption we at least can describe the situation when G_S is a free product of (full) decomposition groups and a free group (see [2] th. 6).

Theorem 1.4. *For a subset $S_0 \subseteq S^f$ the following assertions are equivalent.*

(i) *It exists a finite set of primes $T \supseteq S$, such that the canonical homomorphism*

$$\mathop{\ast}_{\mathfrak{p}\in S\setminus S_0} \mathcal{G}_\mathfrak{p} \ast \mathop{\ast}_{\mathfrak{p}\in T\setminus S} \mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p} \longrightarrow G_S$$

is an isomorphism.

(ii) $\text{Б}^S_{S_0} = 0$ *and* $\displaystyle\sum_{\mathfrak{p}\in S_0} \delta_\mathfrak{p} = \delta$.

If $\mu_p \subseteq k$, then (i) *and* (ii) *are equivalent to*

(ii)' $S_0 = \{\mathfrak{p}_0\}$ *and* $G_{\mathfrak{p}_0} = G_S$.

Furthermore, if (i) *and* (ii) *hold, then*

$$\#(T\backslash S) = 1 + \sum_{\mathfrak{p}\in S_0\cap S_p} [k_\mathfrak{p} : \mathbb{Q}_p] - \#(S\backslash S_0).$$

Corollary 1.5. *The group G_S is of maximal local type if and only if k is totally imaginary if $p = 2$ and there exists a prime $\mathfrak{p}_0 \in S^f$ such that*

$$\sum_{S^f\backslash\{\mathfrak{p}_0\}} \delta_\mathfrak{p} = \delta\,, \quad \text{Б}^S_{S\backslash\{\mathfrak{p}_0\}} = 0 \quad \textit{and} \quad r_2 = \begin{cases} n_{\mathfrak{p}_0}, & \mathfrak{p}_0 \,|\, p\,, \\ 0, & \mathfrak{p}_0 \nmid p\,. \end{cases}$$

Proof: We have $\mathcal{G}_{\mathfrak{p}_0} \xrightarrow{\sim} G_S$ if and only if in (i) of the theorem above $S\backslash S_0 = \{\mathfrak{p}_0\}$ and $\#(T\backslash S) = 0$. Thus $S_0 = S^f\backslash\{\mathfrak{p}_0\}$ and k has to be totally imaginary if $p = 2$. Furthermore, the assertion $\#(T\backslash S) = 0$ is now equivalent to

$$\#(S\backslash S_0) = r_1 + r_2 + 1 = 1 + \sum_{\mathfrak{p}\in S_p\backslash\{\mathfrak{p}_0\}} n_\mathfrak{p} = 1 + r_1 + 2r_2 - \begin{cases} n_{\mathfrak{p}_0}, & \mathfrak{p}_0 \,|\, p\,, \\ 0, & \mathfrak{p}_0 \nmid p\,. \end{cases}$$

Finally, for $p \neq 2$ or k totally imaginary we have $\text{Б}^S_{S^f\backslash\{\mathfrak{p}_0\}} = \text{Б}^S_{S\backslash\{\mathfrak{p}_0\}}$. □

Now we give a characterization for G_S being of local type.

Theorem 1.6. *The group G_S is of local type if and only if there exists a prime $\mathfrak{p}_0 \in S^f$ such that*

$$\sum_{S^f\backslash\{\mathfrak{p}_0\}} \delta_\mathfrak{p} - \delta + \dim_{\mathbb{F}_p} \text{Б}^S_{S\backslash\{\mathfrak{p}_0\}} + r_2 = \begin{cases} n_{\mathfrak{p}_0}, & \mathfrak{p}_0 \,|\, p\,, \\ 0, & \mathfrak{p}_0 \nmid p\,. \end{cases}$$

Proof: Let $\mathfrak{p}_0$ be a prime of S^f. Consider the following commutative and exact diagram

$$\begin{tikzcd}
 & & & 0 \arrow[d] & & & \\
 & & & \prod\limits_{S\backslash\{\mathfrak{p}_0\}} H^1(\mathcal{G}_\mathfrak{p}) \arrow[r, "\sim"] \arrow[d] & \prod\limits_{S\backslash\{\mathfrak{p}_0\}} H^1(k_\mathfrak{p}, \mu_p)^* \arrow[d] & & \\
0 \arrow[r] & (Cl_S/p)^* \arrow[r] & H^1(G_S) \arrow[r, "res"] \arrow[d, equal] & \prod\limits_S H^1(\mathcal{G}_\mathfrak{p}) \arrow[r] \arrow[d] & H^1(k_S|k, \mu_p)^* \arrow[r] \arrow[d] & \text{Б}^S_S \arrow[r] & 0 \\
0 \arrow[r] & \ker(res_{\,\mathfrak{p}_0}) \arrow[r] & H^1(G_S) \arrow[r, "res_{\,\mathfrak{p}_0}"] & H^1(\mathcal{G}_{\mathfrak{p}_0}) \arrow[d] & \text{Б}^S_{S\backslash\{\mathfrak{p}_0\}} \arrow[d] & & \\
 & & & 0 & 0 & &
\end{tikzcd}$$

where the missing coefficients of the cohomology groups are $\mathbb{Z}/p\mathbb{Z}$ and the horizontal sequence in the middle is obtained from the global duality theorem of Tate/Poitou, see [1] ch.VIII §7. The snake lemma implies the exact sequences

$$(Cl_S/p)^* \hookrightarrow \ker(res_{\,\mathfrak{p}_0}) \to \prod_{S\setminus\{\mathfrak{p}_0\}} H^1(\mathcal{G}_\mathfrak{p}) \to \mathrm{coker}(res\,) \twoheadrightarrow \mathrm{coker}(res_{\,\mathfrak{p}_0})\,,$$

$$0 \longrightarrow \mathrm{coker}(res\,) \to H^1(k_S|k,\mu_p)^* \to \text{Б}^S_S \longrightarrow 0\,,$$

$$0 \longrightarrow \mathrm{coker}(res_{\,\mathfrak{p}_0}) \longrightarrow \text{Б}^S_{S\setminus\{\mathfrak{p}_0\}} \longrightarrow \text{Б}^S_S \longrightarrow 0\,.$$

Since

$$\dim_{\mathbb{F}_p} H^1(k_S|k,\mu_p) = \dim_{\mathbb{F}_p} \mathcal{O}_S^\times/p + \dim_{\mathbb{F}_p} {}_pCl_S = \#S - 1 + \delta + \dim_{\mathbb{F}_p} Cl_S/p$$

and

$$\dim_{\mathbb{F}_p} H^1(\mathcal{G}_\mathfrak{p}) = 1 + \delta_\mathfrak{p} + \begin{cases} n_\mathfrak{p}, & \mathfrak{p} \mid p\,, \\ 0, & \mathfrak{p} \nmid p\,, \end{cases}$$

we obtain counting dimensions

$$\dim_{\mathbb{F}_p} \ker(res_{\,\mathfrak{p}_0}) = \sum_{S\setminus\{\mathfrak{p}_0\}} \delta_\mathfrak{p} - \delta + \dim_{\mathbb{F}_p} \text{Б}^S_{S\setminus\{\mathfrak{p}_0\}} - \begin{cases} n_{\mathfrak{p}_0}, & \mathfrak{p}_0 \mid p\,, \\ 0, & \mathfrak{p}_0 \nmid p\,. \end{cases}$$

Now G_S is of local type if and only if there exists a prime $\mathfrak{p}_0 \in S^f$ such that $\ker(res_{\,\mathfrak{p}_0}) = 0$. This proves the theorem. □

If k is not totally real and G_S is of global type, then we will see that the decomposition groups $G_\mathfrak{p}(K)$, $\mathfrak{p} \in S(K)$, can not generate the whole group $G_S(K)$ for every finite extension $K|k$ inside $k_S(p)$. Even more is true:

Theorem 1.7. *Assume that k is not totally real and that G_S is of global type. If $d \in \mathbb{N}$ is given, then there exists a finite Galois extension K of k inside $k_S(p)$ such that*

$$\dim_{\mathbb{F}_p} Cl_S(K)/p \geq d\,.$$

Proof: Let $K|k$ be a finite Galois extension inside $k_S(p)$. We put $G = G_S(K)$ and $G_\mathfrak{p} = G_\mathfrak{p}(K)$ for short and denote the Frattini subgroup of G by G^*. From the Hochschild-Serre spectral sequence

$$0 \longrightarrow H^1(G/G^*) \xrightarrow{\sim} H^1(G) \longrightarrow H^1(G^*)^G \longrightarrow H^2(G/G^*) \longrightarrow H^2(G)$$

with coefficients $\mathbb{Z}/p\mathbb{Z}$ we obtain with $h^i = \dim_{\mathbb{F}_p} H^i(G)$

$$\begin{aligned}
\dim_{\mathbb{F}_p} H^1(G^*)^G &\geq \dim_{\mathbb{F}_p} H^2(G/G^*) - \dim_{\mathbb{F}_p} H^2(G) \\
&= \tfrac{1}{2}h^1(h^1+1) - h^2 \\
&\geq \tfrac{1}{2}h^1(h^1-1) \\
&\geq \tfrac{1}{2}(r_2)^2
\end{aligned}$$

where we used the Künneth formula for the p-elementary abelian group G/G^*. Furthermore we have the exact sequence

$$0 \longrightarrow \mathrm{Hom}(Cl_S(K'), \mathbb{Z}/p\mathbb{Z})^G \longrightarrow H^1(G^*)^G \longrightarrow \prod_{\mathfrak{p}\in S(K)} H^1(G^* \cap G_{\mathfrak{p}})^{G_{\mathfrak{p}}}$$

where K' is the fixed field of G^*. Obviously

$$\dim_{\mathbb{F}_p} H^1(G^* \cap G_{\mathfrak{p}})^{G_{\mathfrak{p}}} = 1 + \delta_{\mathfrak{p}}$$

for the finite primes $\mathfrak{p} \nmid p$. In order to calculate the dimensions of the local terms for $\mathfrak{p}|p$ we consider the exact sequence

$$0 \longrightarrow H^1((G^* \cap G_{\mathfrak{p}})/G^*_{\mathfrak{p}}) \longrightarrow H^1(G^* \cap G_{\mathfrak{p}})^{G_{\mathfrak{p}}} \longrightarrow H^1(G^*_{\mathfrak{p}})^{G_{\mathfrak{p}}}$$

which gives us with $h_{\mathfrak{p}} = \dim_{\mathbb{F}_p} H^1(G_{\mathfrak{p}}) \leq n_{\mathfrak{p}} + 2$

$$\begin{aligned}
\dim_{\mathbb{F}_p} H^1(G^* \cap G_{\mathfrak{p}})^{G_{\mathfrak{p}}} &\leq \dim_{\mathbb{F}_p} H^1((G^* \cap G_{\mathfrak{p}})/G^*_{\mathfrak{p}}) + \dim_{\mathbb{F}_p} H^1(G^*_{\mathfrak{p}})^{G_{\mathfrak{p}}} \\
&\leq \dim_{\mathbb{F}_p} H^1(G_{\mathfrak{p}}/G^*_{\mathfrak{p}}) + \dim_{\mathbb{F}_p} H^1(G^*_{\mathfrak{p}})^{G_{\mathfrak{p}}} \\
&\leq \dim_{\mathbb{F}_p} H^1(G_{\mathfrak{p}}) + \dim_{\mathbb{F}_p} H^2(G_{\mathfrak{p}}/G^*_{\mathfrak{p}}) \\
&= h_{\mathfrak{p}} + \tfrac{1}{2}h_{\mathfrak{p}}(h_{\mathfrak{p}}+1) \\
&\leq \tfrac{1}{2}(n_{\mathfrak{p}}+2)(n_{\mathfrak{p}}+5)\,.
\end{aligned}$$

It follows that

$$\begin{aligned}
\dim_{\mathbb{F}_p} Cl_S(K')/p &\geq \dim_{\mathbb{F}_p} \mathrm{Hom}(Cl_S(K'), \mathbb{Z}/p\mathbb{Z})^G \\
&\geq \tfrac{1}{2}(r_2(K))^2 - \sum_{\mathfrak{p}\in S^f\setminus S_p(K)} (1+\delta_{\mathfrak{p}}) - \sum_{\mathfrak{p}\in S_p(K)} \tfrac{1}{2}(n_{\mathfrak{p}}(K)+2)(n_{\mathfrak{p}}(K)+5) \\
&\geq \tfrac{1}{2}(r_2(K))^2 - \sum_{\mathfrak{p}\in S_p(K)} \tfrac{1}{2}(n_{\mathfrak{p}}(K))^2 - c(K)
\end{aligned}$$

where $c(K) = \sum_{S^f \setminus S_p(K)}(1+\delta_{\mathfrak{p}}) + \sum_{S_p(K)} \frac{7}{2} n_{\mathfrak{p}}(K) + 5$. If $L|K$ is a finite extension inside $k_S(p)$, then $c(L) \leq [L:K]c(K)$. Therefore, since k is not totally real, there exists a finite extension $K|k$ inside $k_S(p)$ such that for the maximal p-elementary abelian extension K' of K inside $k_S(p)$ the inequality

$$\dim_{\mathbb{F}_p} Cl_S(K')/p \quad \geq \quad \tfrac{1}{4}(r_2(K))^2 - \sum_{\mathfrak{p}\in S_p(K)} \tfrac{1}{2}(n_{\mathfrak{p}}(K))^2 \,.$$

holds (and we have this inequality for all finite extensions of K inside $k_S(p)$). Since G_S is of global type, the decomposition groups $G_{\mathfrak{p}}$ for $\mathfrak{p}|p$ are of infinite index in G_S. Therefore, for every $m \in \mathbb{N}$ and every prime $\mathfrak{p}|p$ of K there exists an extension inside $k_S(p)$ in which $\mathfrak{p}$ decomposes in at least m primes. The normal closure L of the compositum of all these fields has the property that every prime $\mathfrak{p}|p$ of K has at least m extensions. It follows for the maximal p-elementary extension L' of L inside $k_S(p)$ that

$$\begin{aligned}
\dim_{\mathbb{F}_p} Cl_S(L')/p \quad &\geq \quad \tfrac{1}{4}(r_2(L))^2 - \sum_{\mathfrak{p}\in S_p(L)} \tfrac{1}{2}(n_{\mathfrak{p}}(L))^2 \\
&= \quad \tfrac{[L:K]^2}{4}(r_2(K))^2 - \tfrac{1}{2} \sum_{\mathfrak{p}\in S_p(K)} \sum_{\mathfrak{P}|\mathfrak{p}} [L_{\mathfrak{P}} : K_{\mathfrak{p}}]^2 (n_{\mathfrak{p}}(K))^2 \\
&\geq \quad \tfrac{[L:K]^2}{4}(r_2(K))^2 - \tfrac{1}{2} \sum_{\mathfrak{p}\in S_p(K)} \tfrac{[L:K]^2}{m}(n_{\mathfrak{p}}(K))^2 \\
&= \quad \tfrac{[L:K]^2}{m^2} \cdot \Big(\tfrac{m^2}{4}(r_2(K))^2 - \tfrac{m}{2} \sum_{\mathfrak{p}\in S_p(K)} (n_{\mathfrak{p}}(K))^2 \Big) \,.
\end{aligned}$$

Since $[L:K] \geq m$ and m can be chosen as large as one wants, the p-rank of the S-ideal class group of $L' = L'(m)$ exceeds every given bound. □

Together with proposition 1.2 the theorem above implies the

Corollary 1.8. *Assume that $p \neq 2$ and k is totally imaginary. Then G_S is of global type if and only if there exists a finite Galois extension K of k inside $k_S(p)$ such that $Cl_S(K)(p) \neq 0$.*

We do not know whether this is also true for number fields having real primes.

2 Free pro-p-groups

In this section we consider the case where G_S is a free pro-p-group. The following proposition is well known, see [1] th. 8.8.10:

Proposition 2.1. *G_S is free if and only if k is totally imaginary if $p = 2$ and*

$$\sum_{\mathfrak{p}\in S^f} \delta_{\mathfrak{p}} = \delta \quad \textit{and} \quad \text{Б}_S^S = 0 \,.$$

Therefore we assume in the following that k is totally imaginary if $p = 2$. Two cases occur

Corollary 2.2.

(i) *Assume there exists a prime $\mathfrak{p} \in S^f$ such that $\mu_p \subseteq k_{\mathfrak{p}}$. Then G_S is free if and only if $\mu_p \subseteq k$, $S^f = S_p = \{\mathfrak{p}\}$ and $B_S^S = 0$ (hence $Cl_S(p) = 0$).*

In particular, G_S is of local type in this case.

(ii) *Assume that $\mu_p \notin k_{\mathfrak{p}}$ for all $\mathfrak{p} \in S^f$. Then G_S is free if and only if $B_S^S = 0$.*

In the following we will show that in case (ii) of the corollary above the group G_S can be of local or of global type.

Let $k = \mathbb{Q}$ and $p \neq 2$. Then G_p surjects onto $G_\Sigma \cong \mathbb{Z}_p$. Hence this group is of local type.

It is more difficult to find an example where G_Σ is free and of global type. We need the following

Lemma 2.3. *Let p be an odd prime number, k a number field and let $S = \{\mathfrak{l}\} \cup \Sigma$, where $\mathfrak{l}$ is a non-archimedean prime of k not above p. Assume that*

$$\mu_p \notin k_{\mathfrak{p}} \ \text{ for all } \ \mathfrak{p}|p, \quad \mu_p \subseteq k_{\mathfrak{l}} \quad \text{and} \quad \text{Б}_\Sigma^S = 0\,.$$

Then there is an isomorphism

$$\mathcal{G}_{\mathfrak{l}}(k) * F_{r_2} \xrightarrow{\ \sim\ } G_S(k)\,,$$

where F_{r_2} is a free pro-p-group of rank $r_2 = r_2(k)$.

If $K|k$ is a Galois extension inside $k_S(p)$ of degree p which is ramified at $\mathfrak{l}$, then

$$\mathcal{G}_{\mathfrak{l}}(K) * F_{p\,r_2} \xrightarrow{\ \sim\ } G_S(K)$$

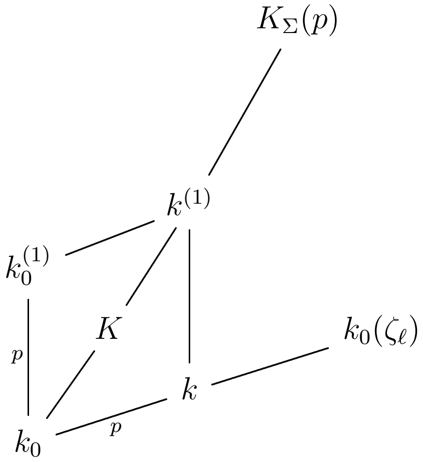
and

$$G_\Sigma(K) \xrightarrow{\ \sim\ } F_{p\,r_2+1}\,.$$

If in addition K is totally imaginary and $Cl_\Sigma(K)(p) \neq 0$, then $G_\Sigma(K)$ is free and of global type.

Proof: Using theorem 1.4 the assumptions imply the statement for $G_S(k)$. The subgroup theorem for free pro-p-product, see [1] th. 4.2.1, gives us the second assertion and the third follows by definition of the group $G_\Sigma(K)$. Finally, if $Cl_\Sigma(K)(p) \neq 0$, then the decomposition groups of $G_\Sigma(K)$ with respect to the primes above p have an index greater than 2. Hence $G_\Sigma(K)$ is of global type by proposition 1.2. □

Now we give an example of a number field for which we can apply lemma 2.3. Let $k_0 = \mathbb{Q}(i)$ and let p and ℓ be odd prime numbers such that $p \mid \ell - 1$. Let k be the unique subfield of $k_0(\zeta_\ell)$ of degree p over k_0. By $k_0^{(1)}$ and $k^{(1)}$ we denote the first layers of the cyclotomic $\mathbb{Z}_p$-extensions of k_0 and k, respectively. We have the following diagram of fields:



where K is some extension of k_0 inside $k^{(1)}$ of degree p and different to $k_0^{(1)}$ and k. Then K is totally imaginary and has the property that $\mu_p \notin K_\mathfrak{p}$ for $\mathfrak{p}|p$ and $\mu_p \subseteq K_\ell$.

Now we assume in addition that

$$p^2 \nmid \ell - 1, \quad \ell \text{ is inert in } k_0, \text{ i.e. } \ell \equiv 3 \mod 4, \quad \text{and } p^{\frac{\ell-1}{p}} \equiv 1 \mod \ell\,.$$

The prime numbers $p = 5$ and $\ell = 31$ give an example for this situation.

We will show that

$$Cl_\Sigma(K)(p) \neq 0 \quad \text{and} \quad \text{Б}_\Sigma^S(K) = 0\,.$$

In order to show the first assertion we first observe that the extension $k^{(1)}|K$ is at most ramified at the primes above p and above ℓ. Since ℓ is ramified in $k|k_0$ and unramified in $k_0^{(1)}|k_0$, the field $k_0^{(1)}$ is the inertia field for the extension $k^{(1)}|k_0$ with respect to ℓ. Hence $k^{(1)}|K$ is unramified at ℓ. With the same argumentation one sees that this extension is unramified at S_p, too: The extension $k^{(1)}|\mathbb{Q}$ is abelian and k is the inertia field of the extension $k^{(1)}|k_0$ with respect to the primes above p. From the assumption that $p^{\frac{\ell-1}{p}} \equiv 1 \bmod \ell$ follows that p decomposes in in the extension $\mathbb{Q}(\zeta_\ell)|\mathbb{Q}$ in d primes with $p|d$. Hence the primes above p decompose in the extension $k|k_0$ and therefore in the extension $k^{(1)}|K$, too. Thus $k^{(1)}|K$ is unramified and split at S_p. From class field theory follows that $Cl_\Sigma(K)(p) \neq 0$.

In order to prove the second assertion we first show that $V_\Sigma^S(k_0) = 0$. Since $Cl(k_0) = 0$ and the 4-th roots of unity form the group of units of k_0, an element of $V_\Sigma^S(k_0)$ is of the form $x = \ell^a \, k_0^{\times p}$, $a \in \mathbb{Z}$. Since $p^2 \nmid \ell - 1$, the element ℓ is not a p-power in $(k_0)_\mathfrak{p}$ for $\mathfrak{p}|p$. Hence $p|a$ and therefore $V_\Sigma^S(k_0) = 0$.

Finally, with $G = G(K|k_0)$ the commutative and exact diagram

$$\begin{tikzcd}
0 \arrow[r] & V_\Sigma^S(k_0) \arrow[r] \arrow[d] & H^1(\mathcal{G}_S(k_0), \mu_p) \arrow[r] \arrow[d, "\wr"] & \prod\limits_{\mathfrak{p} \in \Sigma(k_0)} H^1(\mathcal{G}_\mathfrak{p}(k_0), \mu_p) \arrow[d, "\wr"] \\
0 \arrow[r] & (V_\Sigma^S(K))^G \arrow[r] & H^1(\mathcal{G}_S(K), \mu_p)^G \arrow[r] & \Big(\prod\limits_{\mathfrak{p} \in \Sigma(K)} H^1(\mathcal{G}_\mathfrak{p}(K), \mu_p)\Big)^G
\end{tikzcd}$$

shows that $(V_\Sigma^S(K))^G \cong V_\Sigma^S(k_0) = 0$, hence $V_\Sigma^S(K) = 0$ and therefore $\text{Б}_\Sigma^S(K) = 0$.

3 Demuškin groups

In this paragraph we want to classify number fields k and sets of primes S (containing Σ) such that G_S is a Demuškin group.

Proposition 3.1. *If G_S is a Demuškin group, then either*

$$\text{Б}_S^S = 0 \quad \textit{and} \quad \sum_{\mathfrak{p} \in S \setminus S_\mathbb{C}} \delta_\mathfrak{p} - \delta = 1 \,,$$

or

$$\dim_{\mathbb{F}_p} \text{Б}_S^S = 1 \quad \textit{and} \quad \sum_{\mathfrak{p} \in S \setminus S_\mathbb{C}} \delta_\mathfrak{p} - \delta = 0 \,.$$

Proof: This is clear, since a Demuškin group is a one relator group, i.e. $\dim_{\mathbb{F}_p} H^2(G_S, \mathbb{Z}/p\mathbb{Z}) = 1$, see [1] cor. 8.8.9. □

By the proposition above k must be totally imaginary if $p = 2$ and G_S is a Demuškin group, since every open subgroup of G_S is again a Demuškin group. We will assume this in the following.

Theorem 3.2. *Let $p \neq 2$ and assume that $\mu_p \subseteq k$. Then the following assertions are equivalent:*

(i) *G_S is a Demuškin group.*

(ii) *G_S is a Demuškin group of maximal local type.*

(iii) *$S = \Sigma = S_\infty \cup \{\mathfrak{p}_1, \mathfrak{p}_2\}$, $\text{Б}_{\{\mathfrak{p}_1\}}^S = 0$ and $r_2 = n_{\mathfrak{p}_1}$.*

(iv) *$\# S^f(k_S(p)) = 2$.*

Let $p = 2$ and assume that k is totally imaginary. Then the following assertions are equivalent:

(i) *G_S is a Demuškin group.*

(ii) *G_S is a Demuškin group potentially of maximal local type.*

(iii) $S = \Sigma = S_\infty \cup \{\mathfrak{p}_1, \mathfrak{p}_2\}$, $\text{Б}^S_{\{\mathfrak{p}_1\}} = 0$ *and* $r_2 = n_{\mathfrak{p}_1}$ *or*
$S = \Sigma = S_\infty \cup \{\mathfrak{p}\}$ *and there exists a quadratic extension* $k'|k$ *in which* $\mathfrak{p}$ *splits, say* $\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2$ *such that* $\text{Б}^S_{\{\mathfrak{p}_1\}}(k') = 0$.

(iv) $\#S^f(k_S(2)) = 2$.

Proof: The assertion (iv) obviously implies that

$$\begin{aligned} &S = \Sigma = S_\infty \cup \{\mathfrak{p}_1, \mathfrak{p}_2\} \text{ and } \text{Б}^S_{\{\mathfrak{p}_1\}} = 0 = \text{Б}^S_{\{\mathfrak{p}_2\}} \quad \text{ or (if } p = 2) \\ &S = \Sigma = S_\infty \cup \{\mathfrak{p}\} \text{ and there exists a quadratic extension } k'|k \text{ in which } \mathfrak{p} \\ &\qquad\qquad\qquad \text{splits, say } \mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2 \text{ such that } \text{Б}^S_{\{\mathfrak{p}_1\}}(k') = 0 = \text{Б}^S_{\{\mathfrak{p}_2\}}(k')\,, \end{aligned}$$

since $\mu_p \subseteq k$ and by Kummer theory $\text{Б}^S_{\{\mathfrak{p}\}}$ is non-zero if and only if there exists a subextension of k in $k_S(p)$, in which $\mathfrak{p}$ splits.
Using theorem 1.4 these assertions imply for $G_S(k)$ (resp. for $G_S(k')$ in the second case) free product decompositions

$$G_{\mathfrak{p}_1} = G_S \cong \mathcal{G}_{\mathfrak{p}_2} * (\text{other terms}) \quad \text{and} \quad G_{\mathfrak{p}_2} = G_S \cong \mathcal{G}_{\mathfrak{p}_1} * (\text{other terms}).$$

But

$$\operatorname{rk} \mathcal{G}_{\mathfrak{p}_i} \geq \operatorname{rk} G_{\mathfrak{p}_i},\ i = 1, 2.$$

Hence the other terms are not present and $G_S = \mathcal{G}_{\mathfrak{p}_1} = \mathcal{G}_{\mathfrak{p}_2}$ and $r_2 = n_{\mathfrak{p}_1}$. Thus (iv) implies (iii).
Similar the assertion (iii) implies (ii): Using theorem 1.4 in the first case and the argument above in the second (if $p = 2$) we see that G_S is a Demuškin group of maximal local type in the first case and a virtual Demuškin group which is potentially of maximal local type in the second. But, since k is totally imaginary, G_S is torsion free and therefore it is itself a Demuškin group.
Obviously (ii) implies (i). Now we assume that G_S is a Demuškin group. The fact that $\operatorname{tor}_p C_{S^f}$ is the dualizing module of G_S, see [1] lemma 10.7.10, which has to be isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as abelian group, and the exact sequence

$$0 \longrightarrow \mu_{p^\infty} \longrightarrow \prod_{\mathfrak{p} \in S^f} \operatorname{Ind}_{G_\mathfrak{p}}^{G_S} \mu_{p^\infty} \longrightarrow \operatorname{tor}_p C_{S^f} \longrightarrow 0\,,$$

loc.cit. prop. 10.2.1, imply that $\#S^f(k_S(p)) = 2$. This finishes the proof of the theorem. □

The situation becomes not really more difficult if we drop the assumption that $\mu_p \subseteq k$ but assume that there exists a prime $\mathfrak{p}_0 \in S$ such that $\mu_p \subseteq k_{\mathfrak{p}_0}$.

Theorem 3.3. *Assume that $\mu_p \notin k$ and that there exists a prime $\mathfrak{p}_0 \in S$ such that $\mu_p \subseteq k_{\mathfrak{p}_0}$. Then the following assertions are equivalent:*

(i) *G_S is a Demuškin group.*

(ii) *G_S is a Demuškin group of local type.*

(iii) *$\mu_p \notin k_{\mathfrak{p}}$ for all primes $\mathfrak{p}$ in $S_0 := S^f \backslash \{\mathfrak{p}_0\}$,*

$$\text{Б}_S^S = 0 \quad \textit{and} \quad r_2 + \dim_{\mathbb{F}_p} \text{Б}_{S_0}^S = \begin{cases} n_{\mathfrak{p}_0}, & \mathfrak{p}_0 \mid p\,, \\ 0, & \mathfrak{p}_0 \nmid p\,. \end{cases}$$

Proof: Let G_S be a Demuškin group. Since $\mu_{p^\infty}(k_S(p)) = 0$, we have an injection

$$\mathrm{Ind}_{G_{\mathfrak{p}_0}}^{G_S} \mu_{p^\infty} \hookrightarrow \mathrm{tor}_p\, C_{S^f}$$

where $\mathrm{tor}_p\, C_{S^f}$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as abelian group, we obtain $G_S = G_{\mathfrak{p}_0}$, hence G_S is of local type.

From (ii) follows, since G_S is a Demuškin group,

$$1 = \dim_{\mathbb{F}_p} H^2(G_S, \mathbb{Z}/p\mathbb{Z}) = \dim_{\mathbb{F}_p} \text{Б}_S^S + \sum_{\mathfrak{p} \in S_0} \delta_{\mathfrak{p}} + 1$$

hence $\text{Б}_S^S = 0$ and $\mu_p \notin k_{\mathfrak{p}}$ for all primes $\mathfrak{p} \in S_0$. Since G_S is of local type we conclude by theorem 1.6 the last condition of (iii).

Now we assume (iii). Then G_S is a one relator group, i.e. $\dim_{\mathbb{F}_p} H^2(G_S, \mathbb{Z}/p\mathbb{Z}) = 1$. Furthermore, using again theorem 1.6, we obtain that G_S is of local type, i.e. $G_S = G_{\mathfrak{p}_0}$. Thus $\mathfrak{p}_0$ does not split in $k_S(p)|k$ and therefore

$$\dim_{\mathbb{F}_p} H^2(G_S(K), \mathbb{Z}/p\mathbb{Z}) = \dim_{\mathbb{F}_p} \text{Б}_S^S(K) + 1$$

for every finite Galois extension $K|k$ inside $k_S(p)$. Since $\text{Б}_S^S(K)^{G(K|k)} = \text{Б}_S^S(k)$ as $\mu_p \notin k$, it follows that $\dim_{\mathbb{F}_p} H^2(G_S(K), \mathbb{Z}/p\mathbb{Z}) = 1$. Now we obtain (i) from from the following lemma. □

Lemma 3.4. *Let G be a finitely generated pro-p-group of cohomological dimension equal to 2 such that*

$$\dim_{\mathbb{F}_p} H^2(N, \mathbb{Z}/p\mathbb{Z}) = 1$$

for every normal open subgroup N of G. Then G is a Demuškin group.

For a proof see [1] cor. 3.7.3. As an application of the last two theorems we now consider totally real fields and CM-fields $k|k^+$, i.e. k is totally imaginary and a quadratic extension of its maximal totally real subfield k^+.

Theorem 3.5. *Assume that k is totally real (and $p \neq 2$). Then G_S is a Demuškin group if and only if one of the following assertions hold:*

(i) *There exists a exactly one prime $\mathfrak{p}_0 \in S^f$ such that $\mu_p \subseteq k_{\mathfrak{p}_0}$. If $\mathfrak{p}_0 \nmid p$, then $\text{Б}^S_{S\setminus\{\mathfrak{p}_0\}} = 0$. If $\mathfrak{p}_0 | p$, then $\text{Б}^\Sigma_\Sigma = 0$ and $\dim_{\mathbb{F}_p} \text{Б}^\Sigma_{\Sigma\setminus\{\mathfrak{p}_0\}} = 1$.*

(ii) *For all primes $\mathfrak{p} \in S^f$ hold $\mu_p \notin k_\mathfrak{p}$ and $\dim_{\mathbb{F}_p} \text{Б}^\Sigma_\Sigma(k_n) = 1$ for all $n \in \mathbb{N}$, where k_n is the n-th layer of the cyclotomic $\mathbb{Z}_p$-extension k_∞ of k.*

Remarks: 1. In both cases G_S is not of global type, if we assume in the second case that the Greenberg conjecture holds, i.e. the maximal unramified abelian p-extension of the the cyclotomic $\mathbb{Z}_p$-extension k_∞ of k is finite.
2. In (ii) it is sufficient that $\dim_{\mathbb{F}_p} \text{Б}^\Sigma_\Sigma(k_n) = 1$ for one n which is large enough.
3. Equivalent to the statements in the theorem are the assertions that the Iwasawa λ-invariant of the $\mathbb{Z}_p[\![G(k_\infty|k)]\!]$-module $G(k_S|k_\infty)^{ab}$ is equal to 1 and its μ-invariant is zero.

Proof: If there exists a prime $\mathfrak{p}_0 \in S^f$ such that $\mu_p \subseteq k_{\mathfrak{p}_0}$, then it follows from theorem 3.3 that G_S is a Demuškin group (of local type) if and only if the conditions of (i) are fulfilled (see also proposition 1.1 for an equivalent description). Furthermore, in this case the dualizing module of G_S is equal to μ_{p^∞}, hence $G(k_\infty|k)$ acts non-trivially on $G(k_S(p)|k_\infty) \cong \mathbb{Z}_p(1)$ which shows the remark 3.

If $\mu_p \notin k_\mathfrak{p}$ for all primes $\mathfrak{p} \in S^f$, then $G_S = G_\Sigma$ and

$$\dim_{\mathbb{F}_p} H^2(G_\Sigma(k_n), \mathbb{Z}/p\mathbb{Z}) = \dim_{\mathbb{F}_p} \text{Б}^\Sigma_\Sigma(k_n)\,.$$

Thus, if G_S is a Demuškin group, then condition (ii) holds.

Conversely, from (ii) follows that $\dim_{\mathbb{F}_p} H^1(G_\Sigma(k_n), \mathbb{Z}/p\mathbb{Z}) = 2$ for all $n \geq 1$, hence the group $(G(k_\Sigma(p)|k_\infty)^{ab}/p)_{\Gamma_n}$ is generated by one element, where $\Gamma_n = G(k_\infty|k_n)$. Since $G(k_\Sigma(p)|k_\infty)^{ab}$ is a $\mathbb{Z}_p[\![\Gamma]\!]$-torsion module, there exists an n such that Γ_n acts trivially on $G(k_\Sigma(p)|k_\infty)^{ab}/p$. Therefore this group is generated by one element and it follows that the same is true for the group $G(k_\Sigma(p)|k_\infty)$. (For the Iwasawa theory we used here, see [1] ch.XI §3.) Thus G_Σ is a Demuškin group, loc.cit. th. 3.7.4. Also in this case G_Σ is (potentially) of local type, if we assume that the Greenberg conjecture holds, because then $G_\mathfrak{p}$ is of finite index in G_Σ. □

Examples:

1. Case (i), $\mathfrak{p}_0 \nmid p$: $p = 3$, $k = \mathbb{Q}$, $S = \{3, 7, \infty\}$.
Then $G_S(\mathbb{Q}) = G_7$.
$\mathfrak{p}_0 \mid p$: $p = 3$, $k = \mathbb{Q}(\sqrt{6})$, $S = \{3, \infty\}$.
Then $G_S(k)$ is a Demuškin group of rank 2.
2. Case (ii): $p = 37$, $k = \mathbb{Q}(\zeta_{37} + \zeta_{37}^{-1})$, $S = \{3, \infty\}$.
Then $G_S(k)$ is a Demuškin group of rank 2.

In the second example we have $\mu_3 \subseteq k_3$. The Iwasawa μ-invariant of $G(k_S(3)|k_\infty)^{ab}$ is zero by the theorem of Ferrero and Washington and its λ-invariant is equal to the λ-invariant of the maximal abelian unramified 3-extension of k'_∞, where $k' = \mathbb{Q}(\sqrt{-2})$. But this invariant is equal to 1.

Also in the third example the Iwasawa λ-invariant of $G(k_S(3)|k_\infty)^{ab}$ is equal to 1 and its μ-invariant is zero.

Since $G_S = G_{S'}$, where $S' = \{\mathfrak{p} \in S^f \backslash S_p \mid \mu_p \subseteq k_\mathfrak{p}\} \cup \Sigma \subseteq S$, we assume for the following theorem that $S = S'$.

Theorem 3.6. *Let $p \neq 2$ and let $k|k^+$ be a CM-field. Assume that there exists a prime $\mathfrak{p}_0 \in S^f$ such that $\mu_p \subseteq k_{\mathfrak{p}_0}$. Let $\tilde{\mathfrak{p}_0}$ be the underlying prime of $\mathfrak{p}_0$ of k^+.*

Then $G_S(k)$ is a Demuškin group if and only if the following conditions are fulfilled:

1. *$\#S^f(k) = 1 + \delta$ and $S^f(k^+) = \{\tilde{\mathfrak{p}_0}\}$,*
2. *$G_S(k^+)$ is a Demuškin group and $\mu_p \subseteq k^+_{\tilde{\mathfrak{p}_0}}$,*
3. *$Cl_S(k)^- = 0$.*

In this case G_S is of local type (with respect to the prime $\mathfrak{p}_0$ which lies over p) and of maximal local type, if $\mu_p \subseteq k$.

Proof: Let $G_S(k)$ be a Demuškin group. Then by the theorems 3.2 and 3.3 $G_S(k)$ is of local type with respect to $\mathfrak{p}_0$, which has to lie over p. Furthermore $\text{Б}^S_S(k) = 0$ and $\#S^f(k) = 1 + \delta$ (by our convention that S^f contains only relevant primes). Hence $\text{Б}^S_S(k^+) = 0$.

The action of $G(k|k^+)$ on the 1-dimensional $\mathbb{F}_p$-vector space $H^2(G_S(k), \mathbb{Z}/p\mathbb{Z})$ must be trivial. Indeed, otherwise $H^2(G_S(k^+), \mathbb{Z}/p\mathbb{Z}) = 0$ and therefore $G_S(k^+)$ would be isomorphic to $\mathbb{Z}_p$, since k^+ is totally real. Furthermore the subspaces $H^1(G_S(k), \mathbb{Z}/p\mathbb{Z})^\pm$ would be totally isotropic with respect to the nondegenerated pairing

$$H^1(G_S(k), \mathbb{Z}/p\mathbb{Z}) \times H^1(G_S(k), \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\cup} H^2(G_S(k), \mathbb{Z}/p\mathbb{Z}) .$$

It would follow that

$$r_2(k) + 2 = \dim_{\mathbb{F}_p} H^1(G_S(k), \mathbb{Z}/p\mathbb{Z}) = 2 \cdot \dim_{\mathbb{F}_p} H^1(G_S(k^+), \mathbb{Z}/p\mathbb{Z}) = 2$$

which is absurd. Thus $\dim_{\mathbb{F}_p} H^2(G_S(k^+), \mathbb{Z}/p\mathbb{Z}) = 1$.

Since this argument is true for all finite CM-extensions $K|K^+$ of $k|k^+$ inside $k_S(p)$, we obtain from 3.4 that $G_S(k^+)$ is a Demuškin group. Furthermore the equality $1 = \dim_{\mathbb{F}_p} H^2(G_S(k^+), \mathbb{Z}/p\mathbb{Z}) = \delta_{\tilde{\mathfrak{p}_0}}$ shows that $\mu_p \subseteq k_{\tilde{\mathfrak{p}_0}}$. Thus we obtain condition 2. Finally, condition 3 holds, because G_S is of local type.

Conversely, let us assume that the conditions 1 to 3 are fulfilled. First we consider the case that $\mu_p \subseteq k$. Let $\tilde{\mathfrak{p}_0} = \mathfrak{p}_1\mathfrak{p}_2$ in k by our assumption. Hence

$r_2 = n_{\mathfrak{p}_1} = n_{\mathfrak{p}_2}$ and $\sum_{\mathfrak{p}\in S^f\setminus\{\mathfrak{p}_1\}} \delta_{\mathfrak{p}} = \delta$. We will show that $\text{Б}^S_{S\setminus\{\mathfrak{p}_1\}} = 0$. Suppose the contrary. Then by Kummer theory there exists a Galois extension $K|k$ of degree p inside $k_S(p)$ in which $\mathfrak{p}_2$ decomposes. If this extension is Galois over k^+, then $\mathfrak{p}_1$ decomposes, too. Since $Cl_S(k)^- = 0$ by condition 3 and $Cl_S(k)^+ = 0$ by condition 2 and the remark 1 following theorem 3.5, we obtain a contradiction. Thus K is not Galois over k^+ and we denote by $\tilde{K}$ the normal closure of K over k^+, hence $G(\tilde{K}|k) \cong (\mathbb{Z}/p\mathbb{Z})^2$. Let $\tilde{K}^+$ be the fixed field of $G(\tilde{K}|k)^- \cong \mathbb{Z}/p\mathbb{Z}$. Since $Cl_S(k)^+ = 0$, both primes, $\mathfrak{p}_1$ and $\mathfrak{p}_2$, do not split in $\tilde{K}^+$, but each of them decomposes in p primes in $\tilde{K}$. Thus the extension $\tilde{K}|\tilde{K}^+$ is unramified and all primes of S_p split, hence $G(\tilde{K}|\tilde{K}^+) \cong Cl_S(k)^-$. Again we obtain a contradiction. This proves that $\text{Б}^S_{S\setminus\{\mathfrak{p}_1\}} = 0$.
It follows from theorem 1.5 that $G_S(k)$ is of maximal local type, i.e. $G_S(k) = \mathcal{G}_{\mathfrak{p}_1}(k) = \mathcal{G}_{\mathfrak{p}_2}(k)$ and therefore $G_S(k)$ is a Demuškin group.

Now let $\mu_p \notin k$. Since $\tilde{\mathfrak{p}_0}$ does not split in the extension $k|k^+$, the group $G(k|k^+)$ acts on $\mathcal{G}_{\mathfrak{p}_0}(k)^{ab}$. Using condition 3 we obtain the commutative diagram

$$\begin{tikzcd}
\mathcal{G}_{\mathfrak{p}_0}(k)^{ab-} \arrow[r, "\sim"] \arrow[d, hook] & G_S(k)^{ab-} \arrow[d, hook] \\
\mathcal{G}_{\mathfrak{p}_0}(k)^{ab} \arrow[r] \arrow[d, two heads] & G_S(k)^{ab} \arrow[d, two heads] \\
\mathcal{G}_{\mathfrak{p}_0}(k^+)^{ab} \arrow[r, two heads] & G_S(k^+)^{ab}
\end{tikzcd}$$

where the map at the bottom is surjective, since $G_S(k^+)$ is of local type by condition 2 and the remark 1 to theorem 3.5. Thus $G_S(k)$ is of local type. Since $H^2(G_S(k), \mathbb{Q}_p/\mathbb{Z}_p)^- = 0$ and $G_S(k)^{ab,-}$ is $\mathbb{Z}_p$-torsion free (because $\mu_p \subseteq k^+_{\mathfrak{p}_0}$ and $\mathcal{G}_{\mathfrak{p}_0}(k)^{ab-} \cong G_S(k)^{ab,-}$), we obtain $H^2(G_S(k), \mathbb{Z}/p\mathbb{Z})^- = 0$ and therefore $\dim_{\mathbb{F}_p} H^2(G_S(k), \mathbb{Z}/p\mathbb{Z}) = \dim_{\mathbb{F}_p} H^2(G_S(k^+), \mathbb{Z}/p\mathbb{Z}) = 1$ and $\text{Б}^S_S(k) = 0$.
Since $\mu_p \notin k$, it follows that $\text{Б}^S_S(K) = 0$ for all finite Galois extension $K|k$ inside $k_S(p)$, and since $G_S(k)$ is of local type, we have $\#S^f(K) = 1$. Thus $\dim_{\mathbb{F}_p} H^2(G_S(K), \mathbb{Z}/p\mathbb{Z}) = 1$ for all these extensions $K|k$. Now lemma 3.4 gives the desired result. □

Examples:
Case 1. $\mu_p \subseteq k$: $p = 3$, $k = \mathbb{Q}(\sqrt{6}, \sqrt{-3})$, $S = \{3, \infty\}$.
Then $G_S(k)$ is a Demuškin group of rank 4.
Case 2. $\mu_p \notin k$: $p = 3$, $k = \mathbb{Q}(\sqrt{6}, \sqrt{-1})$, $S = \{3, \infty\}$.
Then $G_S(k)$ is a Demuškin group of rank 4.
We know already that $G_S(k^+)$, where $k^+ = \mathbb{Q}(\sqrt{6})$, is a Demuškin group of rank equal to 2, see the examples for totally real fields. Furthermore we have $Cl_S(k)^- \cong Cl_S(\mathbb{Q}(\sqrt{-6})) \oplus Cl_S(\mathbb{Q}(\sqrt{d}))$, where $d = -3$ or $d = -1$ according to we are in case 1 or 2. Thus $Cl_S(k)^- = 0$.

It remains to classify number fields k and sets of primes S such that G_S is a Demuškin group, k is not totally real and $\mu_p \notin k_\mathfrak{p}$ for all primes $\mathfrak{p} \in S^f$. We do not know any example of this case. Moreover, does there exists a situation where G_S is a Demuškin group of global type? By the considerations above this can only happen in the just mentioned case.

References

[1] Neukirch, J., Schmidt, A., Wingberg, K. *Cohomology of Number Fields.* Springer 1999

[2] Wingberg, K. *On Galois groups of p-closed algebraic number fields with restricted ramification.* J. reine u. angew. Math. **400** (1989) 185-202

Mathematisches Institut
der Universität Heidelberg
Im Neuenheimer Feld 288
69120 Heidelberg
Germany

e-mail: wingberg@mathi.uni-heidelberg.de