Free pro-p extensions of number fields

by Kay Wingberg at Heidelberg

This paper concerns the problem of the existence of Galois extensions of algebraic number fields whose Galois groups are free pro-p groups. Let k be an algebraic number field and

$$F = G(N|k)$$

a free pro-p factor of the Galois group $G(k(p)|k)$ of the maximal p-extension of k. Then $N|k$ is a pro-p extension which is unramified outside p, i.e. F is a factor of the Galois group $G_\Sigma(k) = G(k_\Sigma|k)$, where k_Σ is the maximal p-extension of k which is unramified outside the set Σ of primes of k lying above p or ∞. If

$$\rho(k) \quad \text{is the maximal possible rank}$$

of such a free pro-p factor and assuming that Leopold's conjecture holds for k and p, then $1 \leq \rho(k) \leq r_2 + 1$, where r_2 denotes the number of complex places of k. Some examples are known where $\rho(k) = r_2 + 1$ and there are also number fields with $\rho(k) < r_2 + 1$, see [8]. If k is a global number field which contains the group μ_{2p} of $2p$-th roots of unity and assuming that the generalized Greenberg conjecture holds (see §2), then Lannuzel/Nguyen Quang Do [2] and, independently, McCallum [3] proved that the case $\rho(k) = r_2 + 1$ only occurs when $G_\Sigma(k)$ is itself a free pro-p group, i.e. k has only one prime above p and the p-primary part of its ideal class group is trivial. In this paper we give a short proof of this theorem assuming a weaker form of the Greenberg conjecture.

In general it seems to be difficult to find a free pro-p factor F of $G_\Sigma(k)$ of rank bigger than 1. We will consider the case $k = \mathbb{Q}(\zeta_p)$ and construct free factors under certain conditions.

1 Pro-p Operator Groups

Let p be a prime number. For a pro-p group G we denote its Frattini subgroup by $G^* = G^p[G, G]$. For the cohomology groups of G with coeffients in $\mathbb{Z}/p\mathbb{Z}$ we often set $H^i(G) = H^i(G, \mathbb{Z}/p\mathbb{Z})$. If A is an abelian group, then $A^\vee$ denotes its Pontryagin dual.

Let p be a prime number and let

$$\begin{tikzcd} 1 \arrow[r] & G \arrow[r] & \mathcal{G} \arrow[r] & \Delta \arrow[r] \arrow[l, bend left, "s"] & 1, \end{tikzcd}$$

be a split exact sequence of profinite groups where G is a pro-p group and Δ is a finite group of order prime to p. Thus $\mathcal{G}$ is the semi-direct product of Δ by G and G is a pro-p-Δ operator group where the action of Δ on G is defined via the splitting s. Conversely, given a pro-p-Δ operator group G, we get a semi-direct product $\mathcal{G} = G \rtimes \Delta$ where the action of Δ on G is the given one.

Let $\mathcal{G}(p)$ be the maximal pro-p quotient of $\mathcal{G}$ and let G_Δ be the maximal quotient of G with trivial Δ-action. Observe that G_Δ is well-defined. It can be shown ([7], proposition 1.1) that there is a canonical isomorphism

$$G_\Delta \xrightarrow{\sim} \mathcal{G}(p)\,.$$

Furthermore, if Δ_0 is a subgroup of Δ, then

$$H^2(G_{\Delta_0}) \xrightarrow{inf} H^2(G)^{\Delta_0}$$

is injective; in particular, if $H^2(G)^{\Delta_0} = 0$, then G_{Δ_0} is a free pro-p group.

Proposition 1.1 *Let p be an odd prime number and let Δ be a finite abelian group of exponent $p-1$ with character group $\Delta^\vee$. Let G be a pro-p-Δ operator group, which is finitely generated as a pro-p group, and let*

$$H^2(G) = \bigoplus_{\chi \in \Omega} H^2(G)^\chi$$

be the decomposition into χ-eigenspaces of $H^2(G)$ where Ω is the subset of $\Delta^\vee$ given by the non-trivial eigenspaces. Assume that there exists a subgroup Δ_0 of Δ such that

$$\chi_{|\Delta_0} \neq 1 \quad \textit{for all } \chi \in \Omega.$$

Then the maximal quotient $E = G_{\Delta_0}$ of G with trivial Δ_0-action is a free pro-p group of rank

$$r = \sum_{\chi \in (\Delta/\Delta_0)^\vee} \dim_{\mathbb{F}_p} (G/G^*)^\chi,$$

and there is an isomorphism

$$\bigoplus_{\chi \in (\Delta/\Delta_0)^\vee} (G^{ab})^\chi \cong E^{ab}$$

of $\mathbb{Z}_p[\Delta]$-modules.

Proof: As mentioned above we have $H^2(G_{\Delta_0}) \subseteq H^2(G)^{\Delta_0}$, and so

$$H^2(G_{\Delta_0}) \subseteq \bigoplus_{\psi\in(\Delta/\Delta_0)^\vee} H^2(G)^\psi = \bigoplus_{\psi\in(\Delta/\Delta_0)^\vee} \Big(\bigoplus_{\chi\in\Omega} H^2(G)^\chi\Big)^\psi.$$

From the exact sequence

$$0 \longrightarrow (\Delta/\Delta_0)^\vee \longrightarrow \Delta^\vee \longrightarrow \Delta_0^\vee \longrightarrow 0$$

it follows that $(\Delta/\Delta_0)^\vee \cap \Omega = \varnothing$, and so we obtain $H^2(E) = H^2(G_{\Delta_0}) = 0$, i.e. E is a free pro-p group. Since

$$E^{ab} = (G_{\Delta_0})^{ab} = \bigoplus_{\psi\in(\Delta/\Delta_0)^\vee} (G^{ab})^\psi$$

the proposition is proved. □

2 The Greenberg Conjecture and Free Pro-p Extensions of Number Fields

We use the following notation:

p	is a prime number,
k	is a number field (not nessarily of finite degree over $\mathbb{Q}$),
k_∞	is the cyclotomic $\mathbb{Z}_p$-extension of k,
$\tilde{k}$	is the compositum of all $\mathbb{Z}_p$-extensions of k,
Σ	is the set $S_p \cup S_\infty$ of primes above p and archimedean primes,
k_Σ	is the maximal p-extension of k which is unramified outside Σ,
$G_\Sigma(k)$	is the Galois group $G(k_\Sigma\|k)$ of k_Σ over k
Γ	is the Galois group $G(k_\infty\|k)$,
L_k	is the maximal unramified p-extension of k,
$L_k^{S_p}$	is the maximal unramified p-extension of k, which is completely decomposed at S_p.

If $K|k$ is a Galois extension of number fields, then we denote the decomposition group of $G(K|k)$ with respect to a prime $\mathfrak{p}$ by $G_\mathfrak{p}(K|k)$.

The groups of roots of unity of p-power order of k is denoted by $\mu(k)(p)$, and $Cl(k)(p)$ and $Cl_{S_p}(k)(p)$ is the p-primary part of the ideal class group and the S_p-ideal class group of k, respectively. Let $r_2 = r_2(k)$ be the number of complex places of k. Finally we set

$$X_{cs}(k) = G(L_k^{S_p}|k)^{ab} \quad \text{and} \quad X_{nr}(k) = G(L_k|k)^{ab}.$$

Let k be a number field of finite degree over $\mathbb{Q}$, $k^{(a)}|k$ a multiple $\mathbb{Z}_p$-extension of rank $a \geq 1$, i.e.

$$\Gamma^{(a)} = G(k^{(a)}|k) \cong \mathbb{Z}_p^{\ a},$$

and $\Lambda = \Lambda_{(a)}$ the completed group ring $\mathbb{Z}_p[\![\Gamma^{(a)}]\!]$. The Λ-torsion submodule of a Λ-module M is denotes by $T_\Lambda(M)$ and $F_\Lambda(M)$ is the quotient $M/T_\Lambda(M)$.

If Leopoldt's conjecture for k and p holds, then the compositum $\tilde{k}$ of all $\mathbb{Z}_p$-extensions of k is the unique multiple $\mathbb{Z}_p$-extension $k^{(r_2+1)}$ of rank $r_2 + 1$. The following statement is called "generalized Greenberg conjecture"

$GC(1)$: $\quad X_{cs}(\tilde{k})$ is a pseudo-null Λ-module,

and is due to Greenberg (stated for $X_{nr}(\tilde{k})$) who generalized his earlier conjecture which asserts that for a totally real number field k the $\mathbb{Z}_p[\![\Gamma]\!]$-module $X_{nr}(k_\infty)$ is finite. A weaker form of the conjecture above is the following:

$GC(2)$: $\quad$ If $X_{cs}(\tilde{k}) \neq 0$, then it has a non-trivial pseudo-null Λ-submodule.

Lemma 2.1 *Let k be a number field of finite degree over $\mathbb{Q}$, $F = G(N|k)$ a free pro-p factor group of $G_\Sigma(k)$ of rank $r_2 + 1$, and $k_\infty \subseteq k^{(a)} \subseteq N$ a multiple $\mathbb{Z}_p$-extension of rank a. Then*

$$T_\Lambda(G_\Sigma(k^{(a)})^{ab}) = G_\Sigma(N)/[G_\Sigma(N), G_\Sigma(k^{(a)})].$$

Proof: Let $\Lambda = \mathbb{Z}_p[\![\Gamma^{(a)}]\!]$ and

$$\varphi : G_\Sigma(k^{(a)}) \twoheadrightarrow G(N|k^{(a)}).$$

Since $G(N|k^{(a)})$ is free, we obtain the exact sequence

$$0 \longrightarrow G_\Sigma(N)/[G_\Sigma(N), G_\Sigma(k^{(a)})] \longrightarrow G_\Sigma(k^{(a)})^{ab} \xrightarrow{\varphi^{ab}} G(N|k^{(a)})^{ab} \longrightarrow 0\,.$$

The Λ-module $G(N|k^{(a)})^{ab}$ is torsion-free of rank r_2, see [4] (5.6.6), and the Λ-rank of $G_\Sigma(k^{(a)})^{ab}$ is also equal to r_2 by [1] (4.3) and (5.4)(b) (observe that the weak Leopoldt conjecture holds since $k_\infty \subseteq k^{(a)}$). Therefore the kernel of φ^{ab} is the Λ-torsion part $T_\Lambda(G_\Sigma(k^{(a)})^{ab})$ of $G_\Sigma(k^{(a)})^{ab}$. $\square$

The following theorem is due to Lannuzel/Nguyen Quang Do [2] (assuming $GC(1)$ and that all finite abelian p-extensions of k unramified outside p satisfy Leopoldt's conjecture) and, independently, to McCallum [3] (for $k = \mathbb{Q}(\mu_p)$ and assuming $GC(1)$).

Theorem 2.2 *Let k be a number field of finite degree over $\mathbb{Q}$ containing the group μ_{2p}. Assume that Leopoldt's conjecture for (k,p) and Greenberg's conjecture $GC(2)$ hold.*
Then the following assertions are equivalent:

(i) *$G_\Sigma(k)$ has a free pro-p factor group F of rank r_2+1,*

(ii) *$G_\Sigma(k)$ is a free pro-p group of rank r_2+1,*

(iii) *$\#S_p(k)=1$ and $Cl_{S_p}(k)(p)=0$.*

Proof: For the well-known equivalence (ii)⇔(iii) see for example [4], (8.7.3). So we only have to prove the implication (i)⇒(ii).

Let $F = G(N|k)$ be a free pro-p factor of $G_\Sigma(k)$ of rank r_2+1. Since Leopoldt conjecture holds, we have $G(\tilde{k}|k) \cong \mathbb{Z}_p^{(r_2+1)}$ and $k_\infty \subseteq \tilde{k} \subseteq N$. Let $\Lambda = \mathbb{Z}_p[\![\mathbb{Z}_p^{(r_2+1)}]\!]$. We consider the surjections

$$\varphi : G_\Sigma(k) \twoheadrightarrow G(N|k) \quad \text{and} \quad \tilde{\varphi} : G_\Sigma(\tilde{k}) \twoheadrightarrow G(N|\tilde{k}).$$

By lemma (2.1) we have

$$T_\Lambda(G_\Sigma(\tilde{k})^{ab}) = G_\Sigma(N)/[G_\Sigma(N), G_\Sigma(\tilde{k})].$$

Let $k_0 = \mathbb{Q}(\mu_{2p})$ and consider the abelian Galois group $G(\tilde{k}_0|k_0) \cong \mathbb{Z}_p^{r+1}$, where $r=(p-1)/2$ if $p>2$ and $r=1$ otherwise. Its decomposition group $G_\mathfrak{p}(\tilde{k}_0|k_0)$ with respect to the unique prime $\mathfrak{p}$ above p has finite index, and so $\dim G_\mathfrak{p}(\tilde{k}_0|k_0) = r+1 \geq 2$. Since $\mu_{2p} \subseteq k$, it follows that $\dim G_\mathfrak{p}(\tilde{k}|k) \geq 2$ for all primes $\mathfrak{p}$ of k above p.

For a pro-p group G let I_G be the augmentation ideal of the completed group ring $\mathbb{Z}_p[\![G]\!]$. Setting $E^i(-) = Ext^i_\Lambda(-,\Lambda)$ and using $\dim G_\mathfrak{p}(\tilde{k}|k) \geq 2$ for all primes $\mathfrak{p}|p$, we obtain by Iwasawa theory an inclusion

$$X_{cs}(\tilde{k})(-1) \hookrightarrow E^1(Y_\Sigma)$$

with pseudo-null cokernel, where the Λ-module $Y_\Sigma = I_{G_\Sigma(k)}/I_{G_\Sigma(\tilde{k})}I_{G_\Sigma(k)}$ fits in an exact sequence

$$0 \longrightarrow G_\Sigma(\tilde{k})^{ab} \longrightarrow Y_\Sigma \longrightarrow I \longrightarrow 0,$$

see [1] thm(5.4)(d), lemma(4.3) and [4](5.6.7); here I denotes the augmentation ideal of Λ. Analogously, we have an exact sequence

$$0 \longrightarrow G(N|\tilde{k})^{ab} \longrightarrow Y_F \longrightarrow I \longrightarrow 0,$$

where

$$Y_F = I_{G(N|k)}/I_{G(N|\tilde{k})}I_{G(N|k)} \cong \Lambda^{r_2+1},$$

see [4](5.6.6) and recall that $F = G(N|k)$ is a free pro-p group. We obtain a commutative and exact diagram

$$\begin{tikzcd}
0 \arrow[r] & G_\Sigma(\tilde{k})^{ab} \arrow[r] \arrow[d] & Y_\Sigma \arrow[r] \arrow[d] & I \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & G(N|\tilde{k})^{ab} \arrow[r] & \Lambda^{r_2+1} \arrow[r] & I \arrow[r] & 0,
\end{tikzcd}$$

and so an exact sequence

$$0 \longrightarrow T_\Lambda(G_\Sigma(\tilde{k})^{ab}) \longrightarrow Y_\Sigma \longrightarrow \Lambda^{r_2+1} \longrightarrow 0.$$

It follows that

$$E^1(Y_\Sigma) \cong E^1(T_\Lambda(G_\Sigma(\tilde{k})^{ab})).$$

Therefore we get an inclusion

$$X_{cs}(\tilde{k})(-1) \hookrightarrow E^1(T_\Lambda(G_\Sigma(\tilde{k})^{ab}))$$

with pseudo-null cokernel, showing that $X_{cs}(\tilde{k})$ has no non-trivial pseudo-null Λ-submodule.

From our assumption $GC(2)$ we get $X_{cs}(\tilde{k}) = 0$, and so

$$T_\Lambda(G_\Sigma(\tilde{k})^{ab})^\circ \sim E^1(T_\Lambda(G_\Sigma(\tilde{k})^{ab})) \sim X_{cs}(\tilde{k})(-1) = 0$$

(M° denotes the $\mathbb{Z}_p[\![G(\tilde{k}|k)]\!]$-module M with the inverse action of $G(\tilde{k}|k)$). It follows that

$$T_\Lambda(G_\Sigma(\tilde{k})^{ab}) = 0,$$

since $G_\Sigma(\tilde{k})^{ab}$ has no non-trivial pseudo-null submodule, see [5] (4.2). Therefore $G_\Sigma(N) = 1$, i.e. $k_\Sigma = N$. This finishes the proof of the theorem. $\square$

3 Free Pro-p Extensions of $\mathbb{Q}(\zeta_p)$

We keep the notation of the preceding section. In the following we will construct free pro-p factors of $G = G_\Sigma(k)$, where $k = \mathbb{Q}(\zeta_p)$ and p is an odd prime number. The only method we have is to find a subextension $k_0 = k^{\Delta_0}$ of $k|\mathbb{Q}$, $\Delta_0 \subseteq \Delta = G(k|\mathbb{Q})$, such that $G_\Sigma(k)_{\Delta_0} = G((k_0)_\Sigma|k_0)$ is a free pro-p-group.

Let ω be the Teichmüller character. We define the subsets Ω_{gen} and Ω_{rel} of characters of $\Delta = G(k|\mathbb{Q})$ by

$$\Omega_{rel} = \{\omega^i \in \Delta^\vee \,|\, Cl(k)(p)^{\omega^{1-i}} \neq 0\} \quad \text{and} \quad \Omega_{gen} = \{\omega^0\} \cup \Omega_{rel} \cup \{\omega^i \in \Delta^\vee \,|\, i \;\; odd\}.$$

By Poitou-Tate duality and since Leopoldt's conjecture holds for the abelian extension $k|\mathbb{Q}$, we get

$$\begin{aligned}
{}_pG^{ab} &\cong H^2(G)^\vee \\
&\cong \mathrm{Hom}(Cl(k)(p),\mu_p) = \bigoplus_{\omega^i\in\Omega_{rel}} \mathrm{Hom}(Cl(k)(p),\mu_p)^{\omega^i} \\
&\cong \bigoplus_{\omega^i\in\Omega_{rel}} (H^2(G)^\vee)^{\omega^i} \cong \bigoplus_{\omega^i\in\Omega_{rel}} ({}_pG^{ab})^{\omega^i},
\end{aligned}$$

see [4] (8.6.13). Furthermore, since

$$G^{ab}\otimes\mathbb{Q}_p \cong \mathbb{Q}_p \oplus \bigoplus_{i\ odd} \mathbb{Q}_p[\Delta]^{\omega_i},$$

we have an $\mathbb{F}_p[\Delta]$-isomorphism

$$(G^{ab}/\mathrm{Tor}_{\mathbb{Z}_p}G^{ab})/p \cong \mathbb{F}_p \oplus \bigoplus_{i\ odd} \mathbb{F}_p[\Delta]^{\omega_i}.$$

From the exact sequence

$$0 \longrightarrow \mathrm{Tor}_{\mathbb{Z}_p}G^{ab} \longrightarrow G^{ab} \longrightarrow G^{ab}/\mathrm{Tor}_{\mathbb{Z}_p}G^{ab} \longrightarrow 0$$

and the fact that $\mathrm{Tor}_{\mathbb{Z}_p}G^{ab}/p$ and ${}_pG^{ab}$ are $\mathbb{F}_p[\Delta]$-isomorphic, it follows that

$$G_\Sigma(k)/G_\Sigma(k)^* = \bigoplus_{\omega^i\in\Omega_{gen}} (G_\Sigma(k)/G_\Sigma(k)^*)^{\omega^i}.$$

Since

$$\chi_{|\Delta_0} \neq 1 \quad \text{for all } \chi\in\Omega_{rel} \qquad \text{if and only if} \qquad (\chi^{-1})_{|\Delta_0} \neq 1 \quad \text{for all } \chi\in\Omega_{rel}$$

for a subgroup $\Delta_0 \subseteq \Delta$ and

$$H^2(G) = \bigoplus_{\omega^i\in\Omega_{rel}} H^2(G)^{\omega^{-i}},$$

we get from proposition (1.1)

Theorem 3.1 *Let p be an odd prime number, $k=\mathbb{Q}(\zeta_p)$ and $\Delta = G(k|\mathbb{Q})$. Let*

$$\Omega_{gen} = \{\omega^0\}\cup\Omega_{rel}\cup\{\omega^i\in\Delta^\vee \,|\, i \ \ odd\}, \quad \Omega_{rel} = \{\omega^i\in\Delta^\vee \,|\, Cl(k)(p)^{\omega^{1-i}} \neq 0\}.$$

Assume that there exists a subgroup Δ_0 of Δ such that

$$\chi_{|\Delta_0} \neq 1 \quad \textit{for all } \chi\in\Omega_{rel},$$

and let

$$\Theta = \Omega_{gen} \cap (\varDelta/\varDelta_0)^\vee.$$

Then there exists a $\varDelta$-invariant surjection from $G = G_\Sigma(\mathbb{Q}(\zeta_p))$ onto the free pro-p group $E = G_{\varDelta_0}$ which induces an isomorphism

$$\bigoplus_{\chi\in\Theta} (G^{ab})^\chi \cong E^{ab}$$

of $\mathbb{Z}_p[\varDelta]$-modules. In particular,

$$\operatorname{rank} E \geq \sum_{\chi\in\Theta} \dim_{\mathbb{F}_p}(G/G^*)^\chi \geq \#\Theta.$$

If Vandiver's conjecture holds, i.e. $Cl(k^+)(p) = 0$, then $\operatorname{rank} E = \#\Theta$.

Remark: Since $\omega^0 \notin \Omega_{rel}$, it follows that $\omega^0 \in \Theta$, and so E surjects onto $\varGamma = G(\mathbb{Q}(\zeta_{p^\infty})|\mathbb{Q}(\zeta_p))$, where $\mathbb{Q}(\zeta_{p^\infty})$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\zeta_p)$.

In good cases we obtain small subgroups $\varDelta_0$ such that $\chi_{|\varDelta_0} \neq 1$ for all $\chi \in \Omega_{rel}$, and so large subsets Θ of Ω_{gen} with the properties as above. Let ℓ be a prime number and

$$w_\ell = w_\ell(\Omega_{rel}) = \begin{cases} \max\{v_\ell(i) \,|\, 1 \leq i < p-1,\ \omega^i \in \Omega_{rel}\}\,, & \text{if } \Omega_{rel} \neq \varnothing,\ \ell \text{ odd,} \\ \infty, & \text{if } \Omega_{rel} \neq \varnothing,\ \ell = 2, \\ -1, & \text{otherwise.} \end{cases}$$

where v_ℓ is the ℓ-adic valuation. Consider the following set $M(\Omega_{rel})$ of prime numbers ℓ dividing $p-1$:

$$\ell \in M(\Omega_{rel}) \quad \Leftrightarrow \quad \ell | p-1 \text{ odd and } w_\ell < v_\ell(p-1) \quad \text{or} \quad \ell = 2.$$

If $\Omega_{rel} = \varnothing$, then $M(\Omega_{rel})$ is the set of all prime divisors of $p-1$. We identify $\varDelta$ with

$$\mathbb{Z}/(p-1) = \bigoplus_{\ell|p-1} \mathbb{Z}/\ell^{v_\ell(p-1)}\,,$$

and for $\ell \in M(\Omega_{rel})$ we define

$$\varDelta_0(\ell) = \begin{cases} \mathbb{Z}/\ell^{w_\ell+1}\,, & \text{if } \Omega_{rel} \neq \varnothing,\ \ell \text{ odd,} \\ \varDelta, & \text{if } \Omega_{rel} \neq \varnothing,\ \ell = 2, \\ 1, & \text{otherwise,} \end{cases}$$

and

$$\Theta_\ell = \{\omega^0\} \cup \{\omega^k \mid\ 1 \le k < p-1 \text{ odd}, v_\ell(k) > w_\ell\} \subseteq (\Delta/\Delta_0(\ell))^\vee.$$

It follows that

$$\chi_{|\Delta_0(\ell)} \ne 1 \quad \text{for all } \chi \in \Omega_{rel}$$

and

$$\#\Theta_\ell = 1 + \frac{p-1}{2 \cdot \ell^{w_\ell+1}}\,.$$

In particular, $\#\Theta_2 = 1 + (p-1)/2$ if $\Omega_{rel} = \varnothing$, and $\#\Theta_2 = 1$ otherwise. Interesting is the case when $\Omega_{rel} \ne \varnothing$ and $M(\Omega_{rel})$ contains an odd prime number.

With the notation as above we obtain

Corollary 3.2 *Let $\ell \in M(\Omega_{rel})$, where*

$$\Omega_{rel} = \{\omega^i \in \Delta^\vee \mid Cl(k)(p)^{\omega^{1-i}} \ne 0\}.$$

Then there exists a Δ-invariant surjection from $G = G_\Sigma(\mathbb{Q}(\zeta_p))$ onto a free pro-p group E, which surjects onto the cyclotomic $\mathbb{Z}_p$-extension and has

$$\operatorname{rank} E \ge 1 + \frac{p-1}{2 \cdot \ell^{w_\ell+1}}\,.$$

In particular, if ℓ is odd, then E is non-abelian.

Remark: If $p \equiv 3 \bmod 4$, i.e. $p-1 = 2m$, m odd, then $G = G_\Sigma(\mathbb{Q}(\zeta_p))$ has a free non-abelian pro-p factor which surjects onto the cyclotomic $\mathbb{Z}_p$-extension. Indeed, let $\Delta_0 = 2\Delta$ be the subgroup of Δ of order m. Then

$$H^2(G)^{\Delta_0} \cong (Cl(k)/p(-1))^{\Delta_0} \cong \Big((Cl(k)/p)^{\omega^1} \oplus (Cl(k)/p)^{\omega^{m+1}}\Big)(-1)$$

((-1) denotes the (-1)-Tate-twist). Since the Bernoulli number $B_{\frac{p+1}{2}} = B_{p-m}$ is not divisible by p (cf. [6] page 86), we have $(Cl(k)/p)^{\omega^m} = 0$, and by Leopoldt's Spiegelungsatz (see [6] thm 10.9) we get

$$\dim_{\mathbb{F}_p}(Cl(k)/p)^{\omega^{m+1}} \le \dim_{\mathbb{F}_p}(Cl(k)/p)^{\omega^m}.$$

Since also $(Cl(k)/p)^{\omega^1} = 0$, it follows that $H^2(G)^{\Delta_0} = 0$. The free factor G_{Δ_0} of G can be identify with the Galois group $G_\Sigma(\mathbb{Q}(\sqrt{-p}))$.

Example: Let $k = \mathbb{Q}(\mu_{157})$ and $p = 157$. Then

$$\Omega_{rel}(k) = \{\omega^{62},\, \omega^{110}\}$$

see [6] tables. Let $\mathit{\Delta}_m = \mathbb{Z}/m\mathbb{Z}$, $m \geq 1$. Then

$$\mathit{\Delta} = G(k|\mathbb{Q}) = \mathit{\Delta}_{156} = \mathit{\Delta}_4 \oplus \mathit{\Delta}_3 \oplus \mathit{\Delta}_{13}$$

and the residues of i for $\omega^i \in \Omega_{rel}$ are $62 = (2,2,10)$ and $110 = (2,2,6)$. It follows that

$$\begin{aligned} \Theta_3 &= \{\omega^0\} \cup \{\omega^j \mid j \text{ odd and } j \equiv 0 \bmod 3\} &\subseteq& (\mathit{\Delta}/\mathit{\Delta}_3)^\vee, \\ \Theta_{13} &= \{\omega^0\} \cup \{\omega^j \mid j \text{ odd and } j \equiv 0 \bmod 13\} &\subseteq& (\mathit{\Delta}/\mathit{\Delta}_{13})^\vee, \end{aligned}$$

and $(\mathit{\Delta}/\mathit{\Delta}_i)^\vee \cap \Omega_{rel} = \varnothing$ for $i = 3$, 13. Therefore we have two $G(k|\mathbb{Q})$-invariant free pro-p factors F_{27} and F_7 of $G_\Sigma(k)$ of rank 27 and 7, respectively,

$$\begin{aligned} G_\Sigma(\mathbb{Q}(\mu_{157})) &\twoheadrightarrow& F_{27} \cong G_\Sigma(\mathbb{Q}(\mu_{157})^{\mathit{\Delta}_3})\,, \\ G_\Sigma(\mathbb{Q}(\mu_{157})) &\twoheadrightarrow& F_7 \cong G_\Sigma(\mathbb{Q}(\mu_{157})^{\mathit{\Delta}_{13}})\,, \end{aligned}$$

such that there are $G(k|\mathbb{Q})$-invariant isomorphisms

$$\begin{aligned} F_{27}{}^{ab} &\cong& \mathbb{Z}_p \oplus \mathbb{Z}_p[\mathit{\Delta}_{52}]^-, \\ F_7{}^{ab} &\cong& \mathbb{Z}_p \oplus \mathbb{Z}_p[\mathit{\Delta}_{12}]^-, \quad p = 157. \end{aligned}$$

References

[1] Jannsen, U. *Iwasawa modules up to isomorphism.* Advanced Studies in Pure Mathematics **17** (1989), 171-207.

[2] Lannuzel, A., Nguyen Quang Do, T. *Conjectures de Greenberg et extensions pro-p-libre d'un corps de nombres.* Manuscripta Math. **102** (2000), 187-209.

[3] McCallum,W.G. *Greenberg's conjecture and units in multiple $\mathbb{Z}_p$-extensions.* Amer. J. Math.

[4] Neukirch, J., Schmidt, A., Wingberg, K. *Cohomology of Number Fields.* Springer 2000

[5] Venjakob, O. *On the Iwasasa theory of p-adic Lie extensions.* Compos. Math. **138** (2003) 1-54.

[6] Washington, L.C. *Introduction to Cyclotomic Fields.* Springer 1982 (Second ed. 1997)

[7] Wingberg, K. *Free quotients of Demuškin groups with operators.* Preprint 2004

[8] Yamagishi, M. *A note on free pro-p-extensions of algebraic number fields.* J. Théorie des Nombres de Bordeaux **5** (1993) 165-178.

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

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