ON A RESULT OF IWASAWA ON CLASS NUMBERS OF NUMBER FIELDS

TOMMASO GIORGIO CENTELEGHE

ABSTRACT. For a finite Galois p-extension of number fields K/E *unramified* outside a finite place $\mathfrak{p}$ of E and *totally ramified* at $\mathfrak{p}$, we generalize a result of Iwasawa concerning mod p congruences satisfied by the class numbers of K and E.

INTRODUCTION

Let E be a number field and $\mathfrak{p}$ a finite place of E. Consider a finite Galois extension K/E *unramified* outside $\mathfrak{p}$ and *totally ramified* at $\mathfrak{p}$. In this setting, it is well known that the ideal norm map gives rise to a surjective group homomorphism $N_{K/E}\colon \mathrm{Cl}_K \to \mathrm{Cl}_E$, where Cl_F denotes the ideal class group of a number field F. In particular, for any prime number p, we see that p divides h_K if p divides h_E, where h_F denotes the class number of a number field F. In his generalization of a theorem of Weber, Iwasawa (cf. [1], Theorem II) proved the following converse statement

Theorem 1 (Iwasawa). *If p is a prime number and $G(K/E)$ is cyclic of p–power order then*

$$p|h_K \Rightarrow p|h_E$$

The purpose of this paper is to show that this result depends *only* on the fact that the Galois group $G(K/E)$ is a p–group and not on his structure. Indeed, we prove that (cf. Theorem 7, §2) if K/E is *any* Galois p–extension *unramified* outside a finite place $\mathfrak{p}$ of E and *totally ramified* at $\mathfrak{p}$ then $h_K \equiv h_E \pmod{p}$ (the statement we give is actually slightly stronger). Under the additional assumption that $G(K/E)$ is cyclic we can say more (cf. Theorem 8, §2): if K_i denotes the degree p^i extension of E inside K then $h_{K_{i+1}} \equiv h_{K_i} \pmod{p^i}$.

The theorems we prove rest upon the characterization of Cl_E as the largest quotient of Cl_K on which $G(K/E)$ acts trivially, the projection map being

given by $N_{K/E}$. This fact is completely independent on the assumption that $G(K/E)$ is a p–group and it is proved at the end of the first section (cf. cor. 4) as a consequence of two auxiliary lemmas. In the second section we deduce Theorem 7 using the simple fact that if a p–group acts on a finite set X then the cardinalities of X^G and X are congruent mod p. An additional argument allows us to prove the refined statement of Theorem 8 in the cyclic case of p–power order. In the third and last section we give applications of Theorem 8 of section 2 and of corollary 4 of section 1. Using the first we recover and generalize the fact that an odd prime p is regular if and only if p does not divide the class number of $\mathbf{Q}(\mu_{p^{m+1}})$, for any integer $m \geq 1$ (cf. prop. 9). We then point out two consequences of corollary 4: the first one states that for any finite Galois extension of number fields K/E *unramified* outside a finite place $\mathfrak{p}$ of E and *totally ramified* at $\mathfrak{p}$, if h_K is even and h_E is odd then the 2–part of Cl_K cannot be cyclic. The second application says that if K/E is a cyclic extension then the cardinalities of Cl_E and of the invariant submodule $\mathrm{Cl}_K^{G(K/E)}$ coincide.

Notation and terminology

If F is a number field and l is a prime number we adopt the following standard notation:
h_F = class number of F;
$h_F^{(l)}$ = l–part of h_F;
H_F = Hilbert Class Field of F;
$H_F^{(l)}$ = maximal unramified abelian l-extension of F;
Cl_F = ideal class group of F;
$\mathrm{Cl}_F^{(l)}$ = maximal l-quotient of Cl_F.

If F/E is an extension of number fields and S is a finite set of places of F, when we say that F/E *is unramified outside* S we always mean that every place of E, finite or infinite, that it is not contained in S is unramified in F.
If F/E is a Galois extension, its Galois group is denoted by $G(F/E)$.
If G is a group, a G-module A will always refer to an *abelian* group A toghether with a left action of G by *automorphisms*. Namely, a group homomorphism $G \to \mathrm{Aut}(A)$. Moreover
A^G = submodule of *invariants* of A;

A_G = quotient module of *covariants* of A;
$\widehat{A}$ = Pontrjagin dual of A.

1. Two lemmas

We present two elementary lemmas which lead to corollaryřefcor at the end of the section, important for us in the sequel. The lemmas involve a certain tower of number fields $E \subset K \subset L$, with L/E and K/E both Galois, and a finite prime $\mathfrak{p}$ of E satisfying the following conditions:
i) K/E is *totally ramified* at $\mathfrak{p}$;
ii) L/K is *unramified* at the prime $\mathfrak{b}$ of K above $\mathfrak{p}$.
Throughout the section $E \subset K \subset L$ will always denote such a triple of number fields and $\mathfrak{p}$ and $\mathfrak{b}$ will be the primes of E and K involved. The lemmas are stated in a more general setting then needed in this paper. The situation to keep in mind is when the extension K/E is *unramified* outside $\mathfrak{p}$ and when L is the Hilbert Class Field of K.

Lemma 2. *The exact sequence*

$$1 \longrightarrow G(L/K) \longrightarrow G(L/E) \longrightarrow G(K/E) \longrightarrow 1$$

splits. If $\mathfrak{q}$ *is any prime of* L *above* P *then the corresponding inertia subgroup* $I_{\mathfrak{q}}$ *is a complement of* $G(L/K)$ *in* $G(L/E)$*, so that* $I_{\mathfrak{q}} \simeq G(K/E)$ *and*

$$G(L/E) \simeq G(L/K) \rtimes_{\varphi} G(K/E)$$

Proof. Let $\mathfrak{q}$ be a prime of L above $\mathfrak{p}$. The extension K/E is totally ramified at $\mathfrak{p}$, hence every $s \in G(K/E)$ can be lifted to $\tilde{s} \in I_{\mathfrak{q}} < G(L/E)$. This implies that the natural projection map $G(L/E) \longrightarrow G(K/E)$ remains surjective when restricted to $I_{\mathfrak{q}}$. Now since the extension L/K is unramified at the place $\mathfrak{q}$ above $\mathfrak{b}$, we see that $I_{\mathfrak{q}} \cap G(L/K)$ is trivial and $I_{\mathfrak{q}} \simeq G(K/E)$ through the restriction of the previous map. This shows that the sequence above splits and

$$G(L/E) \simeq G(L/K) \rtimes_{\varphi} G(K/E)$$

where the semidirect product structure φ is given by the conjugation action of $I_{\mathfrak{q}} \simeq G(K/E)$ on $G(L/K)$. □

Remark 1. In the isomorphism $G(L/E) \simeq G(L/K) \rtimes_{\varphi} G(K/E)$ we just described, the action of $G(K/E)$ on $G(L/K)$ depends upon the choice of

the prime $\mathfrak{q}$ of L above $\mathfrak{p}$: different choices of primes give different liftings of $G(K/E)$ to inertia subgroups of $G(L/E)$ of primes above $\mathfrak{p}$.

Remark 2. If we set $L = H_K$, the Hilbert Class Field of K, we have

$$G(H_K/E) \simeq \mathrm{Cl}_K \rtimes_\varphi G(K/E)$$

In this situation $G(L/K) = \mathrm{Cl}_K$ is abelian and the action φ is *independent* on the inertia group $I_\mathfrak{q}$ chosen to lift $G(K/E)$ to a subgroup of $G(L/E)$. From the basic properties of the Artin symbol it follows that φ is described by the natural action of $G(K/E)$ on Cl_K.

In the sequel when refering to the action φ of $G(K/E)$ on $G(L/K)$ we always silently assume that a prime $\mathfrak{q}$ of L above $\mathfrak{p}$ has been chosen together with the corresponding subgroup $I_\mathfrak{q}$ lifting $G(K/E)$. If $x \in G(L/K)$ and $\sigma \in G(K/E)$, we denote by $\tilde{\sigma} \in I_\mathfrak{q}$ the lifting of σ and by x^σ the image of x under the automorphism of $G(L/K)$ defined by σ, i.e. $x^\sigma = \tilde{\sigma} x \tilde{\sigma}^{-1}$ Notice that $x^{\sigma\tau} = (x^\tau)^\sigma$.
Define $\mathbf{D}G(L/K)$ to be the subgroup of $G(L/K)$ generated by elements of the form

$$x^\sigma \cdot x^{-1} = [\tilde{\sigma}, x]$$

for $\sigma \in G(K/E)$ and $x \in G(L/K)$.
Then $\mathbf{D}G(L/K)$ is $G(K/E)$-invariant and the formula

$$y[\tilde{\sigma}, x]y^{-1} = [\tilde{\sigma}, [\tilde{\sigma}^{-1}, y] \cdot x] \cdot [\tilde{\sigma}^{-1}, y]$$

shows that $\mathbf{D}G(L/K)$ is normal in $G(L/E)$.
Denote the quotient $G(L/K)/\mathbf{D}G(L/K)$ by $G(L/K)_{G(K/E)}$. It is the *largest quotient* of $G(L/K)$ on which $G(K/E)$ acts trivially (it is the degree zero homology group of $G(K/E)$ with coefficients in $G(L/K)$).

Remark 3. If $G(K/E)$ and $G(L/K)$ are both *abelian* group then $\mathbf{D}G(L/K)$ is the first derived subgroup of $G(L/E)$. This follows from the definition of $\mathbf{D}G(L/K)$, which is generated by the *commutators* $[\tilde{\sigma}, x]$, where $\sigma \in G(K/E)$ and $x \in G(L/K)$.

We now identify the group $G(L/K)_{G(K/E)}$ as the Galois group over E of a certain subextension F of L.

Lemma 3. *Let F be the maximal intermediate field $E \subset F \subset L$ which is unramified at every place above $\mathfrak{p}$.*
Then the natural map $G(L/K) \longrightarrow G(F/E)$ is surjective and induces a group isomorphism

$$G(L/K)/\mathbf{D}G(L/K) \simeq G(F/E)$$

Proof. Choose a prime $\mathfrak{q}$ of L above the prime $\mathfrak{b}$ of K and denote by $I_{\mathfrak{q}}$ the cooresponding inertia subgroup. Then, by lemma 2, $G(L/E) \simeq G(L/K) \rtimes_{\varphi} I_{\mathfrak{q}}$. The natural map

$$R\colon G(L/E) \simeq G(L/K) \rtimes_{\varphi} I_{\mathfrak{q}} \longrightarrow G(F/E)$$

is certainly surjective. Its kernel is, by the definition itself of F, the *normal closure* of $I_{\mathfrak{q}}$ in $G(L/E)$. This implies that its restriction to $G(L/K)$

$$r\colon G(L/K) \longrightarrow G(F/E)$$

is also surjective. The kernel of r is $G(L/KF)$ and contains $\mathbf{D}G(L/K)$, we can see this observing that for $\sigma \in G(K/E)$ and $x \in G(L/K)$ we have

$$r([\tilde{\sigma}, x]) = r(\tilde{\sigma}x\tilde{\sigma}^{-1}x^{-1}) = r(xx^{-1}) = 1$$

where the second equality follows from the fact that r is the restiction to $G(L/K)$ of R, which is defined on the whole group $G(L/E)$ and is *trivial* on $I_{\mathfrak{q}}$.
Denote by $\bar{r}$ the induced group homomorphism

$$\bar{r} : G(L/K)/\mathbf{D}G(L/K) \longrightarrow G(F/E)$$

we show that $\bar{r}$ is an isomorphism.
Let M be the intermediate field $K \subset M \subset L$ corresponding to the subgroup $\mathbf{D}G(L/K)$, thus $G(M/K) = G(L/K)/\mathbf{D}G(L/K)$. We just remarked that $\mathbf{D}G(L/K) \subset G(L/KF)$ or, equivalently, that $KF \subset M$, all we need is to show that $M \subset KF$.
The extension M/E is Galois and its Galois group is isomorphic to

$$G(M/E) = (G(L/K) \rtimes_{\varphi} I_{\mathfrak{q}})/\mathbf{D}G(L/K)$$

Since $I_{\mathfrak{q}}$ acts trivially on $G(M/K)$ the group $G(M/E)$ is *direct* product $G(M/E) = G(L/K)/\mathbf{D}G(L/K) \times I_{\mathfrak{q}}$. Denote by $I'_{\mathfrak{q}}$ the inertia subgroup of $G(M/E)$ at the prime of M lying below $\mathfrak{q}$. Since L/M is unramified at $\mathfrak{q}$,

we see that $I'_{\mathfrak{q}}$ is isomorphic to $I_{\mathfrak{q}}$ under the restriction map $G(L/E) \to G(M/E)$, hence

$$G(M/E) = G(L/K)/\mathbf{D}G(L/K) \times I'_{\mathfrak{q}}$$

It follows that M is the compositum of $K = M^{G(M/K)}$ and $M^{I'_{\mathfrak{q}}}$, moreover $M^{I'_{\mathfrak{q}}}/E$ is unramified at *every* place above $\mathfrak{p}$, by the normality of $I'_{\mathfrak{q}}$ in $G(M/E)$. Thus $M^{I'_{\mathfrak{q}}} \subset F$ and $M \subset KF$ and the lemma follows. □

We end the section with a basic corollary which is important for our purposes. We apply lemma 3 to the special (and most interesting) case where
i) K/E is *unramified* outside the place $\mathfrak{p}$ of E;
ii) $L = H_K$ the Hilbert Class Field of K.

Corollary 4. *Let K/E be an extension of number fields unramified outside a finite place $\mathfrak{p}$ of E and totally ramified at $\mathfrak{p}$. Then the norm map $N_{K/E}\colon \mathrm{Cl}_K \longrightarrow \mathrm{Cl}_E$ induces an isomorphism*

$$(\mathrm{Cl}_K)_{G(K/E)} \simeq \mathrm{Cl}_E$$

Proof. Assume that the extension K/E is non-trivial, otherwise there is nothing to prove. From the maximality of the Hilbert Class Field it follows easily that $H_E \subset H_K$. By the properties of the Artin symbol the natural map $r\colon G(H_K/K) \to G(H_E/E)$ corresponds to the norm map $N_{K/E}\colon \mathrm{Cl}_K \to \mathrm{Cl}_E$, once we interprete the class group of E (resp. K) as the Galois group $G(H_E/E)$ (resp. $G(H_K/K)$).
The Galois group $G(H_K/E)$ is isomorphic to $G(H_K/K) \rtimes_\varphi G(K/E) = \mathrm{Cl}_K \rtimes_\varphi G(K/E)$, where the semidirect product structure φ is described by the action of $G(K/E)$ induced from the actions on fractional ideals of K (cf. remark 2).
Notice now that the only place of E, finite or infinite, that ramifies in H_K is $\mathfrak{p}$. Therefore the maximal extension of E inside L which everywhere unramified over E *coincides* with the maximal extension of E inside L unramified at every place above $\mathfrak{p}$, we denote it by E^{ur}. Moreover from the fact that $H_E \subset H_K$ we have $H_E \subset E^{ur}$. We see shortly that equality holds.
Applying lemma 3 of the section to $E \subset K \subset H_K$ we get that the natural

restriction map r induces an isomorphism

$$G(H_K/K)_{G(K/E)} \simeq G(E^{ur}/E)$$

viewing $G(H_K/K)$ as a module over $G(K/E)$. In particular E^{ur}/E is abelian and $E^{ur} = H_E$. Reformulating, we conclude that the norm map $N_{K/E}$ induces an isomorphism

$$(\mathrm{Cl}_K)_{G(K/E)} \simeq \mathrm{Cl}_E$$

and the corollary follows. □

Remark 4. Denote by S_r the set of real places of E. The extension K/E considered in corollary 4 is unramified at every place in S_r. If we drop such assumption, so that K/E is unramified outside $S_r \cup \{\mathfrak{p}\}$, the stamement of the corollary remains valid if we replace the class groups Cl_K and Cl_E by the narrow class groups Cl_K^+ and Cl_E^+ as one can see without difficulties.

2. The main theorems

Let G a finite group and A a finite G module. By this we mean that A is a finite abelian group with an action of G by automorphisms. Denote the Pontrjagin dual of A by $\widehat{A}$, it inherits a natural structure of G-module via the formula

$$g.\chi(a) = \chi(g^{-1}.a)$$

for $\chi \in \hat{A}$, $g \in G$ and $a \in A$. For a finite set X we denote its cardinality by $|X|$.

Lemma 5. *If p is a prime number and G is a p–group then $|A_G| \equiv |A| \pmod{p}$.*

Proof. If a finite p-group G acts on a finite set X denote the fixed subset by X^G. Then $|X^G| = |X| \pmod{p}$, indeed $X - X^G$ is union of non trivial G-orbits. Applying this to $\widehat{A}$ we obtain $|(\hat{A})^G| \equiv |\hat{A}| \pmod{p}$. Now since $\widehat{A_G} \simeq \widehat{A}^G$ and any finite G–module has the same cardinality as its dual we have $|A_G| \equiv |A| \pmod{p}$. □

Lemma 6. *Assume that, for a p-group G, a finite G-module A decomposes as direct product $A_1 \times \cdots \times A_n$ of invariant G-submodules.*
Then $A_G \simeq (A_1)_G \times \cdots \times (A_n)_G$.

Proof. This easily follows, for example, from the description of $\mathbf{D}A$ in terms of its generators. They are of the form $g.a - a$, with $g \in G$ and $a \in A$ and writing a as $(a_1, \ldots, a_n)$ with $a_i \in A_i$ we see that $g.a - a = (g.a_1 - a_1, \ldots, g.a_n - a_n)$, thus $\mathbf{D}A = \mathbf{D}A_1 \times \cdots \times \mathbf{D}A_n$. □

We are now ready to prove the main theorem of the paper.

Theorem 7. *Let p be a prime number and K/E be a finite Galois extension of number fields whose Galois group $G(K/E)$ is a p-group. Assume that K/E is unramified outside a finite place $\mathfrak{p}$ of E and totally ramified at $\mathfrak{p}$. Then for any prime number l*

$$h_K^{(l)} \equiv h_E^{(l)} \pmod{p}$$

In particular

$$h_K \equiv h_E \pmod{p}$$

Proof. Set $G = G(K/E)$, corollary 6 of section 1 says that

$$(\mathrm{Cl}_K)_G \simeq \mathrm{Cl}_E$$

The product of the l–Sylow subgroups of Cl_K gives a decomposition of Cl_K into G–submodules:

$$\mathrm{Cl}_K \simeq \Pi_l \, \mathrm{Cl}_K^{(l)}$$

From lemma 6 above we have that

$$\mathrm{Cl}_E = \Pi_l (\mathrm{Cl}_K^{(l)})_G$$

This gives the decomposition of Cl_E into its l–Sylow subgroups, so that $\mathrm{Cl}_E^{(l)} = (\mathrm{Cl}_K^{(l)})_G$. Applying now lemma 5 we obtain $|\, \mathrm{Cl}_E^{(l)} \,| \equiv |\, \mathrm{Cl}_K^{(l)} \,| \pmod{p}$, and the theorem is proved. □

In the special case when $G(K/E)$ is *cyclic* we describe stronger congruences. If $|G(K/E)| = p^n$, denote the subfield of K of degree p^i over E by K_i, for $0 \leq i \leq n$.

Theorem 8. *Assume moreover that $G(K/E)$ is cyclic of order p^n then for any prime l*

$$h_{K_i}^{(l)} \equiv h_{K_{i-1}}^{(l)} \pmod{p^i}$$

In particular

$$h_{K_i} \equiv h_{K_{i-1}} \pmod{p^i}$$

Proof. For an integer i, $0 \leq i \leq n$, set $G_{n-i} = G(K_n/K_i)$, it is the subgroup of $G(K_n/K_0)$ which fixes K_i, set also $G = G_n = G(K/K_0)$. If l is any prime number, we have $\mathrm{Cl}_{K_i}^{(l)} = (\mathrm{Cl}_{K_n}^{(l)})_{G_{n-i}}$, as remarked in the proof of theorem 7. The dual statement is

$$\widehat{\mathrm{Cl}_{K_i}^{(l)}} = \widehat{\mathrm{Cl}_{K_n}^{(l)}}^{G_{n-i}}$$

Since G is cyclic of order p^n we have

$$G_{n-i} = G^{p^i}$$

where G^{p^i} is the subgroup of p^i–th powers of G. Making the previous equality explicit we obtain

$$\widehat{\mathrm{Cl}_{K_i}^{(l)}} = \widehat{\mathrm{Cl}_{K_n}^{(l)}}^{G_{n-i}} = \{\chi \in \widehat{\mathrm{Cl}_{K_n}^{(l)}} | \chi^s = \chi, \text{ for all } s \in G_{n-i}\}$$

Fix now a generator $\sigma \in G$, then

$$\widehat{\mathrm{Cl}_{K_i}^{(l)}} = \widehat{\mathrm{Cl}_{K_n}^{(l)}}^{G_{n-i}} = \{\chi \in \widehat{\mathrm{Cl}_{K_n}^{(l)}} | \chi^{\sigma^{p^i}} = \chi\}$$

This implies that $\widehat{\mathrm{Cl}_{K_i}^{(l)}}$ is given by the disjoint union of the G-orbits of $\widehat{\mathrm{Cl}_{K_n}^{(l)}}$ whose length divides p^i. Setting

$$h_i^{(l)} = |\{G\text{-orbits in } \widehat{\mathrm{Cl}_{K_n}^{(l)}} \text{ of length } p^i\}|$$

we see that
$h_{K_0}^{(l)} = h_0^{(l)}$,
$h_{K_1}^{(l)} = h_0^{(l)} + h_1^{(l)} p$,
$h_{K_2}^{(l)} = h_0^{(l)} + h_1^{(l)} p + h_2^{(l)} p^2$,
...
$h_{K_n}^{(l)} = h_0^{(l)} + h_1^{(l)} p + h_2^{(l)} p^2 + \ldots + h_n^{(l)} p^n$,
and
$h_{K_i}^{(l)} = h_{K_{i-1}}^{(l)} + h_i^{(l)} p^i$.
This completes the proof. □

Remark 5. Let l a prime number, denote by $H_K^{(l)}$ the maximal unramified abelian l–extension of K. We have that $H_K^{(l)} \subset H_K$ and $G(H_K/H_K^{(l)}) \simeq \mathrm{Cl}_K^{(l)}$. The integers $h_i^{(l)}$ just defined are related to the complex representation theory of $G(H_K^{(l)}/E)$. Using the method of Mackey and Wigner for small groups (cf. [3], §8.2), one can show that every irreducible representation of

$G(H_K^{(l)}/E)$ has degree p^i, with $0 \leq i \leq n$, and the number of non-isomorphic, p^i–th dimensional irreducible representations is

$$p^{n-i}h_i^{(l)} = p^{n-2i}(h_{K_i}^{(l)} - h_{K_i-1}^{(l)})$$

where we set $h_{K_{-1}}^{(l)} = 0$.

3. Applications

We conclude the paper with few applications. We first apply theorem 8 to the extension $\mathbf{Q}(\mu_{p^{m+1}})/\mathbf{Q}(\mu_p)$, where p is an odd prime and $m \geq 1$ is an integer. We generalize the known fact (cf. [1]) that for an odd prime p

$$p \textit{ is regular} \Leftrightarrow \ p \text{ doesn't divide } h_{\mathbf{Q}(\mu_{p^{m+1}})} \text{ for } m \geq 1$$

Proposition 9. *Let p be an odd prime and l be any prime. Then for any $m \geq 1$*

$$h_{\mathbf{Q}(\mu_{p^{m+1}})}^{(l)} \equiv h_{\mathbf{Q}(\mu_{p^m})}^{(l)} \pmod{p^m}$$

Proof. Apply Theorem 8 to the extension $\mathbf{Q}(\mu_{p^{m+1}})/\mathbf{Q}(\mu_p)$ which is known to be a cyclic p–extension unramified outside the unique prime of $\mathbf{Q}(\mu_p)$ above the rational prime p. □

In the next two applications we consider a Galois extension K/E unramified outside a finite place $\mathfrak{p}$ of E and totally ramified at $\mathfrak{p}$. We do not require $G(K/E)$ to be a p–group.
The first fact concerns the 2-part of Cl_K under the assumption that h_E is odd.

Proposition 10. *Assume that h_E is odd. Then there are no everywhere unramified $\mathbf{Z}/2\mathbf{Z}$ extensions of K which are Galois over E. In particular, if h_K is even then $\mathrm{Cl}_K^{(2)}$ is not cyclic.*

Proof. If h_K is odd, there's nothing to prove. Assume then that h_K even and let L/K be an unramified $\mathbf{Z}/2\mathbf{Z}$ extension which is Galois over E. Then $G(K/E)$ acts on $G(L/K) = \mathbf{Z}/2\mathbf{Z}$ and the action is forced to be trivial so that $G(L/K)_{G(K/E)} = G(L/K)$. Applying now lemma 3 we see that E has a $\mathbf{Z}/2\mathbf{Z}$–unramfied extension F inside K, contrary to the assumption that h_E is odd. We conclude that there is no such an L.
Consider the 2-part of Cl_K. The group $G(K/E)$ acts on it and, from the first

part of the proposition, it follows that there are no invariant subgroups of index 2. This means that there are at least 2 distinct, isomorphic subgroups of index 2. Therefore, in particular, $\mathrm{Cl}_K^{(2)}$ cannot be cyclic. □

Iwasawa gave a proof of the same fact under slightly different assumptions on the extension K/E (cf. [2], cor. to Theorem 4). His method is different and it is based on lower estimates on the rank of Cl_K^2 as abelian group.

Proposition 11. *If $G(K/E) = G$ is cyclic, then $|\,\mathrm{Cl}_E\,| = |\,\mathrm{Cl}_K^G\,|$.*

Proof. This follows from the fact that, when G is cyclic, the Herbrand quotient of any finite G-module A is 1 (cf. [4], Chap. VIII, §5 Prop. 8). Indeed, for $A = \mathrm{Cl}_K$ this implies that $|A_G| = |A_G|$, showing the required statement. □

We can give a direct proof of the proposition as corollary of the following lemma.

Lemma 12. *Let G be a cyclic group and A a finite G-module. Denote with $\hat{A}$ the dual module of A. Then there is a G-equivariant set-bijection between A and $\hat{A}$. In particular $|\hat{A}^G| = |A^G|$.*

Proof. If M is any finite G module and d is a divisor of $|G|$, denote with $l_M(d)$ the number of G-orbits of length d in M. If $g \in G$, set $\chi_M(g) = |M^g|$, the cardinality of the submodule fixed by g.
Since G is cyclic, the lemma is equivalent to showing that for any divisor d of $|G|$ we have $l_A(d) = l_{\hat{A}}(d)$. In fact for any such d there exists, up to isomorphism, only *one* transitive G-action on a set of cardinality d. The knowledge of the function l_M is equivalent to the knowledge of the character χ_M. To see this, fix a generator σ of G. Then if d divides $|G|$ we have:

$$l_M(d) = \frac{1}{d}[\chi_M(\sigma^d) - \sum_{d'} \chi_M(\sigma^{d'})]$$

where d' in the sum ranges through all positive divisors of d other than 1 and d itself. On the other hand

$$\chi_M(\sigma^k) = \sum_{d|(k,|G|)} d \cdot l_M(d)$$

The lemma is then reduced to proving that $\chi_A = \chi_{\hat{A}}$. Consider $\mathbf{C}[A]$, the

free complex vector space on A. It is a complex linear representation π_A of G whose character is χ_A previously defined. Similarly, $\pi_{\hat{A}}$ is a representation with character given by $\chi_{\hat{A}}$ and it is easy to see that $\pi_{\hat{A}}$ is isomorphic to $\widehat{\pi_A}$, the dual representation of π_A. Thus $\chi_A = \overline{\chi_{\hat{A}}}$ and, since χ_A is real valued (even ineteger valued), $\chi_A = \chi_{\hat{A}}$ and the lemma follows. □

Remark 6. If we allow the extension K/E to be *ramified* at some real place of E then the previous proposition remains valid if we replace Cl_E and Cl_K by the narrow class groups Cl_E^+ and Cl_K^+.

Remark 7. If p is any odd prime and $m \geq 1$ is an integer, we have that there are no non–trivial ideal classed of $\mathbf{Q}(\mu_{p^m})$ invariant under the action of $(\mathbf{Z}/p^m\mathbf{Z})^*$. This follows from the previous remark applied to the extension $\mathbf{Q}(\mu_{p^m})/\mathbf{Q}$.

References

[1] K. Iwasawa, *A note on class numbers of algebraic number fields.* Abh. Math. Sem. Univ. Hamburg, **20** (1956), 257–258.

[2] K. Iwasawa, *A note on ideal class groups.* Nagoya Math.J., **27** (1966), 239–247.

[3] J.-P. Serre, *Représentations linéaires des groupes finis.* Hermann, Cinquième edition, (1998).

[4] J.-P. Serre, *Corps Locaux* Hermann, Quatrième édition, corrigée (2004).

Department of Mathematics, University of Utah, 155 South 1400 East, Salt Lake City, UT 84112-0090, USA

E-mail address: centeleg@math.utah.edu