On arithmetically equivalent fields with distinct p-class numbers

Bart de Smit*
Universiteit Leiden

November 2 2000—**preliminary version**

Abstract

For each odd prime number p we show that number fields with the same zeta-function but distinct p-class numbers have degree at least $2p+2$. Two such number fields of degree $2p+2$ are shown to have a common Galois closure with Galois group $\mathrm{GL}_2(\mathbb{F}_p)/(\mathbb{F}_p^*)^2$.

1. Introduction

Two number fields are said to be *arithmetically equivalent* if they have the same zeta-function. Such fields have the same degree, the same normal closure, the same discriminant and the same product of class number and regulator. Two arithmetically equivalent fields with distinct 2-parts of the class numbers were found in 1994 [3]. The question then arose whether for a given odd prime p there exist two arithmetically equivalent number fields with distinct p-class numbers.

Fields that could provide examples of this, of degree $2p+2$, were proposed in [2]: one takes a Galois extension of $\mathbb{Q}$ with Galois group $G_p = \mathrm{GL}_2(\mathbb{F}_p^*)/\mathbb{F}_p^{*2}$ and considers the invariant fields of the subgroups $H_p = \left(\begin{smallmatrix} \square & * \\ 0 & * \end{smallmatrix}\right)/\square$ and $H_p' = \left(\begin{smallmatrix} * & * \\ 0 & \square \end{smallmatrix}\right)/\square$. Here "$\square$" denotes the squares in $\mathbb{F}_p^*$.

One can find explicit equations for such fields by considering torsion points on elliptic curves [2]. This way, examples of arithmetically equivalent fields with distinct p-class numbers have been found for $p=3$ and later for $p=5$ [5]. For $p \geq 7$ it is presently not known whether such examples exist.

The goal of this paper is to show that the triple (G_p, H_p, H_p') is the unique Galois configuration of minimal degree for this setting. More precisely, we prove the following theorem. Throughout the paper p denotes an odd prime number.

*supported by the Mathematical Sciences Research Institute and the Koninklijke Nederlandse Akademie van Wetenschappen.

Theorem 1. *Let K and L be arithmetically equivalent number fields of degree d with non-isomorphic p-class groups. Then we have $d \geq 2p+2$. If $d = 2p+2$, and M denotes the Galois closure of K, then there is an isomorphism $\mathrm{Gal}(M/\mathbb{Q}) \cong G_p$ so that K is the fixed field of H_p and L is isomorphic to the fixed field of H'_p.*

The proof of this theorem is by a standard deduction from our main group theoretic result, which we is formulated below as Theorem 2. We first introduce the terminology of linear equivalence. When a group G acts on a set X, and R is a commutative ring with 1, then we write $R[G]$ for the group ring, and $R[X]$ for the free R-module on basis X, which has an $R[G]$-module structure because G permutes the basis vectors. If G acts on finite sets X and Y then we say that X and Y are linearly equivalent over R if the permutations modules $R[X]$ and $R[Y]$ over $R[G]$ are isomorphic.

To make the passage to group theory, one considers the sets X and Y of field embeddings of K and L respectively, into $\overline{\mathbb{Q}}$. These sets have an action of the Galois group $\Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. It is known that K and L are arithmetically equivalent if and only if the Γ-sets X and Y are linearly equivalent over $\mathbb{C}$. Moreover, K and L have isomorphic p-class groups when X and Y are linearly equivalent over $\mathbb{Z}_p$. See [7] and [2] for details and examples. Thus, Theorem 1 is a consequence of the following result.

Theorem 2. *Let G be a group acting faithfully and transitively on two sets X and Y of cardinality at most $2p+2$. If X and Y are linearly equivalent over $\mathbb{C}$, but not over $\mathbb{Z}_p$, then there is an isomorphism $\varphi\colon\ G_p \to G$ so that X and Y, viewed as G_p-sets via φ are G_p-isomorphic to G_p/H_p and G_p/H'_p respectively.*

The rest of this paper is devoted to proving Theorem 2. We will use Conlon's induction theorem in integral representation theory, Burnside's theorem on permutation groups of prime degree, a classification result of Feit concerning Zassenhaus groups, and a computation of J. Quer concerning central extensions of $\mathrm{PGL}(2, \mathbb{F}_p)$ and $\mathrm{PSL}_2(\mathbb{F}_p)$ by a cyclic group of order 2. We present these results as "Facts" with references as we need them in the proof.

In [2] an easy argument is given that shows that the G_p-sets G_p/H_p and G_p/H'_p are indeed linearly equivalent over $\mathbb{C}$, but not over $\mathbb{Z}_p$. Note that G_p has an automorphism switching H_p to H'_p: take the inverse transpose and conjugate by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Thus, the conclusion of Theorem 2 is symmetric in X and Y.

The notation C_n will always denote a cyclic group of order n.

2. Combinatorial criteria for linear equivalence

We will frequently make use of two properties of linear equivalence. By considering the rank of the module of coinvariants of the permutation modules one sees that every subgroup of G has the same number of orbits on each of two G-sets which are linearly equivalent over some non-zero ring. If N is a normal subgroup of G, then the N-orbits of a G-set X form a G-set $N\backslash X$ and if X and Y are linearly equivalent G-sets over a certain ring, then so are $N\backslash X$ and $N\backslash Y$.

We only use linear equivalence over $\mathbb{C}$ and over $\mathbb{Z}_p$. Fortunately, there are very explicit group theoretic conditions that determine whether two sets are linearly equivalent over these rings. Over $\mathbb{C}$, representation theory implies that two G-sets X and Y are linearly equivalent if and only if every group element of G fixes the same number of elements on X and on Y. Over $\mathbb{Z}_p$, we use the theory of "Conlon induction" [1]. We say that a finite group G is cyclic modulo p if it has a normal p-Sylow subgroup S so that G/S is cyclic.

Fact 1 (Conlon). *Let G be a finite group, and let X and Y be finite G-sets. Then we have $\mathbb{Z}_p[X] \cong_{\mathbb{Z}_p[G]} \mathbb{Z}_p[Y]$ if and only if every subgroup H of G which is cyclic modulo p has the same number of fix-points on X and on Y.*

Applying this criterion to the situation of Theorem 2, we see that there is a subgroup C of G which is cyclic modulo p and for which $\#X^C \neq \#Y^C$.

Consider the normal Sylow-p-subgroup U of C. Since $p^2 > 2p+2$ all U-orbits of X have length 1 or p. Note that $U \neq 1$ because otherwise C would be cyclic, and $\#X^C = \#Y^C$. The number of U-orbits is the same on X and on Y, so the number of non-trivial U-orbits is the same on X and on Y. This number is 1 or 2 because $3p > 2p + 2 \geq \#X$.

The C-sets $U\backslash X$ and $U\backslash Y$ are linearly equivalent over $\mathbb{C}$, and since C/U is cyclic they have the same number of fix-points under C. Now $\#(U\backslash X)^C - \#X^C$ is the number of C-closed U-orbits of length p. It is distinct from the number of C-closed U-orbits of Y. Thus, U has 2 non-trivial orbits on X and on Y, and after switching X and Y if necessary we can assume that X contains one C-orbit of length $2p$, while Y contains 2 of length p. Switching X and Y is harmless because, as we mentioned already, the conclusion of the theorem is symmetric in X and Y.

Since C has the same number of C-orbits on X and on Y, there must be at least two more points in X and in Y. But $\#X \leq 2p + 2$, so it follows that $\#X = 2p + 2$, and we now know that G has a subgroup C with orbit lengths $2p, 1, 1$ on X and $p, p, 2$ on Y.

3. The point stabilizer

Let $F = \{g \in G : gx = x \text{ for all } x \in X^C\}$. Then $C \subset F$ and F has orbit lengths $2p, 1, 1$ on X, so it has 3 orbits on Y also, and they have lengths $p, p, 2$. We let Y_p be an F-orbit of length p and we let Y_2 be the F-orbit of length 2.

Let us show first that F acts faithfully on Y_p. Let K be the kernel of the action of F on Y_p, and let $K' \subset K$ be the kernel of the action of F on $Y_p \cup Y_2$. Then K' is normal in F, so the number of K'-orbits on X is 2 plus a divisor of $2p$, and on Y it is $p + 2$ plus a divisor of p. That means that $K' = 1$, and that and K acts faithfully on Y_2, so $\#K \mid 2$. Since K is normal in F and of order coprime to p, it acts trivially on the two F-orbits of length p of Y, so the number of K-orbits on Y is $2p+1$ or $2p+2$. And on X it is 2 plus a divisor of $2p$. So $K=1$ and F acts faithfully on Y_p.

We let N be the kernel of the action of F on Y_2. Then N is a normal subgroup of F of index 2. Note that N has either one or two orbits of the same length on every transitive F-set, and that N has orbit lengths $p,p,1,1$ on Y. Since N has 4 orbits on X as well, it follows that N has orbit lengths $p,p,1,1$ on X as well. So the F-set X has two blocks of length p which are switched by the elements of F that are not in N. Thus, such an element g has exactly 2 odd length orbits on X, namely the fix-points. Since X and Y are isomorphic over the cyclic group $\langle g\rangle$ the same is true on Y. Since $\#Y_p$ is odd, g has an odd number of odd length orbits on Y_p, so it has a unique fix-point on Y_p. If N were 2-transitive on Y_p then there would be an element $n\in N$ so that gn would fix at least two elements of Y_p. But $gn\in F$ and $gn\notin N$, so the above argument applied to gn instead of g would give a contradiction. Thus, N is not 2-transitive on Y_p.

Fact 2 (Burnside). *Every faithful transitive action of a non-solvable group on a set of p elements is 2-transitive.*

See [4, Thm. 3.5B] for a proof. We deduce that N is solvable and therefore F is solvable too. By considering a non-trivial elementary abelian normal l-subgroup of F, we see that $l=p$, and that F is contained in $C_p\rtimes\mathbb{F}_p^*$, where C_p denotes a cyclic group or order p. Since $\#C$ is even, we see that

$$2p\mid \#F\mid p(p-1).$$

Note also that N is a characteristic subgroup of F: it is generated by the squares of elements of F.

We now show that F is in fact a point stabilizer of the action of G on X. Let T be the point stabilizer in G of an element $x\in X^F$. Then $F\subset T$ and T has orbit lengths $2p+1,1$ or $2p,1,1$ on X. If it is $2p,1,1$ then $T=F$ and we are done so let us assume it is $2p+1,1$, so that $[T:F]=2p+1$. If T has an orbit of length 2 on Y, then it has a normal subgroup T' of index 2, which must be transitive on the T-orbit of size $2p+1$ of X. But then T' has 2 orbits on X and at least 3 on Y: contradiction. Thus, T has no orbit of length 2 on Y, and its two orbits on Y have length p and $p+2$. The subgroup N of T has index $2(2p+1)$ and it has orbit lengths $p,p,1,1$ on Y, so it is contained in a point stabilizer of a point in the T-orbit of length $p+2$ of Y, which in turn has index $p+2$ in T. It follows that $p+2\mid 4p+2$, which implies $p+2\mid 6$, so we have a contradiction. Thus, $T=F$.

4. Block structure and the Borel subgroup

It follows from the previous step that we have an equivalence relation on X with equivalence classes of size 2, where two points are equivalent if they have the same point stabilizer in G. We denote the set of equivalence classes by $\overline{X}$. Let Z be the kernel of the action of G on $\overline{X}$. We claim that Z is a central normal subgroup of G of order 2.

Let B be the point stabilizer in G of the element X^F of $\overline{X}$. Then F is a normal subgroup of B of index 2. The subgroup N of F is the subgroup generated by the squares in F, so it is characteristic in F and it is normal of index 4 in B.

The orbit lengths of B on X are $2p, 2$. Thus, F acts on the 4 elements of $N\backslash X$ as a two-cycle, and B has two orbits of length 2 on $N\backslash X$. It follows that B/N acts on a set of size 4 as a faithful non-transitive $C_2 \times C_2$. We deduce that N is the subgroup of B generated by squares.

The kernel of F on $\bar{X}$ is a normal subgroup of 2-power order, but any F in $C_p \rtimes \mathbb{F}_p^*$ containing C_p has only a trivial normal subgroup of 2-power order. Thus, F acts faithfully on $\overline{X}$ and $Z \cap F = 1$.

The group B has 2 orbits on $\overline{X}$, of length 1 and p. The image of the solvable group B in the symmetric group on $\overline{X}$ is therefore a Frobenius group on p elements, so it has a cyclic 2-Sylow subgroup. But B has a quotient $C_2 \times C_2$, so Z is a non-trivial normal subgroup of B. Since $Z \cap F = 1$ and $[B : F] = 2$ we have $\#Z = 2$ and $B = F \times Z$. It also follows that $\overline{X} = Z\backslash X$.

There are three intermediate groups of the extension $N \subset B$. They are F and NZ and we denote the third by F'. Note that F and Z act non-trivially on Y_2, so F' fixes two points of Y. Thus, F' is a point stabilizer for the action of G on Y. Moreover, the G-set $\overline{Y} = Z\backslash Y$ is G-isomorphic to $\overline{X}$: both are transitive with point stabilizer B.

We know that our group G fits in a short exact sequence

$$0 \to Z \to G \to \overline{G} \to 0,$$

with $\#Z = 2$. We claim that this extension is not split. Suppose it is split, and let H be a subgroup of G which under the map $G \to \overline{G}$ maps isomorphically to $\overline{G}$. If H is not transitive on X, then it has two orbits, each H-isomorphic to $\overline{X}$, and X is the G-set induced by the H-set $\overline{X}$. But then H also has two orbits on Y, and since $\overline{Y} \cong_{\overline{G}} \overline{X}$, we then have $X \cong Y$: contradiction. Now suppose that H is transitive on X so that H is also transitive on Y. The group $B \cap H$ has index 2 in B and it does not meet Z, so it is either F or F'. But the point stabilizers $H \cap F$ and $H \cap F'$ of H on X and Y have index 2 in F and F' respectively, so we have a contradiction. Thus, the sequence is non-split.

5. Zassenhaus groups

The point stabilizer $\overline{B} = B/Z$ of the action of $\overline{G} = G/Z$ on $\overline{X}$ is isomorphic to F, and it has orbits $p, 1$ on $\overline{X}$. Thus, $\overline{G}$ acts 2-transitively on $\overline{X}$. Moreover, its point stabilizer acts as a Frobenius group on the orbit of length p. In particular, every non-trivial element of $\overline{G}$ has at most 2 fix-points on $\overline{X}$. This is the defining property of Zassenhaus groups in [4] (in [6] there is a slightly stricter definition). The next result allows us to almost pin down the group $\overline{G}$.

Fact 3 (Feit). *A 2-transitive group on $p+1$ elements in which each non-trivial group element has at most 2 fix-points is, as a permutation group, isomorphic to one of the following:* $\mathrm{PGL}(2,\mathbb{F}_p)$ *on* $\mathbb{P}^1(\mathbb{F}_p)$ *or* $\mathrm{PSL}(2,\mathbb{F}_p)$ *on* $\mathbb{P}^1(\mathbb{F}_p)$ *or, if* $p+1=2^l$ *with l prime,* $\mathbb{F}_{2^l} \rtimes (\mathbb{F}_{2^l}^* \rtimes C_l)$ *on* $\mathbb{F}_{2^l}$.

Here C_l denotes the cyclic Galois group $\mathrm{Gal}(\mathbb{F}_{2^l}/\mathbb{F}_2)$ of order l. See [6, Ch. XI, Thm. 6.9] for a proof.

We show first that we can dismiss the third case for our group $\overline{G}$. If $p=3$ then the first and third group are just S_4 on 4 elements. For $p>3$ with $2^l=p+1$ both l and 2^l-1 are odd, so then a point stabilizer of $\mathbb{F}_{2^l}$ has odd order in $\mathbb{F}_{2^l} \rtimes (\mathbb{F}_{2^l}^* \rtimes C_l)$. But we know that F maps injectively to $\overline{G}$, and F has even order, so we are not in this case. Thus, we see that there is an isomorphism from $\overline{G}$ to $\mathrm{PGL}(2,\mathbb{F}_p)$ or to $\mathrm{PSL}(2,\mathbb{F}_p)$, for which the image of $\overline{B}$ is a point stabilizer of the projective line. By applying an inner automorphism of the projective linear group we can assume that the image of $\overline{B}$ is the Borel subgroup $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)/*$ of either projective linear group.

6. Computing a central extension

We showed in Section 4 that G is a non-trivial central extension of $\overline{G}$ by C_2. Moreover, the restriction of the extension to $\overline{B}$ is the trivial extension B. Thus the extension class of G is a non-trivial element of the kernel of the map

$$h\colon\ H^2(\overline{G},C_2) \to H^2(\overline{B},C_2).$$

We now use the classification result of the last section, and compute the kernel of h in the two cases.

Fact 4. *We have* $H^2(\mathrm{PGL}(2,\mathbb{F}_p),C_2) \cong C_2 \times C_2$ *and* $H^2(\mathrm{PSL}(2,\mathbb{F}_p),C_2) \cong C_2$.

We refer to [8] for a proof in a more general setting. Suppose that we have an isomorphism $\overline{G} \cong \mathrm{PSL}_2(\mathbb{F}_p)$ as in the last section. Consider the extension

$$0 \to C_2 \to \mathrm{SL}_2(\mathbb{F}_p) \to \mathrm{PSL}_2(\mathbb{F}_p) \to 0.$$

The Borel subgroup $\left(\begin{smallmatrix} t & * \\ 0 & t^{-1} \end{smallmatrix}\right)$ of $\mathrm{SL}_2(\mathbb{F}_p)$ has cyclic 2-Sylow subgroup, so this extension restricts to a non-trivial element of $H^2(\overline{B},C_2)$. Thus, the map h defined above is non-trivial, and by Fact 4 it follows that h is injective. This is a contradiction.

By the classification result in the last section we now know that there is an isomorphism $\overline{G} \to \mathrm{PGL}_2(\mathbb{F}_p)$ with $\bar{B}$ mapping to the Borel subgroup $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)/*$. Consider $\mathrm{PGL}_2(\mathbb{F}_p)$ as a subgroup of $\mathrm{PSL}_2(\mathbb{F}_{p^2})$ and consider its C_2-extension

$\mathrm{SL}_2(\mathbb{F}_{p^2})$. The induced C_2-extension of $\overline{B}$ is contained in the Borel subgroup $\left(\begin{smallmatrix} t & * \\ 0 & t^{-1} \end{smallmatrix}\right)$ of $\mathrm{SL}_2(\mathbb{F}_{p^2})$, which has a cyclic 2-Sylow subgroup. Thus, h is not the zero map, and by Fact 4 its kernel has order at most 2.

But we know that G_p acting on G_p/H_p and G_p/H'_p satisfy the conditions of Theorem 2, so G_p represents the unique non-zero element in the kernel of h. It follows that there is an isomorphism $\varphi\colon\ G \to G_p$ mapping Z to the scalar subgroup $\mathbb{F}_p^*/\mathbb{F}_p^{*2}$ of G_p, and B to $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)/\square$.

Recall that F and F' are the only two distinct subgroups of B of index 2 that do not contain Z. Note that H_p and H'_p are the two subgroups of index 2 in $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)/\square$. not containing non-trivial scalars. By composing φ with an automorphism of G_p that switches H_p and H'_p if necessary, we therefore find an isomorphism $G \to G_p$ as stated in Theorem 2.

References

[1] Curtis C.W., Reiner I., *Methods of Representation Theory, Volume II*, John Wiley and Sons, New York 1994.

[2] B. de Smit, *Generating arithmetically equivalent number fields with elliptic curves*, pp. 392–399 in: J.P. Buhler (Ed.), *Algorithmic Number Theory*, Lecture Notes in Computer Science **1423**, Springer-Verlag, 1998.

[3] B. de Smit, R. Perlis, *Zeta functions do not determine class numbers*, Bull. Amer. Math. Soc. (N.S.) **31** (1994), 213–216.

[4] J. Dixon, B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics **163**. Springer-Verlag, New York, 1996.

[5] G. Dyer, *Two arithmetically equivalent number fields with class number quotient five*, preprint, 1999, Mathematical Research Experiences for Undergraduates at Louisiana State University, LEQS.

[6] B. Huppert, N. Blackburn, *Finite groups. II*, Grundlehren der Mathematischen Wissenschaften **242**, Springer-Verlag, Berlin-New York, 1982.

[7] N. Klingen, *Arithmetical similarities*, Oxford University Press, 1998.

[8] J. Quer, *Liftings of projective 2-dimensional Galois representations and embedding problems*, J. Algebra **171** (1995), 541–566.