ALBANIAN JOURNAL
OF MATHEMATICS
Volume 3, Number 3, Pages 95–105
ISSN 1930-1235: (2009)

FIELDS GENERATED BY ROOTS OF $x^n + ax + b$

Mohamed Ayad
Laboratoire de Mathématiques Pures et Appliquées
Université du Littoral
F-62228 Calais, France
ayad@lmpa.univ-littoral.fr

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

1. Introduction

Let $n \geq 2$ be a fixed integer. Let a and b be integers and put $f_{a,b}(X) = X^n + aX + b$. Let $\theta_{a,b}^{(1)}, \ldots, \theta_{a,b}^{(n)}$ be all the roots of $f_{a,b}(X)$. In this paper, we investigate the properties of the fields $\mathbb{Q}(\theta_{a,b}^{(i)})$ for $i = 1, \ldots, n$, as the pair (a, b) ranges in $(\mathbb{Z} \cap [-T, T])^2$, where T is some positive real number. Given the pair (a, b), there are at most n distinct fields among $\mathbb{Q}(\theta_{a,b}^{(i)})$ for $i = 1, \ldots, n$. Clearly, there are $(2T + O(1))^2 = 4T^2 + O(T)$ pairs of positive integers (a, b) both in $[-T, T]$. The first question we ask is for how many of such pairs is one of the fields $\mathbb{Q}(\theta_{a,b}^{(i)})$ for some $i = 1, \ldots, n$ (hence, for all such i) of degree n over $\mathbb{Q}$, or, equivalently, for how many such pairs (a, b) is $f_{a,b}(X) \in \mathbb{Q}[X]$ irreducible? Note that by choosing pairs (a, b) such that $p \| b$ and $a \equiv 0 \pmod{p}$ for some prime p, the polynomials $f_{a,b}(X)$ are irreducible by Eisenstein's criterion. However, this gives us only a positive proportion of pairs (a, b) of integers in $[-T, T]$. In fact, as $T \to \infty$, $(6/\pi^2 + o(1))(2T)^2$ of the pairs (a, b) have the property that a and b are coprime, therefore the above argument will not work for them. Our first result shows that $f_{a,b}(X) \in \mathbb{Q}[X]$ is irreducible for almost all pairs $(a, b) \in (\mathbb{Z} \cap [-T, T])^2$.

Theorem 1. *Assume that $n \geq 2$. The set of pairs $(a, b) \in (\mathbb{Z} \cap [-T, T])^2$ such that $f_{a,b} \in \mathbb{Q}[X]$ is not irreducible is of cardinality $O(T^{3/2})$ as $T \to \infty$.*

The proof of Theorem 1 is given in Section 2. We observe that in Theorem 2.1 in reference [2], S. D. Cohen gives, for arbitrary irreducible polynomials $f(Y_1, \ldots, Y_t, X) \in \mathbb{Z}[Y_1, \ldots, Y_t, X]$, an upper bound for the number of integer tuples $(m_1, \ldots, m_t) \in (\mathbb{Z} \cap [-T, T])^t$ such that $f(m_1, \ldots, m_t, X)$ is irreducible in $\mathbb{Z}[X]$. In the special case considered by us, this gives an upper bound of $O(T^{3/2} \log T)$ on the number of pairs $(a, b) \in (\mathbb{Z} \cap [-T, T])^2$ for which $f_{a,b}(X)$ is not irreducible in

$\mathbb{Z}[X]$, which is slightly worse than the conclusion of our Theorem 1. Furthermore, the proof of our Theorem 1 is elementary.

The next natural question we ask is when does the same field arise from two different pairs (a, b)? That is, when can it happen that there exist two pairs $(a, b) \neq (a_1, b_1)$ and two roots $\theta_{a,b}$ of $f_{a,b}(X)$ and θ_{a_1,b_1} of $f_{a_1,b_1}(X)$, respectively, such that $\mathbb{Q}(\theta_{a_1,b_1}) = \mathbb{Q}(\theta_{a,b})$? Clearly, if

$$(a_1, b_1) = (\lambda^{n-1}a, \lambda^n b)$$

holds for some rational number λ, then $\theta_{a_1,b_1} = \lambda\theta_{a,b}$, therefore certainly $\mathbb{Q}(\theta_{a_1,b_1}) = \mathbb{Q}(\theta_{a,b})$. Are there any other instances when this phenomenon happens? We cannot answer this question. However, here is a small contribution towards this problem. Let

$$\mathcal{D} = \{(a, b) \in \mathbb{Z}^2 : a \neq 0,\ \mu(b) \neq 0\},$$

where $\mu(m)$ is the Möbius function of m which is zero if m is divisible by a square of a prime and is $(-1)^k$ if m is a product of k distinct primes.

Theorem 2. *Assume that $n \geq 5$. For each number field $\mathbb{K}$, there are at most finitely many pairs $(a, b) \in \mathcal{D}$ such that $\mathbb{K} = \mathbb{Q}(\theta_{a,b})$ for some root $\theta_{a,b}$ of $f_{a,b}(X)$.*

The proof of Theorem 2 is given in Section 3. Let

$$m(\mathbb{K}) = \#\{(a, b) \in \mathcal{D} : \mathbb{K} = \mathbb{Q}(\theta_{a,b}) \text{ for some root } \theta_{a,b} \text{ of } f_{a,b}(X)\}.$$

Theorem 2 implies that $m(\mathbb{K}) < \infty$ holds for all algebraic number fields $\mathbb{K}$. We conjecture that a stronger statement holds, namely the following:

Conjecture 1. *Assume that $n \geq 5$. There exists a constant c_n depending only on n such that $m(\mathbb{K}) < c_n$ holds for all algebraic number fields $\mathbb{K}$.*

We make a remark about this conjecture at the end of Section 3.

We may ask how important is the condition $n \geq 5$ in the statement of Theorem 2? Section 4 is dedicated to comments regarding this condition. In that section, we show that the conclusion of Theorem 2 is false for $n = 2$ and $n = 3$, and present evidence that it is perhaps false for $n = 4$ as well.

For any real number T, let

$$F(T) = \#\{\mathbb{Q}(\theta_{a,b}^{(i)}),\ i = 1, \ldots, n : a, b \in \mathbb{Z},\ \max\{|a|, |b|\} \leq T\}. \tag{1}$$

Hence, $F(T)$ counts the number of distinct fields of the form $\mathbb{Q}(\theta_{a,b})$, where $\theta_{a,b}$ can be any root of $f_{a,b}(X)$, as a and b vary through integers of absolute value at most T.

We would like to suggest the following conjecture:

Conjecture 2. *There exists a positive constant c_n depending on n such that*

$$F(T) > c_n T^2$$

holds for all sufficiently large real numbers T.

Note that Conjecture 1 implies Conjecture 2, but perhaps Conjecture 2 is easier to prove than Conjecture 1. Note also that $F(T) \ll T^2$ trivially. Thus, Conjecture 2 above suggests that the true order of magnitude of $F(T)$ is T^2.

We have not succeeded in proving Conjecture 2. We have however the following result whose proof is given in Section 5.

Theorem 3. *Assume that $n \geq 4$. There exists a positive constant c_n depending on n such that*

$$F(T) \geq T \exp\left(c_n \frac{\log T}{\log\log T}\right)$$

holds as $T \to \infty$.

One can ask whether it is true that for every algebraic number field $\mathbb{K}$ there exists a pair of integers (a, b) such that $\mathbb{K} = \mathbb{Q}(\theta_{a,b})$ for some root $\theta_{a,b}$ of $f_{a,b}(X)$. The answer to this is yes for $n = 2,\ 3$ and no for $n \geq 4$. To see this, let us note that $\mathbb{Q}(\theta_{a,b})$ does not have too many real conjugates. That is, it is easy to see that $f_{a,b}(X)$ can have at most three real roots. Indeed, for if not, then by Rolle's theorem $f'_{a,b}(x) = nX^n + a$ will have at least three real roots, and this is clearly impossible. Thus, if $n \geq 4$ and $\mathbb{K}$ is a totally real number field of degree ≥ 4, then $\mathbb{K} \neq \mathbb{Q}(\theta_{a,b})$ for any pair of integers (a, b) and any root $\theta_{a,b}$ of $f_{a,b}(X)$.

We conclude this section by pointing out that the Galois group of the polynomial $f_{a,b}(X)$ has been extensively studied. For example, Theorem 1.1 of [3] shows, in particular, that if $\gcd(a, n) = \gcd(a(n-1), b) = 1$, and $f_{a,b}(X)$ is irreducible, then the Galois group of $\mathbb{Q}(\theta_{a,b})$, for any root $\theta_{a,b}$ of $f_{a,b}(X)$, contains A_n. Under these restrictions, and assuming further than $n \geq 5$, then, by the proof of Theorem 2 and the remark at the end of it, there are only finitely many pairs of integers (a, b) such that the discriminant of $f_{a,b}(X)$ is a square (see also [8] and [10] for conditional and unconditional results concerning the square-free values of discriminants of $f_{a,b}(X)$ as a and b range over the integers in certain intervals). Thus, except for such finitely many pairs, the Galois group of $\mathbb{Q}(\theta_{a,b})$ over $\mathbb{Q}$ is S_n. However, note that the conditions $\gcd(n, a) = \gcd(a(n-1), b) = 1$ are fulfilled for a set of positive asymptotic density of pairs of integers (a, b) in $[-T, T]$ as $T \to \infty$. Since by Theorem 1, $f_{a,b}(X)$ is also irreducible for almost all pairs of integers (a, b) in $[-T, T]$ as $T \to \infty$, we deduce, by Theorem 2.1 in [2], the following result.

Theorem 4. *The Galois group of $f_{a,b}(X)$ over the rationals is S_n for all pairs of integers $(a, b) \in [-T, T]$ except for a set of such pairs of cardinality $O(T^{3/2} \log T)$ as $T \to \infty$.*

2. Proof of Theorem 1

Since there are only $O(T)$ pairs $(a, 0)$ with $|a| \leq T$, we may assume that $b \neq 0$. Let (a, b) be a pair for which $f_{a,b}(X)$ is not irreducible and write $f_{a,b}(X) = g(X)h(X)$, where

$$g(X) = X^k + p_0X^{k-1} + \cdots + p_{k-1} \qquad \text{and} \qquad h(X) = X^\ell + q_0X^{\ell-1} + \cdots + q_{\ell-1},$$

and k and ℓ positive integers. If $k = 1$, then $-p_0$ is a root of $f_{a,b}(X)$. Hence, $p_0 \mid b$, therefore p_0 can be chosen in at most $2\tau(|b|)$ ways, where $\tau(m)$ is the number of divisors of m, and once p_0 is fixed then

$$a = -\frac{p_0^n + b}{p_0}$$

is also fixed. Since

$$\sum_{0<|b|\leq T} \tau(|b|) = O(T \log T),$$

it follows that there are $O(T \log T)$ pairs (a, b) for which $k = 1$. Similar arguments apply to the case when $\ell = 1$. This takes care, in particular, of the cases when $n = 2$ and $n = 3$.

Assume now that $n \geq 4$ and that both $k \geq 2$ and $\ell \geq 2$. Identifying coefficients, we get

$$p_0 + q_0 = 0, \quad \cdots, \quad p_{k-2}q_{\ell-1} + p_{k-1}q_{\ell-2} = a, \quad p_{k-1}q_{\ell-1} = b.$$

This is a polynomial system of n equations in the $n = k + \ell$ integer unknowns

$$(p_0, \ldots, p_{k-1}, q_0, \ldots, q_{\ell-1}),$$

where we treat a and b as coefficients. By variable elimination, p_{k-1} satisfies a polynomial equation $P_{k,\ell}(p_{k-1}, a, b) = 0$, whose coefficients are polynomials in $\mathbb{Z}[a, b]$. To detect this relation, note that if we write $\theta_1, \ldots, \theta_n$ for all the roots of $f_{a,b}(X)$, then, by the Viète relations,

$$p_{k-1} = (-1)^k \prod_{i \in I} \theta_i$$

for some subset I of $\{1, \ldots, n\}$ of cardinality k. The polynomial

$$P_{k,\ell}(X) = \prod_{\substack{J \subset \{1,\ldots,n\} \\ \#J = k}} \left(X + (-1)^{k+1} \prod_{j \in J} \theta_j \right)$$

is symmetric in the roots $\theta_1, \ldots, \theta_n$ and admits p_{k-1} as a root. By the Fundamental Theorem of Symmetric Polynomials, $P_{k,\ell}(X)$ is a polynomial whose coefficients are in $\mathbb{Z}[a, b]$. The last coefficient (free term) of $P_{k,\ell}(X)$ is

$$(-1)^{(k+1)\binom{n}{k}} \left(\prod_{j=1}^{n} \theta_j \right)^{\binom{n-1}{k-1}} = \delta b^{\binom{n-1}{k-1}}, \qquad \text{where } \delta = (-1)^{(k+1)\binom{n}{k} + n\binom{n-1}{k-1}},$$

again by the Viète relations, because there are $\binom{n}{k}$ subsets J of $\{1, \ldots, n\}$ of cardinality k and each fixed $j \in \{1, \ldots, n\}$ belongs to precisely $\binom{n-1}{k-1}$ such subsets J. Since $p_{k-1}q_{\ell-1} = b$, it follows that for a fixed b, p_{k-1} can be chosen in at most $\tau(|b|) = b^{o(1)}$ ways as $T \to \infty$. When both b and p_{k-1} are fixed, then $P_{k,\ell}(p_{k-1}, a, b) = 0$ is a polynomial relation for a of degree at most $\binom{n}{k}$, so if $P_{k,\ell}(p_{k-1}, A, b) \in \mathbb{Z}[A]$ is not the zero polynomial, then a can take at most $\binom{n}{k}$ values. Thus, in this case we get at most $T^{1+o(1)}$ possibilities for the pair (a, b) as $T \to \infty$. Assume now that $P_{k,\ell}(p_{k-1}, A, b) = 0$. In particular, its free (constant) term is zero. But the constant term is achieved by taking $a = 0$ in the definition of $f_{a,b}(X) = X^n + b$, getting that $\theta_j = e^{j\pi i/n} b^{1/n}$ for $j = 1, \ldots, n$, where $b^{1/n}$ is a fixed determination of the nth root of b. Thus,

$$P_{k,\ell}(X, 0, b) = \prod_{\substack{J \subset \{1,\ldots,n\} \\ \#J = k}} \left(X + \varepsilon_J b^{k/n} \right),$$

where $\varepsilon_J = e^{(k+1+\sum_{j \in J} j)\pi i/n}$ is some root of unity. Thus, if (p_{k-1}, b) are such that $P_{k,\ell}(p_{k-1}, 0, b) = 0$, then $p_{k-1} = -\varepsilon_J b^{k/n}$ holds for some subset J of $\{1, \ldots, n\}$ with k elements. Since $p_{k-1} \in \mathbb{Z}$, we get that $p_{k-1} = \pm |b|^{k/n}$. Since $1 \leq k < n$, we get that $|b|$ must be a power of exponent > 1 of some other integer. The number of such values for b in $[-T, T]$ is $O(T^{1/2})$. Since a can take at most $2T + 1$ values, it follows that the pair (a, b) can be chosen in at most $O(T^{3/2})$ ways, which completes the proof of this theorem.

3. Proof of Theorem 2

Assume that $\mathbb{K} = \mathbb{Q}(\theta_{a,b})$ for some pair $(a, b) \in \mathcal{D}$ and some root $\theta_{a,b}$ of $f_{a,b}(X)$. We fix the pair (a, b). Let (a_1, b_1) be some other pair in $\mathcal{D}$ such that $\mathbb{Q}(\theta_{a_1,b_1}) = \mathbb{K}$ for some root θ_{a_1,b_1} of $f_{a_1,b_1}(X)$. Assume that p is a prime dividing both a_1 and b_1. Then, in $\mathbb{K}$, we have

$$\theta(\theta^{n-1} + a_1) = -b_1, \tag{2}$$

where $\theta = \theta_{a_1,b_1}$ is in $\mathcal{O}_{\mathbb{K}}$. Assume further that p does not ramify in $\mathbb{K}$. Then

$$p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{j} \pi_i$$

for some distinct prime ideals π_i of $\mathbb{K}$. Since b_1 is square-free, we get that π_1 appears with power 1 in the factorization of b_1 in $\mathcal{O}_{\mathbb{K}}$. But $\pi_1 \mid p \mid \gcd(a_1, b_1)$, therefore $\pi_1 \mid a_1$. Equation (2) shows that $\pi_1 \mid \theta^n$, therefore $\pi_1 \mid \theta$. Thus, π_1^2 divides $\theta(\theta^{n-1} + a_1)$, contradicting that fact that π_1 appears with power 1 in b_1. This argument shows that if $p \mid \gcd(a_1, b_1)$, then $p \in \mathcal{P}_{\mathbb{K}}$, where $\mathcal{P}_{\mathbb{K}}$ is the finite set of primes dividing the discriminant of $\mathbb{K}$.

It is well-known that the discriminant $\Delta_{a,b}$ of $f_{a,b}(X)$ is

$$\Delta_{a,b} = b^{n-1}n^n + (-1)^{n-1}a^n(n-1)^{n-1} \tag{3}$$

(see, for example, [7]). Put $\Delta_{\mathbb{K}}$ for the discriminant of $\mathbb{K}$. Then Δ_{a_1,b_1} is the volume of the lattice $\mathbb{Z}[\theta_{a_1,b_1}]$ inside $\mathcal{O}_{\mathbb{K}}$, so $\Delta_{a_1,b_1} = \Delta_{\mathbb{K}}x^2$ holds, where x is the index of $\mathbb{Z}[\theta_{a_1,b_1}]$ in $\mathcal{O}_{\mathbb{K}}$. Hence, the above discriminant calculation shows that

$$b_1^{n-1}n^n + (-1)^{n-1}a_1^n(n-1)^{n-1} = \Delta_{\mathbb{K}}x^2.$$

Let $D_1 = \gcd(n^n b_1^{n-1}, a_1^n(n-1)^{n-1})$. If $p \mid D_1$, then either $p \le n$ or the divisibility relation $p \mid \gcd(a_1, b_1)$ holds. Thus, either $p \le n$ or $p \in \mathcal{P}_{\mathbb{K}}$ by the arguments from the beginning of this proof. Since b_1 is square-free, we get that

$$D_1 \mid n^n \left(\prod_{p \in \mathcal{P}_{\mathbb{K}}} p \right)^{n-1},$$

so D_1 can take only finitely many values. Fix a value for D_1. For this fixed value of D_1, we must have $b_1 = b_1'X$, where X is a positive integer coprime to D_1, and b_1' is a square-free integer all of whose prime factors are among the prime factors of D_1. Clearly, b_1' can be fixed in only finitely many ways as well. Assume that b_1' is also fixed. Then a_1 is such that $a_1 = a_1'Y$, where Y is an integer and a_1' is the smallest positive integer such that $(n-1)^{n-1}a_1'^n$ is a multiple of D_1. Finally, $x = x_1Z$, where Z is an integer and x_1 is the smallest positive integer such that $\Delta_{\mathbb{K}}x_1^2$ is a multiple of D_1. We thus get the equation

$$n^n(b_1')^nX^n + (-1)^{n-1}(n-1)^{n-1}(a_1')^nY^{n-1} = (\Delta x_1^2)Z^2,$$

or, after simplifying by D_1,

$$A_1X^n + B_1Y^{n-1} = C_1Z^2, \tag{4}$$

where

$$A_1 = n^n (b_1')^n / D_1, \quad B_1 = (-1)^{n-1}(n-1)^{n-1}(a_1')^n / D_1, \quad C_1 = \Delta_{\mathbb{K}} x_1^2 / D_1.$$

Furthermore, notice that in the above equation (4), we have the relation

$$\gcd(A_1X^n, B_1Y^n, C_1Z^2) = 1.$$

Since the sum of the reciprocals of the three exponents $1/n + 1/(n-1) + 1/2 < 1$ for $n \geq 5$, a result of Darmon and Granville [4] shows that the Diophantine equation (4) has at most finitely many solutions (X_1, Y_1, Z_1). Since D_1 can be chosen in only finitely many ways, the theorem is proved.

Remark. Let $\mathcal{D}_1$ be the subset of $\mathcal{D}$ such that $\gcd(a, n) = \gcd(a(n-1), b) = 1$. Fix $(a, b) \in \mathcal{D}_1$ and let Δ be the discriminant of $\mathbb{Q}(\theta_{a,b})$. If $(a_1, b_1) \in \mathcal{D}_1$ is such that $\mathbb{Q}(\theta_{a_1,b_1}) = \mathbb{Q}(\theta_{a,b})$, then

$$nX^{n-1} - (n-1)^{n-1}Y^n = \Delta Z^2 \tag{5}$$

holds with $X = nb_1$ and $Y = -a_1$ and $\gcd(nX, (n-1)Y) = 1$. Darmon and Granville's proof [4] of the finiteness of integer solutions of the above equation proceeds by showing that every integer solution of the above equation produces a rational point on a curve of genus $2n(n-1)(1-1/2-1/n-1/(n-1)) = n^2-5n+2 \geq 2$ defined over an algebraic number field $\mathbb{L}$ of degree and discriminant bounded in terms of n and Δ, and this association is injective. The conclusion follows by appealing to Falting's theorem concerning the finiteness of rational points on a curve of genus $g > 1$. It has been suggested by Lang (see [1]) that there should be a bound on the number of rational points on a curve of genus $g > 1$ which depends only on the genus g, but not on the curve itself. This is usually referred to as the *Rigidity Conjecture*. It thus makes sense to conjecture that the number of solutions (X, Y, Z) of the Diophantine equation (5) with $\gcd(nX, (n-1)Y) = 1$ is bounded by a number depending only on n (hence, not on Δ). This may be interpreted as (weak) evidence in favor of Conjecture 2. Even assuming the rigidity conjecture, the proof of Darmon of Granville does not seem to immediately lead to the above conclusion since it also uses Minkowski's convex body theorem to bound the candidates for $\mathbb{L}$, which are number of fields of degree bounded in terms of n only and unramified at the places not dividing $n(n-1)\Delta$, and this last number does depend on Δ. Perhaps a closer analysis of the arguments from [4] will show that the number of such fields can be bounded by some power of $\tau(\Delta)$. If true, then since $\omega(\Delta) \ll \log\log T$ holds for almost all pairs of integers $(a, b) \in [-T, T]$ as $T \to \infty$, it would follow, under the rigidity conjecture, that $m(\mathbb{K}_{a,b}) \ll (\log T)^{c_n}$ holds for almost all pairs $(a, b) \in [-T, T]$ as $T \to \infty$, where c_n is some constant depending on n. In turn, this will imply that $F(T) \gg T^2/(\log T)^{c_n}$ which is still short by the logarithmic factor from the lower bound conjectured by Conjecture 2, but it is much better than the unconditional lower bound of Theorem 3 of $F(T)$.

4. Theorem 2 and small values of n

In this section, we show that the conclusion of Theorem 2 is false when $n = 2$ and $n = 3$, and present evidence that it is perhaps also false when $n = 4$.

If $n = 2$, then we may assume that $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, where $d \neq 0, 1$ is a square-free positive integer. We prove that there are infinitely many quadratic polynomials $f(x) = x^2 + ax + b$ with $a \neq 0$ and b square-free whose roots generate $\mathbb{K}$. Clearly, this is equivalent to the fact that $a^2 - 4b = d\lambda^2$ for some integer λ. Taking $a = 2a_0,\ \lambda = 2$, it suffices to show that the number $b = a_0^2 - d$ is square-free for infinitely many positive integers a_0. However, it is well-known and easy to prove that the polynomial $X^2 - d$ represents infinitely many square-free positive integers. In fact, this is true for all quadratic polynomials $f(X)$ such that for each prime p there is an integer n with $p^2 \nmid f(n)$.

Assume now that $n = 3$ and fix $a \neq 0$ and b square-free. We let α, β, γ be some integers to be determined later and compute the resultant with respect to X of the polynomial $X^3 + aX + b$ and $\alpha X^2 + \beta X + \gamma - T$. We obtain the polynomial

$$\begin{aligned} R(T) &= -T^3 + (-2a\alpha + 3\gamma)T^2 + (-a^2\alpha^2 - 3\alpha b\beta - a\beta^2 + 4a\alpha\gamma - 3\gamma^2)T \\ &+ (\alpha^3 b^2 - a\alpha^2 b\beta - b\beta^3 + a^2\alpha^2\gamma + 3\alpha b\beta\gamma + a\beta^2\gamma - 2a\alpha\gamma^2 + \gamma^3). \end{aligned}$$

Imposing that the coefficient of T is zero, we get $\gamma = 2a\alpha/3$. Replacing this value of γ in the remaining coefficients of $R(T)$ we get

$$\begin{aligned} R_1(T) &= -T^3 + \left(\frac{a^2\alpha^2}{3} - 3\alpha b\beta - a\beta^2\right)T \\ &+ \frac{2a^3\alpha^3}{27} + \alpha^3 b^2 + a\alpha^2 b\beta^2 + \frac{2a^2\alpha\beta^2}{3} - b\beta^3. \end{aligned}$$

Choosing $a = 3,\ b = 1$ (note that $f_{3,1}(X) = X^3 + 3X + 1$ is irreducible in $\mathbb{Q}[X]$), we get

$$R_1(T) = -T^3 + 3(\alpha^2 - \alpha\beta - \beta^2)T + (3\alpha^3 + 3\alpha^2\beta + 6\alpha\beta^2 - \beta^3).$$

Thus, if we choose $a_1 = 3(\alpha^2 - \alpha\beta - \beta^2)$ and $b_1 = 3\alpha^3 + 3\alpha^2\beta + 6\alpha\beta^2 - \beta^3$, then $\mathbb{Q}(\theta_{a_1,b_1}) = \mathbb{Q}(\theta_{3,1})$, for some appropriately chosen roots θ_{a_1,b_1} and $\theta_{3,1}$ of $f_{a_1,b_1}(X)$ and $f_{3,1}(X)$, respectively. It is clear that $a_1 \neq 0$ unless both α and β are zero. Thus, it suffices, in order for (a_1, b_1) to belong to $\mathcal{D}$, that b_1 is square-free. However, it is well-known that there are infinitely many square-free integers of the form $3X^3 + 3X^2Y + 6XY^2 - Y^3$ (see, for example, [6]).

Finally, let $n = 4$. We let again $(a, b) \in \mathcal{D}$, $\alpha, \beta, \gamma, \delta$ be integers and we take

$$\begin{aligned} S(T) &= \mathrm{Res}_X(X^4 + aX + b, \alpha X^3 + \beta X^2 + \gamma X + \delta - T) \\ &= T^4 + (3a\alpha - 4\delta)T^3 + (3a^2\alpha^2 + 2b\beta^2 + 4\alpha b\gamma + 3a\beta\gamma - 9a\alpha\delta + 6\delta^2)T^2 \\ &+ CT + D, \end{aligned}$$

where C and D are some polynomials in $a, b, \alpha, \beta, \gamma, \delta$ which we no longer explicitly write down. Imposing that the coefficients of T^3 and T^2 in $S(T)$ are zero, we get

$$\delta = \frac{3a\alpha}{4} \qquad \text{and} \qquad \gamma = \frac{3a^2\alpha^2 - 16b\beta^2}{8(4\alpha b + 3a\beta)}.$$

We now choose $\beta = (3 - 4\alpha b)/(3a)$. Putting now $a = 1$ and $b = 6$ (note that $f_{1,6}(X) = X^4 + X + 6$ is irreducible in $\mathbb{Q}[X]$), and $\alpha = 4(17 + 36\alpha_0)$ for some integer α_0, we get that

$$S(T) = T^4 + A(\alpha_0)T + B(\alpha_0),$$

where A and B are polynomials with integer coefficients in the variable α_0. We have that $A(Z)$ is nonzero and

$$B(Z) = 6\,(193103517037550444 7963157 + 32774253999060620818245978Z$$
$$+24336241399338483321730 4976Z^2 + 10326095711996981147285886 72Z^3$$

$$\begin{gathered}+273841210426959744663886041 6Z^4 + 464773587975021032502552576 0Z^5\\ +493019494999761626492372582 4Z^6 + 298846859930915510332470067 2Z^7\\ +7925220594853008008816885 76Z^8\big)\,.\end{gathered}$$

Since $B(Z)$ is an irreducible polynomial of degree 8 and

$$B(1)/6 = 23159 \cdot 83381630052053389523$$

is a product of two primes each exceeding 8, Schinzel's Hypothesis H implies that $B(Z)/6$ should be prime for infinitely many Z. Indeed, the only condition to be verified is that for each prime p, there exists m such that $p \nmid B(m)/6$. For $p \le 11$ this is true by taking $m = 1$, and for $p > 11$ this is true because the equation $B(m)/6 \equiv 0 \pmod{p}$ is a polynomial equation of degree ≤ 8, so it can have at most 8 solutions modulo p, therefore there exist at least $p - 8 > 0$ congruence classes m modulo p such that $B(m)/6$ is not zero modulo p. In particular, certainly $B(\alpha_0)$ should be square-free for infinitely many choices of the integer α_0, showing that there should be infinitely many pairs $(a_1, b_1) \in \mathcal{D}$ (namely, all these of the form $(A(\alpha_0), B(\alpha_0))$ with the second component square-free) such that $\mathbb{Q}(\theta_{a,b}) = \mathbb{Q}(\theta_{1,6})$. All this is conditional upon Schinzel's Hypothesis H. We would like to suggest the following problem for the reader.

Problem 1. *Find a pair $(a, b) \in \mathcal{D}$ and an unconditional proof of the fact that $\mathbb{Q}(\theta_{a,b}) = \mathbb{Q}(\theta_{a_1,b_1})$ for infinitely many pairs $(a_1, b_1) \in \mathcal{D}$ when $n = 4$.*

5. Proof of Theorem 3

Let $\mathcal{P}_T$ be a fixed finite set of prime numbers, which will depend on T. We write $s = s(T)$ for the cardinality of $\mathcal{P}_T$. We choose (a, b) such that $2 \mid a$, $b \equiv 2 \pmod{4}$, $|a| \le T$, $|b| \le T$, $\gcd(a, b) = 2$, and all prime factors of b are in $\mathcal{P}_T$. Note that $f_{a,b}(X)$ is irreducible for such pairs (a, b) because it is Eisenstein with respect to the prime 2.

We also assume that $|a| > nT^{(n-1)/n}$. We let $\mathbb{K}$ be some fixed field and count how many pairs (a, b) can give rise to $\mathbb{K}$. Letting (a, b) be such a pair, then

$$\theta(\theta^{n-1} + a) = -b.$$

Let $\mathbb{L}$ be the normal closure of $\mathbb{K}$. Passing to ideals in $\mathbb{L}$, we get that $\theta\mathcal{O}_{\mathbb{L}}$ is a divisor of b. Let $\mathcal{Q}_{\mathbb{L}}$ be the set of all prime ideals in $\mathbb{L}$ dividing some prime number $p \in \mathcal{P}_T$. Since every prime in $\mathcal{P}_T$ has at most $[\mathbb{L} : \mathbb{Q}] \le n!$ prime ideal divisors in $\mathcal{Q}_{\mathbb{L}}$, it follows that $t = \#\mathcal{Q}_{\mathbb{K}} \le n!s$. Let these ideals be $\pi_1, \ldots, \pi_t$. Let $\zeta_1, \ldots, \zeta_m$ be generators for the free part of the group of units of $\mathbb{L}$. Note that $m \le n! - 1$. Let h be the class number of $\mathbb{L}$. Then π_i^h is principal. For each $i = 1, \ldots, t$, let η_i be a generator of π_i^h. Then the equation

$$\theta(\theta^{n-1} + a) = -b,$$

gives

$$\theta\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{t} \pi_i^{\alpha_i} \qquad \text{and} \qquad (\theta^{n-1} + a)\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{t} \pi_i^{\beta_i},$$

for some nonnegative integers α_i and β_i, $i = 1, \ldots, t$. Raising these relations to the power h, we get

$$\theta^h\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{t} (\pi_i^h)^{\alpha_i} = \prod_{i=1}^{t} \eta_i^{\alpha_i}\mathcal{O}_{\mathbb{L}},$$

and similarly

$$(\theta^{n-1}+a)^h \mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{t} \eta_i^{\beta_i} \mathcal{O}_{\mathbb{L}}.$$

Passing to elements, we get

$$\theta^h = \nu \prod_{i=1}^{t} \eta_i^{\alpha_i} \prod_{j=1}^{m} \zeta_j^{\gamma_j} \tag{6}$$

and

$$(\theta^{n-1}+a)^h = \mu \prod_{i=1}^{t} \eta_i^{\beta_i} \prod_{j=1}^{m} \zeta_j^{\delta_j}, \tag{7}$$

where γ_j and δ_j are integers for $j = 1, \ldots, m$ and ν and μ are roots of unity in $\mathbb{L}$ (their order does not exceed the largest positive integer N such that $\phi(N) \le n!$). Let η_i' and ζ_j' be fixed determinations of the hth roots of η_i and ζ_j, respectively, where $i = 1, \ldots, t$ and $j = 1, \ldots, m$. Let also λ be a generator of the group of torsion units in $\mathbb{L}$ and λ' be a fixed determination of its hth root. Extracting h'th roots in equations (6) and (7), we get

$$\theta = \lambda'^k \prod_{i=1}^{t} \eta_i'^{\alpha_i} \prod_{i=1}^{m} \zeta_j'^{\gamma_j} \qquad \text{and} \qquad \theta^{n-1}+a = \lambda'^\ell \prod_{i=1}^{t} \eta_i'^{\beta_i} \prod_{i=1}^{m} \zeta_j'^{\delta_j}.$$

Let G be the multiplicative group inside the field of complex numbers generated by the numbers $\{\lambda', \eta_i', \zeta_j' : i = 1, \ldots, t,\ j = 1, \ldots, m\}$. Note that it is easy to see that G may be assumed to be invariant under the conjugations from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then the above equation shows that

$$a = s_1 - s_2,$$

where $s_1 = \theta^{n-1}$ and $s_2 = \theta^{n-1} + a$ are elements in G. Conjugating (or replacing θ by one of its conjugates θ'), we get $a = s_3 - s_4$, where $s_3 = (\theta')^{n-1}$ and $s_4 = (\theta')^{n-1} + a$ are also in G. Hence, we have obtained the $\mathcal{S}$-unit equation

$$s_1 - s_2 - s_3 + s_4 = 0. \tag{8}$$

Recall that an $\mathcal{S}$-unit equation is *degenerate* if some sub-sum of it is zero. In this case, being degenerate means that one of $s_1 - s_2$, $s_1 - s_3$ and $s_1 + s_4$ is zero. Observe that:

(i) If $s_1 - s_2 = 0$, then $a = 0$, which is not allowed.

(ii) If $s_1 - s_3 = 0$, then $\theta^{n-1} = (\theta')^{n-1}$. Since $\theta(\theta^{n-1}+a) = -b = \theta'((\theta')^{n-1}+a)$, it follows that $\theta = \theta'$. This is impossible because $f_{a,b}(X)$ is irreducible in $\mathbb{Q}[X]$.

(iii) If $s_1 + s_4 = 0$, then $\theta^{n-1} - (\theta')^{n-1} - a = 0$. Hence, $\theta^{n-1} = \theta'^{n-1} + a = -b/\theta'$. We now get easily that $|\theta|^{n-1}|\theta'| = |b|$. If this is true for all conjugates of θ' of θ, we get that all the roots of $f_{a,b}(X)$ have the same absolute value $|b|^{1/n}$. Thus, by the Viète relations, $|a| \le n|b|^{(n-1)/n} \le nT^{(n-1)/n}$, which is false by our initial assumption on a. Hence, there must be two conjugates θ and θ' having different absolute values, and for these we have $s_1 + s_4 \ne 0$.

The above argument shows that for each of the pairs (a, b) under consideration, there exists an $\mathcal{S}$-unit equation of the form (8) which is nondegenerate. By results of Evertse, Schmidt and Schlickewei [5], the set of ratios s_1/s_2 is of cardinality

$$\le \exp(24^{12}(m+t+1)) \le \exp(24^{12}n!(s+1)).$$

Now let $u = s_1/s_2$ be fixed. Then $-\theta^n/b = u = 1 + a/\theta^{n-1}$. We get $\theta = (-bu)^{1/n}$, so $a = -(1-u)\theta^{n-1} = -(1-u)(-u)^{(n-1)/n}b^{(n-1)/n}$. Thus, $|a|/|b|^{(n-1)/n}$ is uniquely determined in terms of u. Assume that (a, b) and (a_1, b_1) are such that $|a|/|b|^{(n-1)/n} = |a_1|/|b_1|^{(n-1)/n}$. Raising this equality to nth power, we get $|a|^n/|b|^{n-1} = |a_1|^n/|b_1|^{n-1}$. Since $2\|b$ and $\gcd(a, b) = 2$, we get $a = \pm a_1$ and $b = \pm b_1$. Thus, each solution of the nondegenerate equation (8) determines a and b uniquely up to signs.

All we have to do is count. We choose y such that

$$s = \pi(y) \le \frac{c \log T}{\log\log T},$$

where $c < 1$ is some constant to be determined later. Then

$$\prod_{p \le y} p = \exp((1 + o(1))y)$$

holds as $T \to \infty$. Thus, if we let $\varepsilon > 0$ be fixed and we put

$$K = \left\lfloor (1-\varepsilon)\frac{\log T}{y} \right\rfloor,$$

then any number $b = \prod_{p \le y} p^{\alpha_p}$ with $2\|b$ and $\alpha_p \le K$ for all $p \le y$ works. Let $\mathcal{B}$ be the set of such numbers. Then

$$\#\mathcal{B} \gg (K+1)^{\pi(y)-1} = \exp\left((1+o(1))s \log\left(\frac{\log T}{y}\right) + O(s\varepsilon)\right)$$

holds as $T \to \infty$. Let a be an integer such that $2\|a$, a is free of odd primes $p \le y$, and $|a| > T^{1-1/2n}$. Let $\mathcal{A}$ be the set of such acceptable a's. Then the inequality

$$\#\mathcal{A} \ge (1 + o(1)) \prod_{p \le y} \left(1 - \frac{1}{p}\right)^{-1} T + O(T^{1-1/2n}) \ge (e^{-\gamma} + o(1))\frac{T}{\log y}$$

holds as $T \to \infty$. Let $m(\mathbb{K})$ be the multiplicity of $\mathbb{K}$ when (a, b) range in $\mathcal{A} \times \mathcal{B}$. Note that all conditions from beginning of this proof are fulfilled by these pairs (a, b) when T is large. The above argument shows that the number of different fields created in this way is at least

$$\frac{\#\mathcal{A} \times \#\mathcal{B}}{\max\{m(\mathbb{Q}(\theta_{a,b})) : (a,b) \in \mathcal{A} \times \mathcal{B}\}} \ge T \exp\left((s + o(s)) \log\left(\frac{\log T}{c_1 y}\right) + O(s\varepsilon)\right)$$

as $T \to \infty$, where $c_1 = 24^{12}n!$. We now put $c_2 = (c_1 e)^{-1}$, choose $y = c_2 \log T$ for which $s = (c_2 + o(1)) \log T/\log\log T$ as $T \to \infty$, and get that the number of distinct fields we have created is

$$\ge T \exp\left((c_2 + o(1) + O(\varepsilon))\frac{\log T}{\log\log T}\right)$$

as $T \to \infty$. Making now also ε tend to zero, we get the desired result.

Acknowledgements. We thank the referee for suggestions which improved the quality of this paper. This paper was written during a very enjoyable visit by the second author to the LMPA of the Université du Littoral Côte d'Opale of Calais; he wishes to express his thanks to that institution for the hospitality and support. During the preparation of this paper, F. L. was also partly supported by grant SEP-CONACyT 79685 and PAPIIT 100508.

References

[1] C. Caporaso, J. Harris and B. Mazur, 'Uniformity of rational points', *J. American Math. Soc.* **10** (1997), 1–35.

[2] S. D. Cohen, 'The distribution of Galois groups and Hilbert's irreducibility theorem', *Proc. London Math. Soc. (3)* **43** (1981), 227–250.

[3] S. D. Cohen, A. Movahhedi and A. Salinier, 'Galois groups of trinomials', *J. Algebra* **222** (1999), 561–573.

[4] H. Darmon and A. Granville, 'On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$', *Bull. London Math. Soc.* **27** (1995), 513–543.

[5] J.-H. Evertse, H. P Schlickewei and W. M. Schmidt, 'Linear equations in variables which lie in a multiplicative group', *Ann. of Math. (2)* **155** (2002), 807–836.

[6] F. Gouvêa and B. Mazur,'The square-free sieve and the rank of elliptic curves', *J. Amer. Math. Soc.* **4** (1991), no. 1, 1–23.

[7] P. Lefton, 'On the Galois groups of cubics and trinomials', *Bull. Amer. Math. Soc.* **82** (1976), 754–756.

[8] A. Mukhopadhyay, M. R. Murty and K. Srinivas, 'Counting squarefree discriminants of trinomials under *abc*', *Proc. Amer. Math. Soc.* **137**, 3219–3226.

[9] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, third. ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997.

[10] I. Shparlinski, 'On Quadratic Fields Generated by Discriminants of Irreducible Trinomials', *Preprint*, 2009, http://arxiv.org/abs/0811.1300.