K. Wingberg
Nagoya Math. J.
Vol. 104 (1986), 43-53

GALOIS GROUPS OF NUMBER FIELDS GENERATED BY TORSION POINTS OF ELLIPTIC CURVES

KAY WINGBERG

Coates and Wiles [1] and B. Perrin-Riou (see [2]) study the arithmetic of an elliptic curve E defined over a number field F with complex multiplication by an imaginary quadratic field K by using p-adic techniques, which combine the classical descent of Mordell and Weil with ideas of Iwasawa's theory of $\boldsymbol{Z}_p$-extensions of number fields. In a special case they consider a non-cyclotomic $\boldsymbol{Z}_p$-extension F_∞ defined via torsion points of E and a certain Iwasawa module attached to E/F, which can be interpreted as an abelian Galois group of an extension of F_∞. We are interested in the corresponding non-abelian Galois group and we want to show that the whole situation is quite analogous to the case of the cyclotomic $\boldsymbol{Z}_p$-extension (which is generated by torsion points of $\boldsymbol{G}_m$).

To make this precise: The odd prime number p satisfies the following two conditions:

(i) p splits in K into two distinct primes: $(p) = \mathfrak{p}\mathfrak{p}^*$,

(ii) E has good (ordinary) reduction at every prime of F above p.

Then F_∞ is the unique $\boldsymbol{Z}_p$-extension in $F(E_{\mathfrak{p}^\infty})$, where $E_{\mathfrak{p}^\infty} = \bigcup_{n\geq 1} E_{\mathfrak{p}^n}$ is the group all torsion points of $E(\bar{F})$ annihilated by a power of $\mathfrak{p}$.

Now, let $S_\mathfrak{p} = S_\mathfrak{p}(F)$ be the set of primes above $\mathfrak{p}$ in F and let F_S be the maximal p-extension of F unramified outside the set of primes $S = S(F)$. Assuming the weak $\mathfrak{p}$-adic Leopoldt conjecture, the abelian Galois group $G(F_{S_\mathfrak{p}}/F_\infty)^{ab}$ is a $\Lambda = \boldsymbol{Z}_p[\![\Gamma]\!]$-torsion module where $\Gamma = G(F_\infty/F)$. This module gives an alternative description of the Selmer group of E/F_∞, [2] Theorem 12, and its characteristic power series defines the Iwasawa L-function of E/F for which an p-adic analogue of the conjecture of Birch and Swinnerton-Dyer is stated. In the following we will call this situation ($p \neq 2$ with i) and ii), $F_\infty \subseteq F(E_{\mathfrak{p}^\infty})$, $F_{S_\mathfrak{p}}$) the elliptic case.

In general, nothing is known about the (non-abelian) Galois groups

Received November 2, 1984.

https://doi.org/10.1017/S0027763000022662 Published online by Cambridge University Press

$G(F_{S_p}/F_\infty)$ or $G(F_T/F_{S_p})$ for $T \supseteq S_p$ not even their cohomological dimension. On the other hand, let F_∞ be the cyclotomic $\boldsymbol{Z}_p$-extension, i.e. the unique $\boldsymbol{Z}_p$-extension in $F(\mu_{p^\infty})$, where μ_{p^∞} is the group of all torsion points of $\boldsymbol{G}_m$ of p-power order, and let S contain the set S_p of *all* primes above p. Then $G(F_S/F_\infty)$ is a free pro-p-group, if the μ-invariant of $G(F_S/F_\infty)^{ab}$ is zero (hence this holds for abelian extensions $F/\boldsymbol{Q}$). Furthermore, the Galois group $G(F_T/F_S)$, $T \supseteq S$, is the free pro-p-product of all inertia groups $T_v(F(p)/F_\infty)$ with $v \in T\backslash S(F_S)$, where $F(p)$ denotes the maximal p-extension of F. This is a result of Neukirch [6] for $F = \boldsymbol{Q}$ and in general of O. Neumann, [7] or [9] for a short proof. If in addition we assume F to be totally real, then $G(F_{S_p}/F_\infty)$ is finitely generated, and we will call this situation ($p \neq 2$, $F_\infty \subseteq F(\mu_{p^\infty})$, F_{S_p}) the $\boldsymbol{G}_m$-case.

We prove the more general

THEOREM. *Let S be a finite set of primes of F such that the following degree condition holds*

$$(*) \qquad \sum_{v \in S \cap S_p} [F_v : \boldsymbol{Q}_p] = r_1(F) + r_2(F)\,,$$

where $r_1(F)$ resp. $r_2(F)$ is the number of real resp. complex places of F. Let F_∞ be a $\boldsymbol{Z}_p$-extension in F_S for which $S_p\backslash S(F_\infty)$ is a finite set and the "weak Leopoldt conjecture"

$$\mathrm{rank}_\Lambda\, G(F_{S \cap S_p}/F_\infty)^{ab} = 0$$

is satisfied.

(i) *Assume $\mu(G(F_{S \cap S_p}/F_\infty)^{ab})$ is zero. Then the Galois groups $G(F_{S_p}/F_\infty)$ and $G(F_{S \cap S_p}/F_\infty)$ are free pro-p-groups and the same is true for $G(F_S/F_\infty)$ and $G(F_{S \cup S_p}/F_\infty)$ if and only if the set of primes $\{v \in S\backslash S_p(F_\infty) : v \mid \mathfrak{q},\ N(\mathfrak{q}) \equiv 1 \bmod p\}$ is finite.*

(ii) *If $H^3(G(F_{S \cap S_p}/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)$ is zero, then the Galois group $G(F_T/F_S)$ for $T \supseteq S$ is a free pro-p-product of inertia groups:*

$$\mathop{*}_{v \in \mathscr{P}_{T\backslash S}(F_S)} T_v(F(p)/F_\infty) \xrightarrow{\ \sim\ } G(F_T/F_S)\,,$$

where the isomorphism is induced by the maps

$$T_v(F(p)/F_\infty) = T_v(F(p)/F_S) \hookrightarrow G(F(p)/F_S) \twoheadrightarrow G(F_T/F_S)\,, \qquad v \in T\backslash S(F_S)\,.$$

Remark. a) $\mathscr{P}_{T\backslash S}(F_S)$ is the projective limit of the sets $\mathscr{P}_{T\backslash S}(L) = \{v_L \mid v : v \in T\backslash S\}$ provided with the cofinal topology, where L/F runs through all finite Galois subextensions of F_S/F, see [9] Section 2.

b) In the G_m-case the assertion ii) is the result of Neumann (there is no condition in that case, since Iwasawa proved in [4] that the weak Leopoldt conjecture is true, see also [8] Proposition 5.1).

COROLLARY (*The elliptic case for* $F = K$). *Let* E *be an elliptic curve defined over the imaginary quadratic field* K *with complex multiplication by the ring of integers of* K. *Let* $p \neq 2$ *be a prime, which satisfies the conditions* i) *and* ii), *and let* F_∞ *be the unique* Z_p*-extension in* $F(E_{\mathfrak{p}^\infty})$. *Then the Galois group* $G(F_S/F_\infty)$, $S \supseteq S_\mathfrak{p}$, *is a free pro-p-group and* $G(F_T/F_S)$ *for* $T \supseteq S \supseteq S_\mathfrak{p}$ *is a free pro-p-product of inertia groups*:

$$\mathop{*}_{v \in \mathscr{P}_T \setminus S(F_S)} T_v(F(p)/F_\infty) \xrightarrow{\ \sim\ } G(F_T/F_S)\,.$$

This follows immediately from the theorem. Indeed, the (weak) Leopoldt conjecture is valid for K and recently L. Schneps and independently R. Gillard proved $\mu = 0$ for $F = K$. The second assertion is quite remarkable, since the inertia groups $T_v(F(p)/F_\infty)$ are not finitely generated for primes v above $\mathfrak{p}^*/p$ (recall: $T_v(F(p)/F_\infty) \cong Z_p$ or 1 for $v \nmid p$).

We need the following notations: Let M^Γ resp. M_Γ be the Γ-invariants resp. Γ-coinvariants of a compact noetherian Λ-module M. According to the general structure theory we have

$$\operatorname{rank}_\Lambda M = \operatorname{rank}_{Z_p} M_\Gamma - \operatorname{rank}_{Z_p} M^\Gamma\,.$$

Furthermore, $A^* = \operatorname{Hom}(A, Q_p/Z_p)$ denotes the Pontrjagin dual of a Z_p-module A and A_{p^m} and ${}_{p^m}A$ are defined by the exact sequence

$$0 \longrightarrow {}_{p^m}A \longrightarrow A \xrightarrow{\ p^m\ } \longrightarrow A \longrightarrow A_{p^m} \longrightarrow 0\,,$$

where the middle map is the multiplication by p^m.

Now we start with a purely algebraic

LEMMA. *Let*

$$1 \longrightarrow H \longrightarrow G \longrightarrow \Gamma \longrightarrow 1$$

be an exact sequence of pro-p-groups, where G *is finitely generated and* Γ *is isomorphic to* Z_p. *Then we have the following assertions for the compact noetherian* Λ*-module* H^{ab}:

(i) $\operatorname{rank}_\Lambda H^{\mathrm{ab}} = -\chi_2(G) + \dim_{F_p} H^2(G, Q_p/Z_p)_p + \operatorname{rank}_{Z_p}(H^2(H, Q_p/Z_p)^\Gamma)^*$ *with the partial Euler-Poincaré characteristic*

https://doi.org/10.1017/S0027763000022662 Published online by Cambridge University Press

$$\chi_2(G) = \sum_{i=0}^{2} \dim_{F_p} H^i(G, F_p)\,.$$

(ii) *Let $H^2(H, \boldsymbol{Q}_p/\boldsymbol{Z}_p)$ be zero and let $H^2(G, \boldsymbol{Q}_p/\boldsymbol{Z}_p)$ be divisible; then H^{ab} does not contain any non-trivial finite Λ-submodule.*

Proof. Let $1 \to R \to F \to G \to 1$ be a minimal representation of G by a free pro-p-group F of rank $n = \dim_{F_p} H^1(G, F_p)$ and a closed normal subgroup R and let the free pro-p-group E be defined by the commutative and exact diagram

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & & & \\
 & & \uparrow & & \uparrow & & & & \\
1 & \longrightarrow & H & \longrightarrow & G & \longrightarrow & \Gamma & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \| & & \\
1 & \longrightarrow & E & \longrightarrow & F & \longrightarrow & \Gamma & \longrightarrow & 1\,. \\
 & & \uparrow & & \uparrow & & & & \\
 & & R & = & R & & & & \\
 & & \uparrow & & \uparrow & & & & \\
 & & 1 & & 1 & & & &
\end{array}$$

Dualizing the corresponding Hochschild-Serre spectral sequences we get the exact sequences

$$0 \longrightarrow H^2(G, \boldsymbol{Q}_p/\boldsymbol{Z}_p)^* \longrightarrow R/[R, F] \longrightarrow F^{\mathrm{ab}} \longrightarrow G^{\mathrm{ab}} \longrightarrow 0$$
$$0 \longrightarrow H^2(H, \boldsymbol{Q}_p/\boldsymbol{Z}_p)^* \longrightarrow R/[R, E] \longrightarrow E^{\mathrm{ab}} \longrightarrow H^{\mathrm{ab}} \longrightarrow 0\,.$$

Since E^{ab} is a free Λ-module of rank $n-1$ ([5] Satz 3.4 a), we get

$$\begin{aligned}
\operatorname{rank}_\Lambda H^{\mathrm{ab}} &= n - 1 - \operatorname{rank}_\Lambda R/[R, E] + \operatorname{rank}_\Lambda H^2(H, \boldsymbol{Q}_p/\boldsymbol{Z}_p)^* \\
&= n - 1 - (\operatorname{rank}_{Z_p} R/[R, F] - \operatorname{rank}_{Z_p} R/[R, E]^{\Gamma}) \\
&\quad + (\operatorname{rank}_{Z_p} H^2(H, \boldsymbol{Q}_p/\boldsymbol{Z}_p)^*_{\Gamma} - \operatorname{rank}_{Z_p} H^2(H, \boldsymbol{Q}_p/\boldsymbol{Z}_p)^{*\Gamma}) \\
&= n - 1 - (\operatorname{rank}_{Z_p} H^2(G, \boldsymbol{Q}_p/\boldsymbol{Z}_p)^* + \dim_{F_p} {}_pG^{\mathrm{ab}}) \\
&\quad + (\operatorname{rank}_{Z_p} R/[R, E]^{\Gamma} - \operatorname{rank}_{Z_p} H^2(H, \boldsymbol{Q}_p/\boldsymbol{Z}_p)^{*\Gamma}) \\
&\quad + \operatorname{rank}_{Z_p} H^2(H, \boldsymbol{Q}_p/\boldsymbol{Z}_p)^{\Gamma *} \\
&= n - 1 - (\operatorname{rank}_{Z_p} H^2(G, \boldsymbol{Q}_p/\boldsymbol{Z}_p)^* + \dim_{F_p} {}_pG^{\mathrm{ab}}) \\
&\quad + \operatorname{rank}_{Z_p} H^2(H, \boldsymbol{Q}_p/\boldsymbol{Z}_p)^{\Gamma *}\,.
\end{aligned}$$

The exact cohomology sequence

$$0 \longrightarrow ({}_pG^{\mathrm{ab}})^* \longrightarrow H^2(G, F_p) \longrightarrow {}_pH^2(G, \boldsymbol{Q}_p/\boldsymbol{Z}_p) \longrightarrow 0$$

https://doi.org/10.1017/S0027763000022662 Published online by Cambridge University Press

induced by the sequence $0 \to \boldsymbol{Z}/p \to \boldsymbol{Q}_p/\boldsymbol{Z}_p \xrightarrow{p} \boldsymbol{Q}_p/\boldsymbol{Z}_p \to 0$ now gives the first assertion. The second follows by the exact sequence

$$0 \longrightarrow H^1(H, \boldsymbol{Q}_p/\boldsymbol{Z}_p)_\Gamma \longrightarrow H^2(G, \boldsymbol{Q}_p/\boldsymbol{Z}_p) \longrightarrow H^2(H, \boldsymbol{Q}_p/\boldsymbol{Z}_p)^\Gamma \longrightarrow 0\,,$$

since H^{ab} does not contain any non-trivial Λ-submodule if and only if $H^{\mathrm{ab}\Gamma} = (H^1(H, \boldsymbol{Q}_p/\boldsymbol{Z}_p)_\Gamma)^*$ is a free $\boldsymbol{Z}_p$-module.

In the following we deal with the commutative and exact diagram obtained by class field theory:

$$(**) \qquad \begin{array}{ccccccccccc}
0 & \longrightarrow & \overline{U}_S(F_\infty) & \longrightarrow & \prod_{v\in S} U_v(F_\infty) & \longrightarrow & G(F_S/F_\infty)^{\mathrm{ab}} & \longrightarrow & A & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \| & & \\
0 & \longrightarrow & \overline{U}_T(F_\infty) & \longrightarrow & \prod_{v\in T} U_v(F_\infty) & \longrightarrow & G(F_T/F_\infty)^{\mathrm{ab}} & \longrightarrow & A & \longrightarrow & 0 \\
 & & & & \uparrow & & \uparrow & & & & \\
0 & \longrightarrow & \operatorname{Ker}\varphi & \longrightarrow & \prod_{v\in T\setminus S} U_v(F_\infty) & \xrightarrow{\varphi} & G(F_T/F_S)_c & \longrightarrow & 0 & & \\
 & & & & & & \uparrow & & & & \\
 & & & & & & H^2(G(F_S/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)^* & & & & \\
 & & & & & & \uparrow & & & & \\
 & & & & & & H^2(G(F_T/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)^* & & & &
\end{array}$$

Here we have used the following notations: S and T are sets of primes with $T \supseteq S$. If F_n is the n-th layer of F_∞, let $U_v(F_n)$ be the p-primary part of the unit group of the v-completion of F_n and let $\overline{U}_S(F_n)$ be the topological closure of the image of the global unit group of F_n diagonal embedded in the local groups. Then $U_v(F_\infty)$ resp. $\overline{U}_S(F_\infty)$ is the projective limit of $U_v(F_n)$ resp. $\overline{U}_S(F_n)$ relative to the norm map. A denotes the Galois group of the maximal abelian unramified p-extension of F_∞ and for shortness we set $G(F_T/F_S)_c$ for $G(F_T/F_S)/[G(F_T/F_S), G(F_T/F_\infty)]$.

In the diagram the vertical sequence is obtained from the Hochschild-Serre spectral sequence and the horizontal maps in the middle are induced by the reciprocity homomorphism. The map φ is surjective, since F_S has no unramified p-extension.

PROPOSITION 1. *Let T be a finite set of primes of F containing S_p. Then*

$$H^2(G(F_T/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)^*$$

is a free Λ-module of finite rank.

https://doi.org/10.1017/S0027763000022662 Published online by Cambridge University Press

Proof. Since the cohomological dimension of $G(F_T/F)$ is equal or less 2, the group $H^2(G(F_T/F), \boldsymbol{Q}_p/\boldsymbol{Z}_p)$ is divisible, and $H^3(G(F_T/F), \boldsymbol{Q}_p/\boldsymbol{Z}_p)$ is zero. The exact sequences obtained from the Hochschild-Serre spectral sequence

$$0 \longrightarrow H^i(G(F_T/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)_\Gamma \longrightarrow H^{i+1}(G(F_T/F), \boldsymbol{Q}_p/\boldsymbol{Z}_p) \longrightarrow H^{i+1}(G(F_T/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)^\Gamma \longrightarrow 0$$

for $i = 1, 2$ show:

$$H^2(G(F_T/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)^\Gamma \quad \text{is divisible},$$
$$H^2(G(F_T/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)_\Gamma = 0\,.$$

This gives the assertion, [8] 1.2.

Now we are interested in the conditions under which $G(F_S/F_\infty)^{\mathrm{ab}}$ is a Λ-torsion module, where S is a finite set of primes of F such that $S_p \backslash S(F_\infty)$ is finite and the degree condition (*) holds. This is equivalent to the weak Leopoldt conjecture, which says: the defect

$$\delta_n := r_1(F_n) + r_2(F_n) - 1 - \operatorname{rank}_{\boldsymbol{Z}_p} \overline{U}_S(F_n)$$

is bounded for $n \to \infty$, [2] Lemma 14.

PROPOSITION 2. *Let S be a set of primes of F such that the degree condition* (*) *holds and let F_∞ be a $\boldsymbol{Z}_p$-extension in F_S such that $S_p \backslash S(F_\infty)$ is finite. Then the following assertions are equivalent*:

i) $\operatorname{rank}_\Lambda G(F_S/F_\infty)^{\mathrm{ab}} = 0$.

ii) a) $H^2(G(F_S/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p) = H^2(G(F_{S\cup S_p}/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p) = 0$

and

b) $\prod_{v \in S_p \backslash S(F_\infty)} U_v(F_\infty) \xrightarrow[\sim]{\varphi} G(F_{S\cup S_p}/F_S)_c$.

iii) a) $\operatorname{rank}_\Lambda H^2(G(F_S/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p) = \operatorname{rank}_\Lambda H^2(G(F_{S\cup S_p}/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p) = 0$

and

b) $\operatorname{rank}_\Lambda \overline{U}_{S\cup S_p}(F_\infty) = \operatorname{rank}_\Lambda \overline{U}_S(F_\infty)$.

Proof. We estimate the rank of $G(F_S/F_\infty)^{\mathrm{ab}}$ by using the diagram (**) for $T = S \cup S_p$:

$$\begin{aligned}\operatorname{rank}_\Lambda G(F_S/F_\infty)^{\mathrm{ab}} \geq\ & \operatorname{rank}_\Lambda G(F_T/F_\infty)^{\mathrm{ab}} \\ & - (\operatorname{rank}_\Lambda \prod_{v\in T\backslash S} U_v(F_\infty) - \operatorname{rank}_\Lambda \operatorname{Ker}\varphi) \\ & + \operatorname{rank}_\Lambda H^2(G(F_S/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)^* \\ & - \operatorname{rank}_\Lambda H^2(G(F_T/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)^*\end{aligned}$$

By the global duality theorem due to Tate and Poitou one can compute the Euler-Poincaré characteristic of $G(F_T/F)$:

$$\chi_2(G(F_T/F)) = \chi(G(F_T/F)) = -r_2(F),$$

see [3] Proposition 22, Corollary 5. Furthermore, Iwasawa's result on local $\boldsymbol{Z}_p$-extensions, [4] Theorem 25, gives

$$\operatorname{rank}_\Lambda \prod_{v \in S_p \setminus S(F_\infty)} U_v(F_\infty) = \sum_{v \in S_p \setminus S(F)} [F_v : \boldsymbol{Q}_p] = r_2(F).$$

Hence by the lemma we get

$$\operatorname{rank}_\Lambda G(F_S/F_\infty)^{\mathrm{ab}} \geq \operatorname{rank}_\Lambda \operatorname{Ker} \varphi + \operatorname{rank}_\Lambda H^2(G(F_S/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)^*,$$

Therefore i) implies

$$\operatorname{rank}_\Lambda \operatorname{Ker} \varphi = \operatorname{rank}_\Lambda H^2(G(F_S/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)^* = 0.$$

If F_∞ is a non-cyclotomic $\boldsymbol{Z}_p$-extension, we have considering the Λ-module structure of the local groups $U_v(F_\infty)$

$$\prod_{v \in S_p \setminus S(F_\infty)} U_v(F_\infty) \subseteq \Lambda^{r_2(F)}$$

([4] Theorem 25), so $\operatorname{Ker} \varphi$ must be zero as a rank zero submodule of a free Λ-module, i.e., φ is an isomorphism. If F is the cyclotomic $\boldsymbol{Z}_p$-extension, S must contain S_p, and there is nothing to show for φ.

Furthermore, we obtain

$$\operatorname{rank}_\Lambda G(F_T/F_\infty)^{\mathrm{ab}} = r_2(F),$$

hence by the lemma and Proposition 1

$$H^2(G(F_T/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p) = 0.$$

Therefore we get the inclusion

$$H^2(G(F_S/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)^* \subseteq G(F_T/F_S)_c \cong \prod_{v \in S_p \setminus S} U_v(F_\infty) \subseteq \Lambda^{r_2(F)},$$

hence as above

$$H^2(G(F_S/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p) = 0.$$

Assertion iii) follows from ii) for trivial reasons. Finally, iii) implies i) by combining the following rank equalities:

$$\operatorname{rank}_\Lambda G(F_S/F_\infty)^{\mathrm{ab}} = \operatorname{rank}_\Lambda G(F_T/F_\infty)^{\mathrm{ab}} - r_2(F),$$
$$\operatorname{rank}_\Lambda G(F_T/F_\infty)^{\mathrm{ab}} = r_2(F) + \operatorname{rank}_\Lambda H^2(G(F_T/F_\infty), \boldsymbol{Q}_p/\boldsymbol{Z}_p)^*.$$

https://doi.org/10.1017/S0027763000022662 Published online by Cambridge University Press

(the last one follows from the lemma, Proposition 1 and $cd_p(G(F_T/F)) \leq 2$).

PROPOSITION 3. *Let S and F_∞ be as in Proposition 2. If the Λ-rank of $G(F_S/F_\infty)^{ab}$ is zero, the following is true:*

i) *$G(F_S/F_\infty)^{ab}$ and $G(F_{S\cup S_p}/F_\infty)^{ab}$ do not contain any non-trivial finite Λ-submodule.*

ii) *There exists an inclusion*

$$\mathrm{Tor}_{Z_p} G(F_{S\cup S_p}/F_\infty)^{ab} \hookrightarrow \mathrm{Tor}_{Z_p} G(F_S/F_\infty)^{ab}.$$

In particular, there is an inequality

$$\mu(G(F_{S\cup S_p}/F_\infty)^{ab}) \leq \mu(G(F_S/F_\infty)^{ab}).$$

iii) *The Galois group $G(F_S/F_\infty)$ (resp. $G(F_{S\cup S_p}/F_\infty)$) is a free pro-p-group if and only if $\mu(G(F_S/F_\infty)^{ab})$ (resp. $\mu(G(F_{S\cup S_p}/F_\infty)^{ab})$) is zero.*

Proof. We have $cd_p(G(F_{S\cup S_p}/F)) \leq 2$ and $H^2(G(F_{S\cup S_p}/F_\infty), \boldsymbol{Q}_p/Z_p) = 0$ by Proposition 2, so the lemma implies i) for $G(F_{S\cup S_p}/F_\infty)^{ab}$.

Now assume $S_p \not\subset S$ (hence F_∞ is not the cyclotomic Z_p-extension). Proposition 2 and Theorem 25 in [4] give

$$(G(F_{S\cup S_p}/F_S)_c)^\Gamma \cong \Big(\prod_{v\in S_p\setminus S(F_\infty)} U_v(F_\infty)\Big)^\Gamma = 0.$$

Therefore we obtain the exact sequence

$$0 \longrightarrow G(F_{S\cup S_p}/F_\infty)^{ab\Gamma} \longrightarrow G(F_S/F_\infty)^{ab\Gamma}$$
$$\longrightarrow \Big(\prod_{v\in S_p\setminus S(F_\infty)} U_v(F_\infty)\Big)_\Gamma \xrightarrow{\psi} G(F_{S\cup S_p}/F_\infty)^{ab}_\Gamma.$$

Since F_∞/F is unramified for all $v \in S_p\setminus S$ we get an isomorphism

$$0 = H^1(\Gamma_{n,v}, U_v(F_n)) \longrightarrow U_v(F_n)_{\Gamma_{n,v}} \xrightarrow{\sim} U_v(F) \longrightarrow \hat{H}^0(\Gamma_{n,v}, U_v(F_n)) = 0$$

($\Gamma_{n,v} = G(F_{n,v}/F_v)$), and consequently

$$\Big(\prod_{v\in S_p\setminus S(F_\infty)} U_v(F_\infty)\Big)_\Gamma = \prod_{v\in S_p\setminus S(F)} U_v(F).$$

By class field theory we have a commutative and exact diagram

$$\begin{array}{ccccccc} & & {}_{p^m}\Big(\prod_{v\in S_p\setminus S} U_v(F)\Big) & \xrightarrow{\psi} & {}_{p^m}(G(F_{S\cup S_p}/F_\infty)^{ab}_\Gamma) \\ & & \big\downarrow & & \big\| \\ 0 \longrightarrow {}_{p^m}\mu(F) & \xrightarrow{\Delta} & {}_{p^m}\Big(\prod_{v\in S\cup S_p} U_v(F)\Big) & \longrightarrow & {}_{p^m}G(F_{S\cup S_p}/F)^{ab}. \end{array}$$

Since the group $\mu(F)$ of all roots of unity in F is diagonal embedded in the local groups, we see that ψ restricted to the Z_p-torsion subgroup of $\prod_{v\in S_p\setminus S} U_v(F)$ is injective. In the beginning of the proof we showed that $G(F_{S\cup S_p}/F_\infty)^{\mathrm{ab}\Gamma}$ is Z_p-free, hence we now get the same assertion for $G(F_S/F_\infty)^{\mathrm{ab}\Gamma}$.

Since $\mathrm{Tor}_{Z_p}(\prod_{v\in S_p\setminus S(F_\infty)} U_v(F_\infty))$ is trivial, the exact sequence

$$0\longrightarrow \prod_{v\in S_p\setminus S(F_\infty)} U_v(F_\infty)\longrightarrow G(F_{S\cup S_p}/F_\infty)^{\mathrm{ab}}\longrightarrow G(F_S/F_\infty)^{\mathrm{ab}}\longrightarrow 0$$

gives the assertion ii), whereas iii) follows from the isomorphism

$$0\longrightarrow {}_pG(F_T/F_\infty)^{\mathrm{ab}*}\xrightarrow{\sim} H^2(G(F_T/F_\infty), F_p)\longrightarrow {}_pH^2(G(F_T/F_\infty), Q_p/Z_p)=0$$

with $T=S$ resp. $T=S\cup S_p$.

Proof of the Theorem. In order to prove the second statement we first consider the exact sequence

$$0\longrightarrow G(F_S/F_{S\cap S_p})_c\longrightarrow G(F_S/F_\infty)^{\mathrm{ab}}\longrightarrow G(F_{S\cap S_p}/F_\infty)^{\mathrm{ab}}\longrightarrow 0$$

(observe: $H^2(G(F_{S\cap S_p}/F_\infty), Q_p/Z_p)=0$, Proposition 2 ii)). Now the surjection induced by the reciprocity map

$$\prod_{v\in S\setminus S_p(F_\infty)} U_v(F_\infty)\xrightarrow{\varphi} G(F_S/F_{S\cap S_p})_c$$

gives the rank equality

$$\mathrm{rank}_\Lambda G(F_S/F_\infty)^{\mathrm{ab}}=\mathrm{rank}_\Lambda G(F_{S\cap S_p}/F_\infty)^{\mathrm{ab}}=0\,.$$

Indeed, the module

$$\prod_{v\in S\setminus S_p(F_\infty)} U_v(F_\infty)\cong \prod_{\substack{\mathfrak{q}\in S\setminus S_p(F)\\ N(\mathfrak{q})\equiv 1 \bmod p}} U_\mathfrak{q}(F_\infty)\,[\![\Gamma/\Gamma_\mathfrak{q}]\!]$$

is Λ-torsion, because we have for a decomposition group $\Gamma_\mathfrak{q}$ of Γ, $\mathfrak{q}\nmid p$:

$$\Gamma_\mathfrak{q}=1\Longleftrightarrow U_\mathfrak{q}(F_\infty)=U_\mathfrak{q}(F)\qquad\text{(cyclic of finite order)}$$
$$[\Gamma:\Gamma_\mathfrak{q}]<\infty\Longleftrightarrow U_\mathfrak{q}(F_\infty)\cong Z_p\,.$$

Using Proposition 2 we get

$$\prod_{v\in S_p\setminus S(F_\infty)} T_v(F(p)/F_\infty)^{\mathrm{ab}}\xrightarrow{\sim} G(F_{S_p}/F_{S\cap S_p})_c\,,$$
$$H^2(G(F_{S_p}/F_\infty), Q_p/Z_p)=0\,,$$

and the Hochschild-Serre spectral sequence implies

$$0 = H^2(G(F_{S_p}/F_\infty), \mathbf{Q}_p/\mathbf{Z}_p) \longrightarrow H^1(G(F_{S\cap S_p}/F_\infty), H^1(G(F_{S_p}/F_{S\cap S_p}), \mathbf{Q}_p/\mathbf{Z}_p)) \longrightarrow H^3(G(F_{S\cap S_p}/F_\infty), \mathbf{Q}_p/\mathbf{Z}_p) = 0\,.$$

Therefore Lemma 2.1 in [9] gives the isomorphism

$$\mathop{*}_{v\in\mathscr{P}_{S_p\setminus S}(F_{S\cap S_p})} T_v(F(p)/F_\infty) \xrightarrow{\ \sim\ } G(F_{S_p}/F_{S\cap S_p})\,.$$

In the commutative and exact diagram

$$\begin{array}{ccc}
 & 0 & & 0 \\
 & \uparrow & & \uparrow \\
\mathop{*}_{v\in\mathscr{P}_{S_p\setminus S}(F_{S\cup S_p})} & T_v(F(p)/F_\infty) & \xrightarrow{\ \sim\ } & G(F_{S_p}/F_{S\cap S_p}) \\
 & \uparrow & & \uparrow \\
\mathop{*}_{v\in\mathscr{P}_{T\cup S_p\setminus S\cap S_p}(F_{S\cup S_p})} & T_v(F(p)/F_\infty) & \longrightarrow & G(F_{T\cup S_p}/F_{S\cap S_p}) \\
 & \uparrow & & \uparrow \\
\mathop{*}_{v\in\mathscr{P}_{T\cup S_p\setminus S_p}(F_{S_p})} & T_v(F(p)/F_\infty) & \longrightarrow & G(F_{T\cup S_p}/F_{S_p}) \\
 & \uparrow & & \uparrow \\
 & 0 & & 0
\end{array}$$

the bottom map is an isomorphism by the theorem of Neumann. Therefore we obtain the assertion ii) for the sets $T\cup S_p$ and $S\cap S_p$, hence for T and $S\cap S_p$ by dividing through the normal subgroup generated by all inertia groups for $v\in S_p\setminus T$. Finally, the normal subgroup

$$\mathop{*}_{v\in\mathscr{P}_{S\setminus T}(F_S)} T_v(F(p)/F_\infty) \quad \text{of} \quad \mathop{*}_{v\in\mathscr{P}_{T\setminus S\cap S_p}(F_{S\cap S_p})} T_v(F(p)/F_\infty) \cong G(F_T/F_{S\cap S_p})$$

is just the kernel of the canonical surjection $G(F_T/F_{S\cap S_p}) \twoheadrightarrow G(F_S/F_{S\cap S_p})$, hence isomorphic to $G(F_T/F_S)$.

In order to prove i) we observe that by the just established isomorphism

$$\mathop{*}_{v\in\mathscr{P}_{S\setminus S\cap S_p}} T_v(F(p)/F_\infty) \xrightarrow{\ \sim\ } G(F_S/F_{S\cap S_p})$$

the surjection φ is in fact an isomorphism. Thus we get

$$\mu(G(F_S/F_\infty)^{\mathrm{ab}}) = \mu(G(F_{S\cap S_p}/F_\infty)^{\mathrm{ab}}) + \sum_{\substack{\mathfrak{q}\in S\setminus S_p \\ N(\mathfrak{q})\equiv 1 \bmod p}} \mu(U_{\mathfrak{q}}(F_\infty)[\![\Gamma/\Gamma_{\mathfrak{q}}]\!])\,.$$

Now the proof of the theorem is accomplished by using Proposition 3 ii), iii).

References

[1] Coates, J. and Wiles, A., On the conjecture of Birch and Swinnerton-Dyer, Invent. Math., **39** (1977), 223–251.

[2] ——, Infinite descent on elliptic curves with complex multiplication, Progress in Mathematics Vol. **35** (Birkhäuser) Arithmetic and Geometry I dedicated to I.R. Šafarevič Boston-Basel-Stuttgart 1983.

[3] Haberland, K., Galois cohomology of algebraic number fields, Deutscher Verlag der Wissenschaften, Berlin (1978).

[4] Iwasawa, K., On Z_ℓ-extensions of algebraic number fields, Ann. of Math., **98** (1973), 246–326.

[5] Jannsen, U., Über Galoisgruppen lokaler Körper, Invent. Math., **70** (1982), 53–69.

[6] Neukirch, J., Einbettungsprobleme mit lokaler Vorgabe und freie Produkte lokaler Galoisgruppen, J. reine angew. Math., **259** (1973), 1–47.

[7] Neumann, O., On p-closed number fields and an analogue of Riemann's existence theorem, In A. Fröhlich, Algebraic number fields, Acad. Press, London (1977), 625–647.

[8] Wingberg, K., Duality theorems for Γ-extensions of algebraic number fields, Compositio Math., **55** (1985), 333–381.

[9] ——, Ein Analogon zur Fundamentalgruppe einer Riemann'schen Fläche im Zahlkörperfall, Invent. Math., **77** (1984), 557–584.

NWF I—Mathematik der Universität Regensburg
Universitätsstraße 31
D-8400 Regensburg
F.R.G.