Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Journal of Number Theory 105 (2004) 387–400

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

Trinomial extensions of $\mathbb{Q}$ with ramification conditions ☆

Bernat Plans[a] and Núria Vila[b,*]

[a] *Dept. de Matemàtica Aplicada I, Universitat Politècnica de Catalunya, Av. Diagonal, 647, 08028 Barcelona, Spain*

[b] *Dept. d'Àlgebra i Geometria, Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, 08007 Barcelona, Spain*

Received 28 June 2003

Communicated by D. Goss

Abstract

This paper concerns trinomial extensions of $\mathbb{Q}$ with prescribed ramification behavior. We first characterize the positive integers n such that, for every finite set S of prime numbers, there exists a degree n monic trinomial in $\mathbb{Z}[X]$ whose Galois group over $\mathbb{Q}$ is contained in the alternating group A_n and such that its discriminant is not divisible by any prime p in S. We also characterize the positive integers n such that, for a given finite set of primes S, there exist trinomial extensions with Galois group over $\mathbb{Q}$ contained in A_n which are not ramified at the primes of S. In addition, we study the existence of trinomial extensions of $\mathbb{Q}$ with Galois group A_n which are tamely ramified. In particular, we show that such extensions do exist for every odd n. On the other hand, we obtain that, for $n \equiv 4 \pmod 8$, every A_n-extension of $\mathbb{Q}$ defined by a degree n trinomial must be wildly ramified at $p = 2$.

Keywords: Trinomials; Ramification; Galois groups; Alternating groups

1. Introduction

The present paper concerns Galois extensions of $\mathbb{Q}$, obtained as splitting fields of rational trinomials, with prescribed ramification behavior at finitely many primes. The Galois groups of irreducible trinomials with integer coefficients have been

---

☆ Research partially supported by MCYT Grant BFM2000-0794-C02-01.

*Corresponding author.

E-mail address: vila@mat.ub.es (N. Vila).

0022-314X/$ - see front matter
doi:10.1016/j.jnt.2003.11.001

widely studied, see for example, [3,4]. The determination of the discriminant of number fields defined by trinomials has been considered in [5].

For a positive integer n and an arbitrary given finite set S of prime numbers, we consider the existence of degree n separable monic trinomials $f(X) \in \mathbb{Z}[X]$ satisfying additional properties such as the following ones:

(a) the discriminant of $f(X)$ is not divisible by any prime $p \in S$,
(b) every prime $p \in S$ is unramified in the splitting field of $f(X)$ over $\mathbb{Q}$,
(c) every prime $p \in S$ is tamely ramified in the splitting field of $f(X)$ over $\mathbb{Q}$.

When there is no restriction on the Galois group of $f(X)$ over $\mathbb{Q}$, such trinomials do exist for every n and every S. As a consequence, one can also require $f(X)$ to have Galois group over $\mathbb{Q}$ isomorphic to the symmetric group S_n. However, this is no longer true if we only admit trinomials with square discriminant in $\mathbb{Z}$, that is, with Galois group contained in the alternating group A_n.

Our main results characterize pairs of coprime positive integers $k < n$ for which there exists a trinomial $X^n + aX^k + b \in \mathbb{Z}[X]$ whose Galois group over $\mathbb{Q}$ is contained in A_n and such that property (a) (resp. (b), resp. (c)) holds for a given finite set S. Furthermore, this turns out to be equivalent to requiring that the above Galois group is precisely A_n. In addition, only primes which divide n or $k(n-k)$ appear in the conditions we obtain.

We also consider the question of which positive integers n meet, for every finite set S, the criteria given by these characterizations (for some suitable k depending on S).

As a particular case of our results we show that, for every odd n, there exist trinomial extensions of $\mathbb{Q}$ with Galois group A_n which are tamely ramified. On the other hand, for infinitely many n we obtain that trinomials do not suffice to realize A_n as the Galois group of some tame extension of $\mathbb{Q}$. For instance, we show that every A_n-extension of $\mathbb{Q}$ defined by a degree $n \equiv 4 \pmod 8$ trinomial must be wildly ramified at $p = 2$. This provides examples of $\mathbb{Q}$-regular A_n-extensions of $\mathbb{Q}(T)$ which do not admit tamely ramified rational specializations.

We thank Carl Pomerance for his suggestion that a sieve argument should suffice to prove Proposition 17. We also thank Alain Salinier for pointing out to us that, as in Proposition 8, there is also an exceptional case for $p = 3$ in Proposition 7, and for providing us with the example of Remark 9.

2. Trinomials with discriminant coprime with the primes of S

It is well known that, if $k < n$ are coprime positive integers, the discriminant of a trinomial $f(X) = X^n + aX^k + b$ is

$$D(f) = (-1)^{\frac{n(n-1)}{2}} b^{k-1}(n^n b^{n-k} + (-1)^{n-1}(n-k)^{n-k}k^k a^n).$$

Let S be a given finite set of prime numbers. It is clear that we can choose the coefficients $a, b \in \mathbb{Z}$ such that the discriminant $D(f)$ is not divisible by any prime of S.

In this case, the primes of S are not ramified in the Galois extension $\mathbb{Q}_f/\mathbb{Q}$, where $\mathbb{Q}_f$ denotes the splitting field of the trinomial $f(X)$ over $\mathbb{Q}$.

Proposition 1. *Let S be a finite set of prime numbers. For every positive integer n, there exists a trinomial $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ with Galois group over $\mathbb{Q}$ isomorphic to the symmetric group S_n and with discriminant $D(f)$ not divisible by any prime in S.*

Proof. Let T_1, T_2 be indeterminates. For every n, the Galois group of the trinomial $X^n + T_1X + T_2$ over $\mathbb{Q}(T_1, T_2)$ is

$$\mathrm{Gal}_{\mathbb{Q}(T_1,T_2)}(X^n + T_1X + T_2) \cong S_n.$$

By Hilbert's irreducibility theorem, the set of pairs $(t_1, t_2) \in \mathbb{Q}^2$ for which the specialized trinomial $X^n + t_1X + t_2$ has S_n as Galois group over $\mathbb{Q}$ is I-adically dense in $\mathbb{Q}^2$, for every ideal $I \subset \mathbb{Z}$. Thus, given two rational numbers $a_0, b_0 \in \mathbb{Q}$, there must exist a trinomial $f(X) = X^n + aX + b \in \mathbb{Q}[X]$ with Galois group over $\mathbb{Q}$ isomorphic to S_n and such that, for every $p \in S$, we have

$$f(X) \equiv X^n + a_0X + b_0 \pmod{p}.$$

So, taking, for example, $a_0 = 1$ and

$$b_0 \equiv \begin{cases} 0 \pmod{p} & \text{if } p \nmid n-1, \\ 1 \pmod{p} & \text{if } p \mid n-1, \end{cases}$$

we have that p does not divide the discriminant of $f(X)$, for all primes $p \in S$. Moreover, we can assume that $f(X)$ has integer coefficients, replacing $f(X)$ by $M^n f(X/M)$, with $M \in \mathbb{Z}$ appropriate.

Let $(\frac{u}{v})$ denote the Jacobi symbol of integers $u, v \in \mathbb{Z}$, with v odd.

Proposition 2. *Let $k < n$ be coprime positive integers. For a prime number p, the following properties are equivalent:*

(i) *There exists a trinomial $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ with square discriminant in $\mathbb{Z}$ not divisible by p.*

(ii) *If n is even and p is odd, then $v_p(n) = 0$ or $(\frac{-1}{p})^{n/2} = 1$.*
If n is even and $p = 2$, then $(-1)^{n/2}(1 - kn) \equiv 1 \pmod{8}$.
If n is odd and p is odd, then $v_p(k(n-k)) = 0$ or $(\frac{p}{n}) = 1$.
If n is even and $p = 2$, then $(-1)^{\frac{n-1}{2}} n \equiv 1 \pmod{8}$ or $(-1)^{\frac{n-1}{2}} n \equiv 5 \pmod{8}$ and $k(n-k) = 2(n-2)$.

Proof. Using the quadratic reciprocity law and the formula for the discriminant of a trinomial, we can check that (i) implies the conditions of (ii).

Assume that (ii) is satisfied and that n is even. Let $r, s \in \mathbb{N}$ be such that

$$s(n-k) - rn = 1, \quad 0 < s < n \quad \text{and} \quad 0 \leqslant r < n-k.$$

Let us write $h = v_p(n)$ and $n = mp^h$. Taking $a = mt^r$ and $b = t^s$, the discriminant of the trinomial $f(X) = X^n + aX^k + b$ is

$$D(f) = t^{s(k-1)+rn} m^n ((-1)^{n/2}(k-n)^{n-k}k^k + (-1)^{n/2}p^{hn}t).$$

For the primes p dividing n, hypothesis (ii) implies that the equation

$$Y^2 - ((-1)^{n/2}(k-n)^{n-k}k^k) \equiv 0 \pmod{p^{hn}}$$

has integer solutions. Since p does not divide $(k-n)^{n-k}k^k$ $(n>2)$, there exists a $t \in \mathbb{Z}$ such that $D(f)$ is a square in $\mathbb{Z}$ which is not divisible by p. The result in the case where $p \nmid n$ is clear since then $h = 0$ and $p^{hn} = 1$.

Assume that (ii) is satisfied and that n is odd. Let $r, s \in \mathbb{N}$ such that

$$rn - s(n-k) = 1, \quad 0 < s < n \quad \text{and} \quad 0 < r \leqslant n-k.$$

Let $(n-k)^{n-k}k^k = mp^h$, where $h = v_p((n-k)^{n-k}k^k)$. Taking $a = mp^h t^r$ and $b = m^{n+1}t^s$, the discriminant of the trinomial $f(X) = X^n + aX^k + b$ is

$$D(f) = t^{s(n-1)} m^{(n+1)k} ((-1)^{\frac{n-1}{2}} n^n m^{(n+1)(n-k-1)} + (-1)^{\frac{n-1}{2}} p^{h(n+1)} t).$$

For every prime p dividing $k(n-k)$, hypothesis (ii) ensures that the equation

$$Y^2 - ((-1)^{\frac{n-1}{2}} n^n m^{(n+1)(n-k-1)}) \equiv 0 \pmod{p^n}$$

has integer solutions. Since p does not divide $n^n m^{(n+1)(n-k-1)}$ (and $n+1>2$), there exists an integer $t \in \mathbb{Z}$ such that $D(f)$ is a square not divisible by p. The same conclusion is clear if $p \nmid k(n-k)$.

Remark 3. It is known that trinomials of type $f(X) = X^n + aX^k + b$ can be classified by the parameter $\frac{b^{n-k}}{a^n}$. Namely, if $(n,k) = 1$, there exist positive integers s, r such that $s(n-k) - rn = 1$, $0 < s < n$, $0 \leqslant r < n-k$ and we have

$$\left(\frac{b^r}{a^s}\right)^n f\left(\frac{a^s}{b^r}X\right) = X^n + \left(\frac{b^{n-k}}{a^n}\right)^r X^k + \left(\frac{b^{n-k}}{a^n}\right)^s.$$

Clearly, the discriminant of the trinomial

$$X^n + T^r X^k + T^s \in \mathbb{Q}(T)[X],$$

as a polynomial in X is, modulo squares in $\mathbb{Q}(T)$, a polynomial of degree 1 in $\mathbb{Q}[T]$ or $\mathbb{Q}[1/T]$. As a consequence, there exists $a(T) \in \mathbb{Q}(T)$ such that the coefficients of any trinomial $X^n + aX^k + b \in \mathbb{Q}[X]$ whose discriminant is a square in $\mathbb{Q}$ can be obtained by

$$a = a(t)^r \mu^{n-k}, \quad b = a(t)^s \mu^n, \quad \text{where } t, \mu \in \mathbb{Q}.$$

In addition, the trinomial $X^n + a(T)^r X^k + a(T)^s \in \mathbb{Q}(T)[X]$ defines a $\mathbb{Q}$-regular Galois extension of $\mathbb{Q}(T)$ with Galois group isomorphic to A_n (cf., for example, [4]).

Proposition 4. *Let $k < n$ be coprime positive integers. For every finite set S of prime numbers, the following properties are equivalent*:

(i) *There exists a trinomial $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ with Galois group $\mathrm{Gal}_{\mathbb{Q}}(f(X)) \cong A_n$ and discriminant $D(f)$ not divisible by any prime in S.*
(ii) *For each prime $p \in S$, there exists a trinomial $X^n + a_p X^k + b_p \in \mathbb{Z}[X]$ whose discriminant is a square integer not divisible by p.*

Proof. Clearly, (i) ⇒(ii). Assume that condition (ii) holds. By the above remark, for each $p \in S$ there exist rational numbers $t_p, \mu_p \in \mathbb{Q}$ such that

$$a_p = a(t_p)^r \mu_p^{n-k} \quad \text{and} \quad b_p = a(t_p)^s \mu_p^n.$$

Assume that T_1, T_2 are indeterminates and consider the polynomial

$$f(T_1, T_2, X) = X^n + a(T_1)^r T_2^{n-k} X^k + a(T_1)^s T_2^n \in \mathbb{Q}(T_1, T_2)[X].$$

If $t_1, t_2 \in \mathbb{Q}$ are rational numbers such that, for every $p \in S$, t_1, t_2 are p-adically near enough to t_p, μ_p, then we have

$$f(t_1, t_2, X) \equiv X^n + a_p X^k + b_p \pmod{p}, \text{for all } p \in S.$$

Since we know that

$$\mathrm{Gal}_{\mathbb{Q}(T_1,T_2)}(f(T_1, T_2, X)) \cong A_n,$$

Hilbert's irreducibility theorem allows us to take $t_1, t_2 \in \mathbb{Q}$ as above and such that

$$\mathrm{Gal}_{\mathbb{Q}}(f(t_1, t_2, X)) \cong A_n.$$

Hence, we can choose an integer $M \equiv 1$ (mod $\prod_{p \in S} p$) such that the trinomial

$$f(X) = M^n f(t_1, t_2, X/M)$$

has integer coefficients and satisfies property (i).

Theorem 5. *For a positive integer n, the following properties are equivalent*:

(i) *For every finite set S of prime numbers, there exists a trinomial $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ with Galois group over $\mathbb{Q}$ isomorphic to A_n and discriminant not divisible by any prime in S.*

(ii) *For every finite set* S *of prime numbers, there exists a trinomial* $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ *with Galois group over* $\mathbb{Q}$ *contained in* A_n *and discriminant not divisible by any prime in* S.

(iii) n *satisfies one of the following conditions*:

$n \equiv 0,\ 1 \pmod 8$,

$n \equiv 2 \pmod 8$ *and every odd prime number* $p \mid n$ *is* $p \equiv 1 \pmod 4$,

$n \equiv 3 \pmod 8$ *and every prime number* $p \mid (n-2)$ *is* $p \equiv 1$ *or* $3 \pmod 8$.

Proof. Assume that $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ satisfies the hypothesis of (ii), for the set S of primes less than or equal to n. Then, $(n,k) = 1$. If n is even, by Proposition 2, we have

(a) $(\frac{-1}{p})^{\frac{n}{2}} = 1$, for every odd prime p dividing n,

(b) $(-1)^{\frac{n}{2}}(1 - nk) \equiv 1 \pmod 8$.

Condition (a) is only possible if $n \equiv 0, 4 \pmod 8$ or $n \equiv 2, 6 \pmod 8$ and $p \equiv 1 \pmod 4$. For $n \equiv 6 \pmod 8$, necessarily there is a prime $p \mid n$ with $p \equiv 3 \pmod 4$. If $n \equiv 4 \pmod 8$, condition (b) is not satisfied. In conclusion, the only possibilities for n even are those considered in (iii). In an analogous way, we obtain that only the possibilities of (iii) can appear, also in the odd n case.

Now assume that n is a positive integer as in (iii). Let us take $k = n - 2$, if $n \equiv 3 \pmod 8$, and $k = n - 1$, otherwise. Then, for each prime number p, the conditions in Proposition 2 (ii) hold. From Proposition 4, we obtain property (i).

Remark 6. In fact, if S is a given finite set of prime numbers and n is a positive integer satisfying condition (iii) in Theorem 5, then there exist infinitely many monic trinomials in $\mathbb{Z}[X]$, with discriminant not divisible by any prime in S, and such that their splitting fields define linearly disjoint A_n-extensions of $\mathbb{Q}$.

3. Trinomial A_n-extensions of $\mathbb{Q}$ unramified at S

The following propositions establish that, under certain hypotheses on the p-adic valuations of the coefficients a, b of a rational trinomial $f(X) = X^n + aX^k + b$, the prime p must divide, not only the discriminant of $f(X)$, but also the discriminant of the extension $\mathbb{Q}_f/\mathbb{Q}$. In some cases, these hypotheses are precisely the conditions that one obtains when requiring the discriminant $D(f)$ to be a square in $\mathbb{Q}$. In order to know the ramification behavior in $\mathbb{Q}_f/\mathbb{Q}$ of the primes dividing $D(f)$, we use basic results in Newton polygon theory (cf., for example, [6, II.Section 6.]).

Proposition 7. *Let* $k<n$ *be coprime positive integers and let* $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ *be a separable trinomial such that* $b \neq 0$.

(a) *Let* p *be an odd prime number such that* $v_p(a^n) \geqslant v_p(n^n b^{n-k})$. *Assume we are not in the case* $n = p = 3$. *If* $v_p(n) > 0$ (*resp.* $v_p(n) > 1$), *then* p *is ramified* (*resp. wildly ramified*) *in the extension* $\mathbb{Q}_f/\mathbb{Q}$.

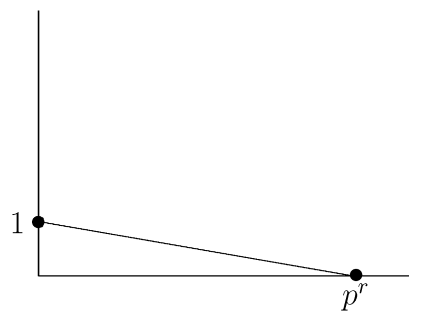
(b) *If* $v_2(n)>1$ *and* $v_2(a^n)\geqslant v_2(n^n b^{n-k})-2$, *then* $p=2$ *is wildly ramified in the extension* $\mathbb{Q}_f/\mathbb{Q}$.

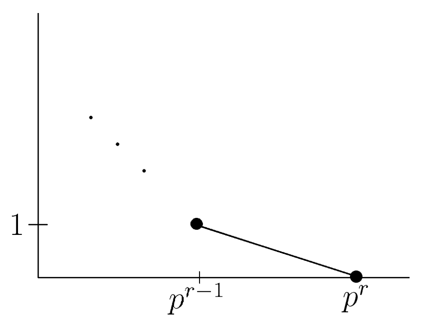
Proof. Let p be a prime divisor of n which satisfies the above hypothesis (we allow $p=2$). Since $v_p(a^n)\geqslant v_p(b^{n-k})$, we can assume $v_p(b)<n$. Let us write $d=(n,v_p(b))$, $v_p(b)=dh$, $n=de$, $r=v_p(n)$, $n=n'p^r$ and $b=b'p^{dh}$. In case $v_p(e)>0$, the Newton polygon of $f(X)$ has a segment of slope $-\frac{h}{e}$ and the extension $\mathbb{Q}_f/\mathbb{Q}$ is wildly ramified at p.

From now on, we assume that $v_p(e)=0$. Let $\theta,\eta\in\overline{\mathbb{Q}_p}$ be roots of X^e-p and $X^{n'}+b'$, respectively. Note that the extension $\mathbb{Q}_p(\eta)/\mathbb{Q}_p$ (resp. $\mathbb{Q}_p(\theta)/\mathbb{Q}_p$) is unramified (resp. tamely ramified). Let us consider the following polynomial in $\mathbb{Q}_p(\theta,\eta)[X]$:

$$g(X)=\frac{1}{\theta^{hn}}f(\theta^h(X+\eta))=(X+\eta)^n+\frac{a}{\theta^{h(n-k)}}(X+\eta)^k+b'=\sum_{0\leqslant i\leqslant n}c_iX^i.$$

If $r=v_p(n)>1$, then it must be $v_p(\frac{a}{\theta^{h(n-k)}})\geqslant r$. This forces the Newton polygon of $g(X)$ to be of one of the following types:





In both cases, p must be wildly ramified in $(\mathbb{Q}_p)_g/\mathbb{Q}_p$ and, hence, also in $\mathbb{Q}_f/\mathbb{Q}$.

We now consider the case $r=v_p(n)=1$ and $p\neq 2$. If $v_p(b)>0$, then clearly the extension $\mathbb{Q}_f/\mathbb{Q}$ is ramified at p. Assume that $v_p(b)=0$. So, $\theta^h=1$. If $p\neq n$, then we can choose η such that $v_p(c_1)=1$. Otherwise, $p\neq 3$ and, replacing, if necessary, $f(X)$

by $\frac{X^n}{b}f(\frac{b}{X})$ and k by $n-k$, one checks that we can assume $v_p\binom{k}{j}>0$ or $k<j$, for some $j<p-1$. It follows that $v_p(c_j)=1$. We conclude that the Newton polygon of $g(X)$ must have a segment of non-integer slope $-\frac{1}{p-j}>-1$. This ensures that p is ramified in $(\mathbb{Q}_p)_g/\mathbb{Q}_p$, hence, in $\mathbb{Q}_f/\mathbb{Q}$.

The same type of argument allows us to prove the following analogous result.

Proposition 8. *Let $k<n$ be coprime positive integers and let $f(X)=X^n+aX^k+b\in\mathbb{Z}[X]$ be a separable trinomial such that $b\neq 0$.*

(a) *Let p be an odd prime number such that $v_p(b^{n-k})\geqslant v_p(k^k(n-k)^{n-k}a^n)$. Assume we are not in the case $n=4$ and $p=3$. If $v_p(k(n-k))>0$ (resp. $v_p(k(n-k))>1$), then p is ramified (resp. wildly ramified) in the extension $\mathbb{Q}_f/\mathbb{Q}$.*
(b) *If $v_2(k(n-k))>1$ and $v_2(b^{n-k})\geqslant v_2(k^k(n-k)^{n-k}a^n)-2$, then $p=2$ is wildly ramified in the extension $\mathbb{Q}_f/\mathbb{Q}$.*

Remark 9. The above results fail in the "exceptional case". For example, one checks that $p=3$ does not ramify in $\mathbb{Q}_f/\mathbb{Q}$ if we take $f(X)=X^3-21X^2+49$ or $f(X)=X^4+5X^3-216$.

As the following result shows, statement (a) in the above two propositions does not hold for the prime $p=2$.

Proposition 10. *Let $k<n$ be coprime positive integers and let $f(X)=X^n+aX^k+b\in\mathbb{Z}[X]$ be a separable trinomial. Assume that we are in one of the following cases:*

(1) *n even, $v_2(n)=1$, $(-1)^{n/2}(1-kn)\not\equiv 1 \pmod 8$, $v_2(b+1)\geqslant 3$ and $v_2(a)\geqslant 3$.*
(2) *n odd, $v_2(k)=1$, $(-1)^{\frac{n-1}{2}}n\not\equiv 1 \pmod 8$, $v_2(a+1)\geqslant 2$ and $v_2(b)=\lambda(n-k)\geqslant 2$ for some $\lambda\in\mathbb{N}$.*

Then $p=2$ does not ramify in the splitting field of $f(X)$ over $\mathbb{Q}$.

Proof. Assume that we are in case (1), let $\eta\in\overline{\mathbb{Q}_2}$ be a root of $\psi(X)=X^{\frac{n}{2}}-1$ and consider the following polynomial in $\mathbb{Q}_2(\eta)[X]$:

$$h(X)=f(X+\eta)=(X+\eta)^n+a(X+\eta)^k+b=\sum_{0\leqslant i\leqslant n}c_iX^i.$$

It can be checked that $v_2(c_0)\geqslant 3$, $v_2(c_1)=1$ and $v_2(c_2)=0$. It follows that $h(X)$ has two roots in $\mathbb{Q}_2(\eta)$ (with different positive valuations), corresponding precisely to the two roots of $f(X)$ congruent to η modulo 2. Hence, we have an inclusion $(\mathbb{Q}_2)_f\subseteq(\mathbb{Q}_2)_\psi$ and the extension $(\mathbb{Q}_2)_f/\mathbb{Q}_2$ must be unramified.

If we are in case (2), let us first consider the factorization $f(X)=f_1(X).f_2(X)$ in $\mathbb{Z}_2[X]$ given by Hensel's Lemma, where $f_1(X)\equiv X^{n-k} \pmod 2$ and $f_2(X)\equiv$

$(X^{k'}-1)^2 \pmod 2$. The extension $(\mathbb{Q}_2)_{f_1}/\mathbb{Q}_2$ must be unramified. To see this, it suffices to note that the polynomial

$$g(X) = \frac{X^n}{b} f\left(\frac{2^\lambda b}{X}\right) \equiv X^n - X^k \pmod 2$$

has a factor $g_1(X) \equiv X^{n-k} - 1 \pmod 2$ in $\mathbb{Z}_2[X]$ such that $(\mathbb{Q}_2)_{f_1} = (\mathbb{Q}_2)_{g_1}$. In order to prove that also the extension $(\mathbb{Q}_2)_{f_2}/\mathbb{Q}_2$ is unramified, let $\eta \in \overline{\mathbb{Q}_2}$ be a root of $\psi(X) = X^{k'} - 1$ and consider the following polynomial in $\mathbb{Q}_2(\eta)[X]$

$$h(X) = f(X+\eta) = (X+\eta)^n + a(X+\eta)^{n-k} + b = \sum_{0 \leqslant i \leqslant n} c_i X^i.$$

From our hypothesis, it can be seen that $v_2(c_0) \geqslant 2$, $v_2(c_1) = 1$ and $v_2(c_2) = 0$. The polynomial $h(X)$ must have a degree 2 factor $h_2(X) = (X-\beta_1)(X-\beta_2)$ in $\mathbb{Q}_2(\eta)[X]$, obtained from the two roots of $f_2(X)$ which are congruent to η modulo 2. In case $v_2(c_0) > 2$, we have that $(\mathbb{Q}_2(\eta))_{h_2} = \mathbb{Q}_2(\eta)$. If $v_2(c_0) = 2$, then $\frac{2}{\beta_1}, \frac{2}{\beta_2}$ are precisely the two roots of valuation 0 of the following polynomial in $\mathbb{Q}_2(\eta)[X]$

$$\frac{X^n}{c_0} h\left(\frac{2}{X}\right) \equiv X^{n-2}\left(X^2 + \frac{2c_1}{c_0}X + \frac{4c_2}{c_0}\right) \pmod 2.$$

Since $X^2 + \frac{2c_1}{c_0}X + \frac{4c_2}{c_0}$ is a separable polynomial modulo 2, it follows that the extension $(\mathbb{Q}_2(\eta))_{h_2}/\mathbb{Q}_2(\eta)$ must be unramified. We conclude that the extension $((\mathbb{Q}_2)_\psi)_{f_2}/(\mathbb{Q}_2)_\psi$ is unramified, so this is also true for the extension $(\mathbb{Q}_2)_{f_2}/\mathbb{Q}_2$.

From the above, we obtain the main result of this section.

Theorem 11. *Let $k < n$ be coprime positive integers and let S be an arbitrary prefixed finite set of prime numbers. Then the following properties are equivalent*:

(i) *For every prime $p \in S$, there exists a trinomial $f(X) = X^n + a_p X^k + b_p \in \mathbb{Z}[X]$ whose discriminant is a non-zero square in $\mathbb{Z}$ and such that p does not ramify in the extension $\mathbb{Q}_f/\mathbb{Q}$.*

(ii) *Every prime $p \in S$ satisfies one of the following conditions*:

If n is even and p is odd, then $v_p(n) = 0$ or $(\frac{-1}{p})^{n/2} = 1$.

If n is even and $p = 2$, then $(-1)^{n/2}(1-kn) \equiv 1 \pmod 8$ or $v_2(n) = 1$.

If n is odd and p is odd, then $v_p(k(n-k)) = 0$ or $(\frac{p}{n}) = 1$.

If n is odd and $p = 2$, then $(-1)^{\frac{n-1}{2}} n \equiv 1 \pmod 8$ or $v_2(k(n-k)) = 1$.

Proof. Let p be a prime number and let $f(X) = X^n + a_p X^k + b_p \in \mathbb{Z}[X]$ be a separable trinomial. If p does not ramify in the extension $\mathbb{Q}_f/\mathbb{Q}$, then the possible p-adic valuations of the coefficients a_p, b_p are restricted by Propositions 7 and 8. It can be checked that, when one also requires $f(X)$ to have square discriminant in $\mathbb{Z}$, these restrictions force p to satisfy condition (ii).

In Proposition 2, we already obtained that condition (i) follows from condition (ii), in some cases. Only the following ones are new:

- even n, $p = 2$, $v_2(n) = 1$ and $(-1)^{n/2}(1 - kn) \not\equiv 1 \pmod 8$.
- odd n, $p = 2$, $v_2(k(n-k)) = 1$ and $(-1)^{\frac{n-1}{2}} n \not\equiv 1 \pmod 8$.

Both can be easily obtained from Proposition 10. For example, for even n, we can consider natural numbers r, s such that $s(n-k) - rn = 1$ and take $a_2 = nAt^r$, $b_2 = t^s$, for well-chosen $A, t \in \mathbb{Z}$.

Remark 12. Property (ii) above characterizes the existence of trinomials $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ with A_n as Galois group over $\mathbb{Q}$ and such that all primes in S are unramified in $\mathbb{Q}_f/\mathbb{Q}$. This follows from Hilbert's irreducibility theorem and Krasner's Lemma, arguing as in the proof of Proposition 4.

As a consequence of Theorem 11, we obtain:

Corollary 13. *Let n be a positive integer. The following properties are equivalent*:

(i) *For every finite set S of prime numbers, there exists a trinomial $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ with A_n as Galois group over $\mathbb{Q}$ and such that all primes in S are unramified in the extension $\mathbb{Q}_f/\mathbb{Q}$.*

(ii) *For every finite set S of prime numbers, there exists a trinomial $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ with discriminant a non-zero square in $\mathbb{Z}$ and such that all primes in S are unramified in the extension $\mathbb{Q}_f/\mathbb{Q}$.*

(iii) *n satisfies one of the following conditions*:
$n \equiv 0, 1 \pmod 8$,
$n \equiv 2 \pmod 8$ *and* $p \equiv 1 \pmod 4$, *for every odd prime number* $p|n$,
$n \equiv 3 \pmod 8$ *and there exists a natural number* $k < n$ *such that* $(k, n) = 1$, $v_2(k(n-k)) = 1$ *and* $\left(\frac{p}{n}\right) = 1$, *for every odd prime number* $p|k(n-k)$.

4. Tamely ramified trinomial A_n-extensions of $\mathbb{Q}$

Proposition 14. *Let $k < n$ be coprime positive integers and let S be an arbitrary prefixed finite set of prime numbers. Then the following conditions are equivalent*:

(i) *There exists a separable trinomial $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ whose discriminant is a square in $\mathbb{Z}$ and such that all primes in S are tamely ramified in the extension $\mathbb{Q}_f/\mathbb{Q}$.*

(ii) *Every prime $p \in S$ satisfies one of the following conditions*:

If n is even and p is odd, then $v_p(n) \leqslant 1$ *or* $(\frac{-1}{p})^{n/2} = 1$.
If n is even and $p = 2$, *then* $(-1)^{n/2}(1 - kn) \equiv 1 \pmod 8$ *or* $v_2(n) = 1$.
If n is odd and p is odd, then $v_p(k(n-k)) \leqslant 1$ *or* $(\frac{p}{n}) = 1$.
If n is odd and $p = 2$, *then* $(-1)^{\frac{n-1}{2}} n \equiv 1 \pmod 8$ *or* $v_2(k(n-k)) = 1$.

Proof. We can proceed as in the proof of Theorem 11, taking into account Propositions 7, 8 and 10. The only additional point that must be proved is that condition (i) also holds in the following (new) cases:

(a) even n, odd p, $v_p(n) = 1$ and $(\frac{-1}{p})^{n/2} = -1$,
(b) odd n, odd p, $v_p(k(n-k)) = 1$ and $(\frac{p}{n}) = -1$.

Let us prove the even n case. The odd n case works analogously.

One easily checks (as in Proposition 11) that there exists a trinomial $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ with non-zero square discriminant in $\mathbb{Z}$ such that

$$v_p(b+1) \geqslant 2 \text{ and } v_p(a) \geqslant 2.$$

We want to show that these conditions suffice to ensure that p is tamely ramified in the extension $\mathbb{Q}_f/\mathbb{Q}$. Let us consider the following polynomial in $\mathbb{Q}_p(\eta)[X]$:

$$h(X) = f(X+\eta) = (X+\eta)^n + a(X+\eta)^k + b = \sum_{0 \leqslant i \leqslant n} c_i X^i,$$

where $\eta \in \overline{\mathbb{Q}_p}$ is a root of $\psi(X) = X^{\frac{n}{p}} - 1$. By inspection of the Newton polygon of $h(X)$, one immediately concludes that the extensions $((\mathbb{Q}_p)_\psi)_f/(\mathbb{Q}_p)_\psi$ and $(\mathbb{Q}_p)_f/\mathbb{Q}_p$ are tamely ramified.

The above result allows us to characterize the existence of tame A_n-extensions of $\mathbb{Q}$ obtained as splitting fields of degree n trinomials.

Theorem 15. *For a positive integer n, the following properties are equivalent*:

(i) *There exists a trinomial* $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ *such that the extension* $\mathbb{Q}_f/\mathbb{Q}$ *is tamely ramified and has Galois group isomorphic to* A_n.
(ii) *If n is even, then there exists a natural number* $k < n$ *such that* $(k,n) = 1$ *and* $v_p(n) = 1$, *for every prime* $p \mid n$ *such that* $(\frac{p}{k(n-k)}) = -1$.
If n is odd, then there exists a natural number $k < n$ *such that* $(k,n) = 1$ *and* $v_p(k(n-k)) = 1$, *for every prime* $p \mid k(n-k)$ *such that* $(\frac{p}{n}) = -1$.

Now we exhibit infinitely many natural numbers n such that property (ii) (and (i)) above holds.

Proposition 16. *Let n be a positive integer which satisfies one of the following conditions*:
$n \equiv 0 \pmod 8$,

n is square-free and even,
n is odd.

Then, there exists a degree n trinomial $f(X) = X^n + aX^k + b \in \mathbb{Z}[X]$ *such that the extension* $\mathbb{Q}_f/\mathbb{Q}$ *is tamely ramified and has* A_n *as Galois group.*

Only the case n odd requires a proof, which follows immediately from the next result.

Proposition 17. *Every positive integer* $n>1$ *can be represented as the sum of two square-free coprime positive integers.*

Proof. For each prime number q, let $r_q(n)$ denote the number of positive integers $a \leqslant n-1$ such that $(a,n)=1$ and $v_q(a)>1$. The property we must prove clearly follows from the inequality

$$\sum_{q\nmid n} r_q(n) < \frac{\phi(n)}{2},$$

where ϕ stands for Euler's function.

Let $p_1, \dots, p_s$ be the prime factors of n. If q does not divide n, then we have

$$\begin{aligned} r_q(n) &= \left[\frac{n}{q^2}\right] - \sum_{1\leqslant i\leqslant s}\left[\frac{n}{q^2 p_i}\right] + \sum_{1\leqslant i<j\leqslant s}\left[\frac{n}{q^2 p_i p_j}\right] - \cdots \\ &< \frac{n}{q^2}\prod_{1\leqslant i\leqslant s}\left(1-\frac{1}{p_i}\right) + 2^{s-1} = \frac{\phi(n)}{q^2} + 2^{s-1}. \end{aligned}$$

Hence, we obtain

$$\sum_{q\nmid n} r_q(n) < \phi(n)\left(\sum_{q\nmid n}\frac{1}{q^2}\right) + 2^{s-1}\pi(\sqrt{n}),$$

where $\pi(x)$ denotes the number of rational primes $\leqslant x$. Thus, it suffices to prove the following inequality:

$$\frac{2^{s-1}\pi(\sqrt{n})}{\phi(n)} < \frac{1}{2} - \sum_{q\nmid n}\frac{1}{q^2}.$$

It is well known that, for every $m \geqslant 2$, we have (cf. [1, Theorem 4.6]):

$$\pi(m) < \frac{6m}{\ln(m)}.$$

In addition, from equality $\zeta(2) = \frac{\pi^2}{6}$, one immediately obtains

$$\sum_{q}\frac{1}{q^2} < 0,4523.$$

Thus, the stated property holds for every n such that

$$\alpha(n) < 0,0477 + \sum_{1 \leqslant i \leqslant s} \frac{1}{(p_i)^2}, \qquad (*)$$

where we define the function $\alpha(n)$ as being

$$\alpha(n) = \frac{2^s n}{\phi(n)} \frac{6}{\sqrt{n}\ln(n)}.$$

If $q_1, \ldots, q_s$ are the smallest s prime numbers, then we have that $\alpha(n) \leqslant \alpha(q_1 . \cdots . q_s)$. One then easily checks that inequality $(*)$ holds provided $s \geqslant 10$.

On the other hand, if n has at most 9 different prime divisors, then

$$\alpha(n) \leqslant 2^9 . \frac{2.3.5.7.11.13.17.19.23}{\phi(2.3.5.7.11.13.17.19.23)} . \frac{6}{\sqrt{n}\ln(n)}.$$

It follows that n satisfies inequality $(*)$, for every $n \geqslant 10^9$. Indeed, it can be checked that the same conclusion holds for every $n \geqslant 15 \times 10^4$. For, it suffices to argue as above, also taking into account which of the primes $2, 3, 5$ divide n.

Finally, the stated result can be directly checked in the finitely many remaining cases $1 < n < 15 \times 10^4$.

There are also infinitely many n for which neither property (ii) (nor property (i)) in Theorem 15 holds: for example, every $n \equiv 4 \pmod 8$. Moreover, we have:

Proposition 18. *Let $\mathbb{Q}_f$ be the splitting field over $\mathbb{Q}$ of a separable trinomial $f(X) = X^n + aX^k + b \in \mathbb{Q}[X]$ of degree $n \equiv 4 \pmod 8$, where $k < n$ is assumed to be an odd positive integer. If $Gal_{\mathbb{Q}}(f(X)) \subseteq A_n$, then the extension $\mathbb{Q}_f/\mathbb{Q}$ is wildly ramified at $p = 2$.*

Proof. It suffices to note that, if we put $d = (n, k)$, $n = n'd$ and $k' = kd$, then the trinomial $g(X) = X^{n'} + aX^{k'} + b$ also has degree $n' \equiv 4 \pmod 8$ and, clearly, $\mathbb{Q}_g \subseteq \mathbb{Q}_f$.

Remark 19. Using the same type of argument as above, one checks that Proposition 18 remains valid if we replace $f(X) = X^n + aX^k + b$ by $f(X) = X^k(X - a)^{n-k} + b$. As in the case with trinomials, the polynomials of such a family can be classified by one parameter (in this case, by $t = \frac{b}{a^n}$), giving rise to a cover of $\mathbb{P}^1_{\mathbb{Q}}$ ramified at three rational points and unramified elsewhere. These covers ($(k, n) = 1$) are typically obtained when one uses the rigidity method in order to obtain $\mathbb{Q}$-regular S_n-extensions of $\mathbb{Q}(T)$. Moreover, in this situation one can always deduce $\mathbb{Q}$-regular A_n-extensions of $\mathbb{Q}(U)$, defined by polynomials of the same type (see, for example, [8, Lemma 4.5.1] and [8, 8.3.1]). The fact that these A_n-extensions do not admit tamely ramified rational specializations seems consistent with Birch's suggestion [2, p. 35] that 'rigid' constructions usually give rise to wild specializations. We may note that, however, only the S_n-extensions of $\mathbb{Q}(T)$ alluded to above are 'rigid' (not the deduced A_n-extensions of $\mathbb{Q}(U)$) and these always admit tame specializations (as in Proposition 1).

Remark 20. If we do not restrict ourselves to considering trinomial extensions, then it is possible to obtain, for every n, A_n-extensions of $\mathbb{Q}$ unramified at all primes in an arbitrary prefixed finite set S, possibly including the infinity prime. Indeed, in [7] we proved that there always exists a totally real monic polynomial $f(X) \in \mathbb{Z}[X]$ of degree n, with Galois group A_n over $\mathbb{Q}$, and such that its discriminant $D(f)$ is not divisible by any prime in S. Moreover, more specific local behaviors can also be required (for every n and every S) as, for example, that all primes in S split completely in the A_n-extension $\mathbb{Q}_f/\mathbb{Q}$.

References

[1] T.M. Apostol, Introduction to Analytic Number Theory, Springer, Berlin, 1976.
[2] B. Birch, Noncongruence subgroups, in: Leila Schneps (Ed.), Covers and Drawings, The Grothendieck theory of dessins d'enfants, Cambridge University Press, Cambridge, 1994, pp. 25–46.
[3] S.D. Cohen, A. Movahhedi, A. Salinier, Double transitivity of Galois groups of trinomials, Acta Arith 82 (1997) 1–15.
[4] A. Hermez, A. Salinier, Rational trinomials with the alternating group as Galois group, J. Number Theory 90 (2001) 113–129.
[5] P. Llorente, E. Nart, N. Vila, Discriminants of number fields defined by trinomials, Acta Arith. 43 (1984) 367–373.
[6] J. Neukirch, Algebraic Number Theory, Springer, Berlin, 1999.
[7] B. Plans, N. Vila, Tame A_n-extensions of $\mathbb{Q}$, J. Algebra 266 (2003) 27–33.
[8] J-P. Serre, Topics in Galois Theory, Jones and Bartlett, Boston, 1992.