Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 340 (2005) 411–414
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Number Theory

A counter example to Malle's conjecture on the asymptotics of discriminants

Jürgen Klüners

Universität Kassel, Fachbereich Mathematik/Informatik, Heinrich-Plett-Straße 40, 34132 Kassel, Germany

Received 20 October 2004; accepted after revision 1 February 2005

Presented by Christophe Soulé

Abstract

In this Note we give a counter example to a conjecture of Malle which predicts the asymptotic behavior of the counting functions for field extensions with given Galois group and bounded discriminant. ***To cite this article: J. Klüners, C. R. Acad. Sci. Paris, Ser. I 340 (2005).***

Résumé

Un contre-exemple à la conjecture de Malle sur le nombre de corps de discriminant borné. Dans cette Note, nous donnons un contre-exemple à une conjecture de Malle, qui prédit le comportement asymptotique du nombre de corps de clôture galoisienne fixée et discriminant borné. ***Pour citer cet article : J. Klüners, C. R. Acad. Sci. Paris, Ser. I 340 (2005).***

1. Introduction

Let $G \leqslant S_n$ be a finite transitive permutation group and k be a number field. We say that a finite extension K/k has Galois group G if the normal closure $\widehat{K}$ of K/k has Galois group isomorphic to G and K is the fixed field in $\widehat{K}$ under a point stabilizer of G. By abuse of notation we will write $\mathrm{Gal}(K/k) = G$ in this situation. We let

$$Z(k, G; x) := \#\bigl\{K/k\colon \mathrm{Gal}(K/k) = G,\ \mathrm{N}_{k/\mathbb{Q}}(d_{K/k}) \leqslant x\bigr\}$$

be the number of field extensions of k (inside a fixed algebraic closure $\overline{\mathbb{Q}}$) of relative degree n with Galois group permutation isomorphic to G (as explained above) and norm of the discriminant $d_{K/k}$ bounded above by x. It is well known that the number of extensions of k with bounded norm of the discriminant is finite, hence $Z(k, G; x)$ is finite for all G, k and $x \geqslant 1$.

E-mail address: klueners@mathematik.uni-kassel.de (J. Klüners).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2005.02.010

Malle [7,8] has given a precise conjecture about the asymptotic behavior of the function $Z(k, G; x)$ for $x \to \infty$. In order to state it, we introduce some group theoretic invariants of permutation groups.

Definition 1.1. Let $1 \neq G \leqslant S_n$ be a transitive subgroup acting on $\Omega = \{1, \dots, n\}$.

(i) For $g \in G$ we define the index $\operatorname{ind}(g) := n -$ the number of orbits of g on Ω.
(ii) $\operatorname{ind}(G) := \min\{\operatorname{ind}(g)\colon\ 1 \neq g \in G\}$.
(iii) $a(G) := \operatorname{ind}(G)^{-1}$.

Since all elements in a conjugacy class C of G have the same index we can define $\operatorname{ind}(C)$ in a canonical way. The absolute Galois group of k acts on the set of conjugacy classes of G via the action on the $\overline{\mathbb{Q}}$-characters of G. The orbits under this action are called k-conjugacy classes.

Definition 1.2. For a number field k and a transitive subgroup $1 \neq G \leqslant S_n$ we define:

$$b(k, G) := \#\big\{C\colon\ C \text{ } k\text{-conjugacy class of minimal index } \operatorname{ind}(G)\big\}.$$

Now we can state the conjecture of Malle [8], where $f(x) \sim g(x)$ is a notation for $\lim_{x\to\infty} f(x)/g(x) = 1$.

Conjecture 1.3 (Malle). *For all number fields k and all transitive permutation groups $1 \neq G$ there exists a constant $c(k, G) > 0$ such that*

$$Z(k, G; x) \sim c(k, G) x^{a(G)} \log(x)^{b(k,G)-1},$$

where $a(G)$ and $b(k, G)$ are given as above.

This conjecture is proved for Abelian groups [9]. For all number fields k and all nilpotent groups G it is shown in [6] that

$$\limsup_{x\to\infty} \frac{\log Z(k, G; x)}{\log x} \leqslant a(G).$$

If we furthermore assume that G is in its regular representation, i.e., we count normal nilpotent number fields, we get:

$$\lim_{x\to\infty} \frac{\log Z(k, G; x)}{\log x} = a(G).$$

For more results see also the survey articles [1,2]. In the following we use the notation $f(x) = \mathrm{O}(g(x))$, if $\limsup_{x\to\infty} f(x)/g(x) < \infty$. Furthermore, we write $f(x) = \theta(g(x))$, if $f(x) = \mathrm{O}(g(x))$ and $g(x) = \mathrm{O}(f(x))$.

2. The counter example

We present a counter example to Conjecture 1.3 for $k = \mathbb{Q}$ and the wreath product $G := C_3 \wr C_2 = C_3^2 \rtimes C_2 \leqslant S_6$ of order 18, where C_n is the cyclic group of order n.

Theorem 2.1. *Conjecture* 1.3 *does not hold for $k = \mathbb{Q}$ and $G = C_3 \wr C_2$.*

Proof. In the following we count all field towers $L/K/\mathbb{Q}$ such that $\operatorname{Gal}(L/K) = C_3$ and $\operatorname{Gal}(K/\mathbb{Q}) = C_2$. Therefore the Galois group of $L/\mathbb{Q}$ is one of the groups $C_6, S_3(6), G \leqslant S_6$, where $S_3(6)$ denotes the group S_3 in its degree 6 representation. Since C_6 is Abelian we get from [9] that

$$Z(\mathbb{Q}, C_6; x) \sim c(C_6) x^{1/3}. \tag{1}$$

From the Davenport–Heilbronn theorem [3] we know that

$$Z\big(\mathbb{Q}, S_3(3); x\big) \sim c\big(S_3(3)\big)x.$$

Using the fact that the discriminant of the splitting field of an S_3-extension is at least the square of the discriminant of the S_3-extension, we easily get that

$$Z\big(\mathbb{Q}, S_3(6); x\big) = \mathrm{O}(x^{1/2}).$$

Since extensions with Galois group $S_3(6)$ are normal we can use a result in [4, Proposition 2.8] which states that $Z(\mathbb{Q}, S_3(6); x) = \mathrm{O}_\epsilon(x^{3/8+\epsilon})$ for all $\epsilon > 0$. With a more careful analysis we are able to prove

$$Z\big(\mathbb{Q}, S_3(6); x\big) = \theta(x^{1/3}). \tag{2}$$

We remark that the results for $S_3(6)$ and C_6 are as conjectured since $a(C_6) = a(S_3(6)) = 1/3$ and $b(\mathbb{Q}, C_6) = b(\mathbb{Q}, S_3(6)) = 1$.

Now we define the counting function corresponding to field towers $L/K/\mathbb{Q}$ as above:

$$\widetilde{Z}(\mathbb{Q}, C_3 \wr C_2; x) := \#\big\{L/\mathbb{Q} \mid \exists K\colon \mathrm{Gal}(L/K) = C_3, [K:\mathbb{Q}] = 2, |d_L| \leqslant x\big\}.$$

We have two conjugacy classes of elements of order 3 in G which have three fixed points. Considered as $\mathbb{Q}$-conjugacy classes we have only one orbit. In number fields k containing a primitive third root of unity ζ_3 we have two k-conjugacy classes of this type. Therefore $a(G) = 1/2$ and $b(\mathbb{Q}, G) = 1$. Since, by (1) and (2), the counting functions for $S_3(6)$ and C_6 have lower asymptotics Conjecture 1.3 implies that

$$\widetilde{Z}(\mathbb{Q}, C_3 \wr C_2; x) \sim Z(\mathbb{Q}, C_3 \wr C_2; x) \sim c(G)x^{1/2}.$$

Certainly we get a lower estimate for $\widetilde{Z}(\mathbb{Q}, C_3 \wr C_2; x)$ if we only count the number fields which contain a fixed quadratic subfield K. We choose $K = \mathbb{Q}(\zeta_3)$ and using $d_L = d_K^3 \mathrm{N}(d_{L/K})$ we get for x large enough:

$$\widetilde{Z}(\mathbb{Q}, C_3 \wr C_2; x) \geqslant Z(K, C_3; x/27) \sim c(K, C_3)x^{1/2}\log(x).$$

For the latter we used the fact that $b(K, C_3) = 2$ and that the conjecture is true for the Abelian group C_3. This already gives a contradiction to Conjecture 1.3. □

Now we introduce a counting function avoiding $\mathbb{Q}(\zeta_3)$.

$$\hat{Z}(\mathbb{Q}, C_3 \wr C_2; x) := \#\big\{L/\mathbb{Q} \mid \exists K \neq \mathbb{Q}(\zeta_3)\colon \mathrm{Gal}(L/K) = C_3, [K:\mathbb{Q}] = 2, |d_L| \leqslant x\big\}.$$

Using the averaging results for the 3-ranks of the class group of quadratic fields [3] we can prove that

$$\hat{Z}(\mathbb{Q}, C_3 \wr C_2; x) \sim c(C_3 \wr C_2)x^{1/2} \quad \text{for some constant } c(C_3 \wr C_2) > 0$$

as predicted by Malle's conjecture. This means that the cyclotomic intermediate extension is the reason for the failure of the conjecture.

We remark that we can produce more counter examples in the same spirit in the following way. Define $G := C_\ell \wr H$ and assume that there exists an $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) = H$ and $K := L \cap \mathbb{Q}(\zeta_\ell) \neq \mathbb{Q}$. We remark that we have the identity $a(G) = a(C_\ell) = \ell - 1$. Now we are in the situation that $b(\mathbb{Q}, G) = b(\mathbb{Q}, C_\ell) = 1$ and $b(K, G) = b(K, C_\ell) = (\ell - 1)/[K:\mathbb{Q}] > 1$. Analogously as in the proof of Theorem 2.1 there exists $c(G) > 0$ such that

$$Z(\mathbb{Q}, G; x) > c(G)x^{a(G)}\log(x)^{b(K,G)-1} \quad \text{for } x \text{ large enough.}$$

The following example shows that this happens infinitely often.

Example 1. Let $G = C_\ell \wr C_2$ for an odd prime ℓ. Then $L = K := \mathbb{Q}(\sqrt{\pm\ell}) \subseteq \mathbb{Q}(\zeta_\ell)$ has the wanted property.

We remark that for $\ell > 3$ we are only able to prove $Z(\mathbb{Q}, C_\ell \wr C_2; x) = \mathrm{O}(x^{3/(2\ell)})$ since we do not know good estimates for the ℓ-rank of the class group of quadratic fields in these cases.

3. Comments about the conjecture

It is interesting to look at the global function field case. Malle's conjecture can be easily generalized to this setting and these generalizations are true for Abelian groups [9]. In the function field setting it is natural to consider only extensions $K/\mathbb{F}_q(t)$ such that the normal closure contains no constant field extension. Assuming this and some (unproven) heuristic about the number of points of irreducible varieties over $\mathbb{F}_q$, Ellenberg and Venkatesh [5] are able to deduce

$$Z\big(\mathbb{F}_q(t), G; x\big) = \theta\big(x^{a(G)}\log(x)^{b(\mathbb{F}_q(t),G)-1}\big) \quad \text{for } \gcd(\#G, q) = 1.$$

If we allow constant field extensions we can give the type of counter examples as in the number field case. E.g. choosing $q \equiv 2 \bmod 3$ and $G = C_3 \wr C_2$ works as a counter example, when we choose $\mathbb{F}_{q^2}/\mathbb{F}_q$ as the quadratic extension.

Constant field extensions are always contained in extensions generated by suitable roots of unity. We could fix the conjecture in the number field case if we forbid intermediate extensions which are contained in cyclotomic extensions $\mathbb{Q}(\zeta_\ell)$, where ℓ must be chosen from a set containing all orders of elements of G which have minimal index. But this is not very natural in the number field case.

The problem in the presented counter examples is that there exist intermediate extensions K such that $b(\mathbb{Q}, G) < b(K, G)$. The following example shows that this is not sufficient to produce counter examples. E.g. for the group $G = (C_3 \wr C_3) \times C_2$ we get $a(G) = 1/4, b(\mathbb{Q}, G) = 1, b(\mathbb{Q}(\zeta_3), G) = 2$. We can prove that

$$Z(\mathbb{Q}, G; x) = \theta(x^{1/4}).$$

Therefore this group does not contradict Conjecture 1.3. Similar to our original example it is possible to choose $K = \mathbb{Q}(\zeta_3)$ as an intermediate extension, but this time it does not change the log-factor.

Since we do not know if there are other type of groups which contradict Conjecture 1.3 we do not give a new formulation of this conjecture.

Acknowledgements

I thank Karim Belabas and Gunter Malle for fruitful discussions and reading a preliminary version of the paper.

References

[1] K. Belabas, Paramétrisation de structures algébriques et densité de discriminants [d'après Bhargava], Séminaire Bourbaki, 56ème année (935), 2004.
[2] H. Cohen, F. Diaz y Diaz, M. Olivier, A survey of discriminant counting, in: Algorithmic Number Theory (Sydney, 2002), in: Lecture Notes in Computer Science, vol. 2369, Springer, Berlin, 2002, pp. 80–94.
[3] H. Davenport, H.A. Heilbronn, On the density of discriminants of cubic fields. II, Proc. Roy. Soc. London Ser. A 322 (1551) (1971) 405–420.
[4] J. Ellenberg, A. Venkatesh, The number of extensions of a number field with fixed degree and bounded discriminant, math.NT/0309153, 2003.
[5] J. Ellenberg, A. Venkatesh, Counting extensions of function fields with bounded discriminant and specified Galois group, in: Geometric Methods in Algebra and Number Theory, in: Progr. Math., vol. 235, Birkhäuser, 2005, pp. 151–168.
[6] J. Klüners, G. Malle, Counting nilpotent Galois extensions, J. Reine Angew. Math. 572 (2004) 1–26.
[7] G. Malle, On the distribution of Galois groups, J. Numer. Theory 92 (2002) 315–322.
[8] G. Malle, On the distribution of Galois groups II, Exp. Math. 13 (2004) 129–135.
[9] D. Wright, Distribution of discriminants of Abelian extensions, Proc. London Math. Soc. 58 (1989) 17–50.