Scientific Research Publishing

Advances in Pure Mathematics, 2022, 12, 744-756
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

An Infinite Family of Number Fields with No Inert Primes

François Emmanuel Tanoé

UFR Mathematics and Computer Science, Félix Houphouet-BOIGNY University, Abidjan, Ivory Coast
Email: aziz_marie@yahoo.fr

How to cite this paper: Tanoé, F.E. (2022) An Infinite Family of Number Fields with No Inert Primes. *Advances in Pure Mathematics*, **12**, 744-756.
https://doi.org/10.4236/apm.2022.1212057

Received: November 12, 2022
Accepted: December 26, 2022
Published: December 29, 2022

Abstract

The goal of this paper is to show that there are infinitely many number fields $K/\mathbb{Q}$, for which there is no inert prime $p \in \mathbb{N}^*$, *i.e.* $\forall p \in \mathbb{N}^*$ a prime number, $\nexists$ $\mathfrak{P}$ prime ideal of K such that $p\mathbb{Z}_K = \mathfrak{P}$, where: $\mathbb{Z}_K$ is the Dedekind domain of the integer elements of K. To prove such a result, consider for any prime p, the decomposition into a product of prime ideals of $\mathbb{Z}_K$, of the ideal $p\mathbb{Z}_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_{i,p}}$. From this point, we use on the one hand: 1) The well-known property that says: If $\exists\ \theta \in \mathbb{Z}_K \,/\, \mathbb{Z}_K = \mathbb{Z}[\theta]$, then the ideal $p\mathbb{Z}_K$ decomposes into a product of prime ideals of $\mathbb{Z}_K$ as following:

$p\mathbb{Z}_K = \prod_{i=1}^{g} \mathfrak{P}_i^{e_{i,p}} = \prod_{i=1}^{g} \left(p\mathbb{Z}[\theta] + f_{i,p}(\theta)\mathbb{Z}[\theta] \right)^{e_{i,p}}$. (where: $f_\theta(X) = X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$; is the irreducible polynomial of θ, and,

$\overline{f}_{\theta,p}(X) = X^n + \overline{a_{n-1}}X^{n-1} + \cdots + \overline{a_1}X + \overline{a_0} = \prod_{i=1}^{g} \left(\overline{f}_{i,p}(X) \right)^{e_{i,p}} \in \mathbb{F}_p[X]$ is its reduction modulo p, which leads to a product of irreducible polynomials in $\mathbb{F}_p[X]$). It is clear that because if $\overline{f}_p(X)$ is reducible in $\mathbb{F}_p[X]$, then consequently p is not inert. Now, we prove the existence of such p, by proving explicit such p as follows. So we use on the other hand: 2) this property that we prove, and which is: If $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{Z}[X]$, is an irreducible normalized integer polynomial, whose splitting field is $\Sigma_f = \mathbb{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$, then for any prime number $p \in \mathbb{N}$:

$\overline{f}_p(X) = X^4 + \overline{a_3}X^3 + \overline{a_2}X^2 + \overline{a_1}X + \overline{a_0} \in \mathbb{F}_p[X]$ is always a reducible polynomial. 3) Consequently, and this closes our proof: let's consider the set (whose cardinality is infinite) of monogenic biquadratic number fields:

$\mathcal{M} = \left\{ K = \mathbb{Q}\left(\sqrt{dm}, \sqrt{dn}\right) \,/\, \exists \theta_K \in \mathbb{Z}_K \text{ such that } \mathbb{Z}_K = \mathbb{Z}[\theta_K] \right\}$. Then each

$f_\theta(X)$ checks the above properties, this means that for family $\mathcal{M}$, all its fields, do not admit any inert prime numbers $p \in \mathbb{N}$.

2020-Mathematics Subject Classification (MSC2020)

11A41 - 11A51 - 11D25 - 11R04 - 11R09 - 11R11 - 11R16 - 11R32 - 11T06 - 12E05 - 12F05 -12F10 -13A05-13A15 - 13B02 - 13B05 - 13B10 - 13B25 -13F05

Keywords

Fields Extensions, Splitting Fields Polynomials, Finite Fields Extensions, Polynomials of $\mathbb{F}_p[X]$, Dedekind Ring, Ramification Theory, Monogeneity, Quadratic & Biquadratic Fields, Irreducible Polynomials of Degree 3 & 4

1. Introduction

Let $K/\mathbb{Q}$ be a Galois extension of $\mathbb{Q}$ of degree *n*. The question we ask ourselves is the following: Do such Galois extensions exist, which are free of inert primes? To our knowledge, there are no studies on such a property, although we have many theorems on ramification, which could allow in certain cases to seriously study this problem. The question is relevant, because apart from the arithmetic description of the prime ideals of $\mathbb{Z}_K$, this kind of results can facilitate the calculation of the number of classes of *K*.

All the reminders and definitions that follow can be found in [1].

- Let us recall, that it is well known that the ring of integers $\mathbb{Z}_K$ of *K*, is a free $\mathbb{Z}$-module of rank $n = [\mathbb{Z}_K : \mathbb{Z}]$, moreover it is a Dedekind ring, and therefore, $\forall p$ a prime of $\mathbb{N}$, then:

$$n = efg \tag{1}$$

where: $p\mathbb{Z}_K = \mathfrak{P}_1^e \cdots \mathfrak{P}_g^e$ with $\mathfrak{P}_i / p$ being all prime ideals of $\mathbb{Z}_K$ lying above *p*, and that they are in number $g = g_{K/\mathbb{Q}}$, where $e = e_{K/\mathbb{Q}}$ is the ramification index of the $\mathfrak{P}_i$, and $f = f_{K/\mathbb{Q}} = \left[\mathbb{Z}_{K/\mathfrak{P}_i} : \mathbb{F}_p\right]$, $\forall i = 1, \cdots, g$, is the residual degree of the $\mathfrak{P}_i / p$.

Definition 1.1. *The notations remaining the same, we have*:

1) *The prime number* $p \in \mathbb{N}$, *is said to be inert in K* $\Leftrightarrow$ $\exists$ $\mathfrak{P}$ *a prime ideal of K such that* $p\mathbb{Z}_K = \mathfrak{P} \Leftrightarrow f = n$, $e = 1$ *and* $g = 1$.

2) *The prime number* $p \in \mathbb{N}$ *is said to be ramified in K* $\Leftrightarrow$ $e \geq 2$ $\Leftrightarrow$ $p / discr(K)$.

Definition 1.2. *The Galois number field K is said to be monogenic* $\Leftrightarrow$ $\exists$ $\theta \in \mathbb{Z}_K$ *such that* $\mathbb{Z}_K = \mathbb{Z}[\theta] \Leftrightarrow \{1, \theta^2, \cdots, \theta^{n-1}\}$ *forms a* $\mathbb{Z}$*-basis* (*called power basis*) *of the* $\mathbb{Z}$*-module* $\mathbb{Z}_K$.

Notations 1.1. *When K is monogenic, then in particular* $K = \mathbb{Q}[\theta]$. *Let denotes by* $f_\theta(X)$ *or simply* $f(X)$, *the irreducible polynomial of* θ, *then*:

$$f(X) = X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X];$$

And $\forall p$ *a prime number of* $\mathbb{N}$, *we note*

$\overline{f}_p(X) = X^n + \overline{a_{n-1}}X^{n-1} + \cdots + \overline{a_1}X + \overline{a_0} \in \mathbb{F}_p[X]$, *and by* $\overline{f}_p(X) = \prod_{i=1}^{g}\left(\overline{f}_{i,p}(X)\right)^e$, *its decomposition into irreducible factors product of* $\mathbb{F}_p[X]$:

Where: $f_{i,p}(X) = X^{n_i} + b_{i,n_i-1}X^{n_i-1} + \cdots + b_{i,1}X + b_{i,0} \in \mathbb{Z}[X]$, *and* $\overline{f}_{i,p}(X) = X^{n_i} + \overline{b_{i,n_i-1}}X^{n_i-1} + \overline{b_{i,n_i-2}}X^{n_i-2} + \cdots + \overline{b_{i,1}}X + \overline{b_{i,0}} \in \mathbb{F}_p[X]$, *are irreducibles in* $\mathbb{F}_p[X]$.

Definition 1.3. *We denote by* $\mathcal{M} = \left\{K = \mathbb{Q}\left(\sqrt{dm}, \sqrt{dn}\right) / \exists \theta \in \mathbb{Z}_K \text{ such thay } \mathbb{Z}_K = \mathbb{Z}[\theta]\right\}$, *the set of monogenic biquadratic number fields.* (*This set has infinite cardinality cf.* [2]);

We have the following well-known important proposition, the notations being the same:

Proposition 1.1. *Let K be a monogenic Galois number field and* $\theta \in \mathbb{Z}_K / \mathbb{Z}_K = \mathbb{Z}[\theta]$, *then* $\forall p$ *a prime number of* $\mathbb{N}$, *we have*:

$$p\mathbb{Z}_K = p\mathbb{Z}[\theta] = \prod_{i=1}^{g}\left(p\mathbb{Z}[\theta] + f_{i,p}(\theta)\mathbb{Z}[\theta]\right)^e.$$

As a result we have the following corollary.

Corollary 1.1. *Let K be a monogenic Galois number field. If for all prime numbers* $p \in \mathbb{N}$, *the polynomial* $\overline{f}_p(X)$ *is decomposed in* $\mathbb{F}_p[X]$. (*i.e. is not irreducible*), *then there does not exist any prime number* $p \in \mathbb{N}$, *which is inert in K.*

In this paper, from the introduction, we ask whether there exist number fields *K*, such that $\forall p$, a prime integer, *p* is never inert in *K*. The answer is positive for small degree 4, since we have found an infinite family of such degree, for which all its fields satisfy this property.

From a general point of view, and as a relevant issue, one can look for other families of fields where this property remains true, those could be Galois or not.

The main goal of this article, is to show Theorem 3.1., which proves the existence of an infinite family of Galoisian numbers fields, namely $\mathcal{M}$ (cf. Definition 1.3.), having no inert prime integer *p*, when considering each field $K \in \mathcal{M}$.

To proove this, we show that all fields belonging to the family $\mathcal{M}$, are such that the irreducible polynomials associated with their monogenic element, satisfy Proposition 3.1.; then as a result, the Proposition 1.1. is true, but with necessarily $g \neq 1$, which established the seeked result.

Thus, in the family $\mathcal{M}$, the equation: $4 = efg$, cf. (1), is always checked with necessarily $f \neq 4$.

2. Ramification—Quadratic and Biquadratic Fields—Lemmas

Let's take $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{Z}[X]$ an irreducible normalized integer polynomial, and for any prime number *p*, and let's consider the map $\overline{\alpha_p}$ (cf. Lemma 2.2.) and denotes its restriction morphisme map by $\overline{\alpha_{p|\mathbb{Z}[X]}}: \mathbb{Z}[X] \to \mathbb{F}_p[X]$, defined by: $\left(\overline{\alpha_{p|\mathbb{Z}[X]}}(f)\right)(X) = \left(\overline{\alpha_p}(f)\right)(X) = \overline{f}_p(X)$ $= X^4 + \overline{a_3}X^3 + \overline{a_2}X^2 + \overline{a_1}X + \overline{a_0} \in \mathbb{F}_p[X]$.

Let's put Σ_f for the splitting field of the polynomial $f(X)$. Then it is known that Σ_f can be (cf. [3]): either a biquadratic field; or a cyclic quartic field (with a single sub-quadratic field); or a non-galoisian quartic field (with a single sub-quadratic field); or to finish a non-galoisian quartic field, without any subquadratic fields. In our case we will deal with Σ_f when it belongs to a biquadratic field type.

Notations 2.1. *For a square free integer* $a \neq 0,1$, *let's denotes by* $\mathbb{Z}_{\mathbb{Q}(\sqrt{a})}$ *the integral ring of* $\mathbb{Q}(\sqrt{a})$. *It is well known that*:

$$\mathbb{Z}_{\mathbb{Q}(\sqrt{a})} = \mathbb{Z}\left[\sqrt{a^*}\right] = \begin{cases} \mathbb{Z}\left[\dfrac{1+\sqrt{a}}{2}\right] & \text{if } a \equiv 1 \pmod 4 \\ \mathbb{Z}\left[\sqrt{a}\right] & \text{if } a \equiv -1 \text{ or } 2 \pmod 4. \end{cases},$$

And that the conjugate of $\sqrt{a^*}$ *is* $\overline{\sqrt{a^*}} = \begin{cases} \dfrac{1-\sqrt{a}}{2} = 1 - \dfrac{1+\sqrt{a}}{2}, & \text{if } a \equiv 1 \pmod 4 \\ -\sqrt{a}, & \text{if } a \equiv -1 \text{ or } 2 \pmod 4. \end{cases}$.

Let's recall that for a prime ideal $\mathfrak{p}$ of $\mathbb{Z}_{\mathbb{Q}(\sqrt{a})}$ over a prime p, we get $\left(\mathbb{Z}_{\mathbb{Q}(\sqrt{a})}\right)_{/\mathfrak{p}} = \mathbb{F}_p\left[\sqrt{a^*}\right]$, where the element $\sqrt{a^*}$ is a root of $X^2 - X + \dfrac{1-a}{4} \in \mathbb{Z}[X]$ if $a \equiv 1 \pmod 4$ (resp. $X^2 - a \in \mathbb{Z}[X]$, if $a \equiv -1$ or $2 \pmod 4$).

As a consequence:

Proposition 2.1. *For a square free integer* $a \neq 0,1$, *and a rationnal prime integer p/a, if we take a look at* $\mathbb{F}_p\left[\sqrt{a^*}\right]$, *we have*:

$$\mathbb{F}_p \ni \sqrt{a^*} = \begin{cases} 2^{-1}; \text{ if } a \equiv 1 \pmod 4; \text{ because } X^2 - X + 4^{-1} = \left(X - 2^{-1}\right)^2; \\ 0_{\mathbb{F}_p}; \text{ if } a \equiv -1 \text{ or } 2 \pmod 4. \end{cases}$$

Note that we have a canonical written form for $\mathbb{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$, which we will use in this paper (cf. [2]):

Remarks 2.1. *In the following we'll use the unique written form for a biquadratic field* $\mathbb{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$, *that is*:

1) $d, m, n \in \mathbb{Z}^*$, *square free and pairwise relatively prime, and* $d > 0$, $m > n$ *odds*, $dm, dn, mn \neq 1$, $dm \equiv dn \equiv -1, 1$ *or* 2 (*mod* 4), *and in the case where* $dm \equiv dn \equiv 1 \pmod 4$ *we put* $d < Inf\left(|m|, |n|\right)$.

In addition, in the other cases, we define $\delta = 0$ *or* 1 *such that* $mn \equiv (-1)^{\delta} \pmod 4$, *when* $dm \equiv dn \equiv -1$ *or* 2 (*mod* 4). *That is* $\delta = 0$ *when* $dm \equiv dn \equiv -1 \pmod 4$, *and* $\delta = 1$ *when* $dm \equiv dn \equiv 2 \pmod 4$.

2) *When* $\alpha_0 \in \mathbb{Z}_{\mathbb{Q}(\sqrt{dm}, \sqrt{dn})}$ (*the ring of integer elements of the field* $\mathbb{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$), *we will consider its conjugates under the Galois group*, $G = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$, *where the action on the basis of K*: $\varepsilon = \left\{\varepsilon_0 = 1, \varepsilon_1 = \sqrt{dm}, \varepsilon_2 = \sqrt{dn}, \varepsilon_3 = \sqrt{mn}\right\}$ *is given by the matrix*:

$$\left(a_{ij}\right)_{0\le i,j\le 3}=\left(\sigma_i\left(\varepsilon_j\right)/\varepsilon_j\right)_{0\le i,j\le 3}=\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&1&-1\\1&-1&-1&1\end{pmatrix}.$$

There let's make some other remarks and lemmas we'll need further:

2.1. Lemmas

In the following we will be dealing with fields $\mathbb{F}_p\left[\sqrt{dm^*}\right]$, $\mathbb{F}_p\left[\sqrt{dn^*}\right]$, and $\mathbb{F}_p\left[\sqrt{mn^*}\right]$, so we need the following lemmas

Lemma 2.1. *Let* $a\neq 0,1$ *be a square free integer, and* p *be a prime integer, such that any one of the following* 3 *cases is realized*:

i) $p\nmid a$;

ii) $p\neq 2,\ p\nmid a$ *but* $\left(\frac{a}{p}\right)=1$;

iii) $p=2$ *and* $p\nmid a$, *where*: $a\equiv 3\left(\mathrm{mod}\,4\right)$ *or* $a\equiv 1\left(\mathrm{mod}\,8\right)$.

Then we have:

$\left(\mathbb{Z}_{\mathbb{Q}\left(\sqrt{a}\right)}\right)_{/\mathfrak{p}}=\mathbb{F}_p\left[\sqrt{a^*}\right]=\mathbb{F}_p$, *for any prime ideal* $\mathfrak{p}\mid p$ *of* $\mathbb{Z}_{\mathbb{Q}\left(\sqrt{a}\right)}$.

Proof 2.1. *This remains to proove in fact that* $\sqrt{a^*}\in\mathbb{F}_p$.

- *If case* i) *holds, then cf. Proposition* 2.1., $\sqrt{a^*}=2^{-1}$ or $0_{\mathbb{F}_p}\Rightarrow\mathbb{F}_p\left[\sqrt{a^*}\right]=\mathbb{F}_p$.
- *If case* ii) *holds*: *From* $\left(\frac{a}{p}\right)=1\ \Rightarrow\ a=\beta^2$ *is a square in* $\mathbb{F}_p$, *so the polynomials* $X^2-X+\frac{1-a}{4}$ *or* X^2-a, *admit the square* β^2 *or* $(2\beta)^2$ *as discriminant so* $\sqrt{a^*}\in\left\{\beta,2^{-1}\left(1+\beta\right)\right\}\subset\mathbb{F}_p$, *then we get* $\mathbb{F}_p\left[\sqrt{a^*}\right]=\mathbb{F}_p$.
- *If case* iii) *holds*: *i.e.* $p=2$ *and* $p\nmid a$, *let's consider in* $\mathbb{F}_2\left[X\right]$, *the two subcases*:

1) $a\equiv 3\left(\mathrm{mod}\,4\right)\ \Rightarrow\ X^2-a=\left(X+1\right)^2\ \Rightarrow\ \sqrt{a^*}=1\in\mathbb{F}_2$.

2) $a\equiv 1\left(\mathrm{mod}\,4\right)$ *but* $a\equiv 1\left(\mathrm{mod}\,8\right)\ \Rightarrow\ X^2-X+\frac{1-a}{4}=X^2-X\ \Rightarrow$ $\sqrt{a^*}\in\left\{0_{\mathbb{F}_p},1\right\}\subset\mathbb{F}_2$.

So in these two cases, we get as stated: $\mathbb{F}_2\left[\sqrt{a^*}\right]=\mathbb{F}_2$.

Now look at the morphisme map α_p, and its extension $\overline{\alpha_p}$, and let's take accompt the lemma upthere, then we deduce this other Lemma.

Lemma 2.2. *Let* $a\neq 0,1$ *be a square free integer and consider any prime ideal* $\mathfrak{p}\mid p$, *taken as in lemma* 2.1. *We get this commutative diagram of ring morphisms*:

$$\begin{array}{ccc}\mathbb{Z}_{\mathbb{Q}\left(\sqrt{dm}\right)}=\mathbb{Z}\left[\sqrt{a^*}\right] & \xrightarrow{\alpha_p} & \left(\mathbb{Z}_{\mathbb{Q}\left(\sqrt{dm}\right)}\right)_{/\mathfrak{p}}=\mathbb{F}_p\left[\sqrt{a^*}\right]=\mathbb{F}_p\\ \downarrow & \circlearrowleft & \downarrow\\ \mathbb{Z}\left[\sqrt{a^*}\right][X] & \xrightarrow{\overline{\alpha_p}} & \mathbb{F}_p\left[\sqrt{a^*}\right][X]=\mathbb{F}_p[X]\end{array}$$

Remarks 2.2. a) *From this lemma, if a rationnal prime integer p, and an integer a are such that given ones in the Lemma* 2.1, *then any factorization of normalized polynomials, each of degree* 2:

$f = g \times h$ *in* $\mathbb{Z}\left[\sqrt{a^*}\right][X]$, *induces the non-trival factorization*:

$$\overline{\alpha_p}(f) = \overline{\alpha_p}(g) \times \overline{\alpha_p}(h) \text{ in } \mathbb{F}_p[X] = \mathbb{F}_p\left[\sqrt{a^*}\right][X].$$

That implies that: $\overline{f_p} = \overline{g_p} \times \overline{h_p}$ *is reduced in* $\mathbb{F}_p[X]$.

b) *Always as a consequence of lemma* 2.2, *if* $p = 2$, *and* $2 \nmid a$, *once* $\sqrt{a^*} \in \mathbb{F}_2$ *then any factorization of the same type that above*:

$f = g \times h$ *in* $\mathbb{Z}\left[\sqrt{a^*}\right][X]$, *induces the non-trivial factorization*:

$$\overline{\alpha_2}(f) = \overline{\alpha_2}(g) \times \overline{\alpha_2}(h) \text{ in } \mathbb{F}_2[X] = \mathbb{F}_2\left[\sqrt{a^*}\right][X].$$

And therefore: $\overline{f_2} = \overline{g_2} \times \overline{h_2}$ *is reduced in* $\mathbb{F}_2[X] = \mathbb{F}_2\left[\sqrt{a^*}\right][X]$.

⋆ *Let's note that we can have different type of factorization*:

- *If* $\overline{g_p} = \overline{h_p}$ *then* $\overline{f_p} = \left(\overline{g_p}\right)^2$, *and in this case for instance* $\overline{g_p}(X) = X^2 \Rightarrow \overline{f_p} = X^4$.
- *If* $\overline{g_p} \neq \overline{h_p}$ *and if* $\overline{g_p}$ *and* $\overline{h_p}$ *split, and binomes are different in pairs, then* $\overline{f_p} = \prod_{i=0}^{3}(X - \beta_i)$.

2.2. Integral Bases and Notations in $\mathbb{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$.

Looking at $\mathbb{Q}\left(\sqrt{dm}, \sqrt{dn}\right)$, let's recall that from [2] and [4], we have.

Proposition 2.2. *When* $dm \equiv dn \equiv 1 \pmod 4$, *we have an integral basis for* $\mathbb{Z}_{\mathbb{Q}\left(\sqrt{dm}, \sqrt{dn}\right)}$, *which is*: $\mathfrak{B} = \left\{1, \frac{1+\sqrt{mn}}{2}, \frac{1+\sqrt{dn}}{2}, \frac{1+\sqrt{dm}+\sqrt{dn}+\lambda\sqrt{mn}}{4}\right\}$ *where* $\pm 1 = \lambda \equiv d \equiv m \equiv n \pmod 4$.

So for $\alpha_0 \in \mathbb{Z}_{\mathbb{Q}\left(\sqrt{dm}, \sqrt{dn}\right)}$, there exist $a_0, a_1, a_2, a_3 \in \mathbb{Z}$, and consequently $A_0, A_1, A_2, A_3 \in \mathbb{Q}$ hereafter, such that:

$$\begin{aligned}\alpha_0 &= a_0 + a_1\frac{1+\sqrt{mn}}{2} + a_2\frac{1+\sqrt{dn}}{2} + a_3\frac{1+\sqrt{dm}+\sqrt{dn}+\lambda\sqrt{mn}}{4} \\ &= A_0 + A_1\sqrt{dm} + A_2\sqrt{dn} + A_3\sqrt{mn},\end{aligned}$$

where: $\begin{cases} A_0 = \dfrac{4a_0 + 2a_1 + 2a_2 + a_3}{4}, \\ A_1 = \dfrac{a_3}{4}, \\ A_2 = \dfrac{2a_2 + a_3}{4}, \\ A_3 = \dfrac{2a_1 + \lambda a_3}{4}. \end{cases}$,

So we get by action of the Galois group $\left(a_1 = \sigma_1(a_0); a_2 = \sigma_2(a_0); a_3 = \sigma_3(a_0)\right)$:

$$\begin{aligned}\alpha_1 &= a_0 + a_1 + a_2 + a_3\left(\frac{1+\lambda}{2}\right) - \left(a_1 + \lambda a_3\right)\frac{1+\sqrt{mn}}{2}\\ &\quad - \left(a_2 + a_3\right)\frac{1+\sqrt{dn}}{2} + a_3\frac{1+\sqrt{dm}+\sqrt{dn}+\lambda\sqrt{mn}}{4}:\\ &= A_0 + A_1\sqrt{dm} - A_2\sqrt{dn} - A_3\sqrt{mn};\end{aligned}$$

$$\begin{aligned}\alpha_2 &= a_0 + a_1 - a_1\frac{1+\sqrt{mn}}{2} + \left(a_2 + a_3\right)\frac{1+\sqrt{dn}}{2} - a_3\frac{1+\sqrt{dm}+\sqrt{dn}+\lambda\sqrt{mn}}{4}\\ &= A_0 - A_1\sqrt{dm} + A_2\sqrt{dn} - A_3\sqrt{mn};\end{aligned}$$

$$\begin{aligned}\alpha_3 &= a_0 + a_2 + a_3\left(\frac{1-\lambda}{2}\right) + \left(a_1 + \lambda a_3\right)\frac{1+\sqrt{mn}}{2}\\ &\quad - a_2\frac{1+\sqrt{dn}}{2} - a_3\frac{1+\sqrt{dm}+\sqrt{dn}+\lambda\sqrt{mn}}{4}\\ &= A_0 - A_1\sqrt{dm} - A_2\sqrt{dn} + A_3\sqrt{mn}.\end{aligned}$$

Proposition 2.3. *When* $dm \equiv dn \equiv -1 \pmod 4$, *we have an integral basis for* $\mathbb{Z}_{\mathbb{Q}\left(\sqrt{dm},\sqrt{dn}\right)}$, *which is*: $\mathfrak{B} = \left\{1, \frac{1-\delta+2^{\delta}\sqrt{mn}}{2}, \sqrt{dn}, \frac{\sqrt{dm}+\sqrt{dn}}{2}\right\}$.

And there exist too $a_0, a_1, a_2, a_3 \in \mathbb{Z}$, and consequently $A_0, A_1, A_2, A_3 \in \mathbb{Q}$, hereafter, such that:

$$\begin{aligned}\alpha_0 &= a_0 + a_1\frac{1-\delta+2^{\delta}\sqrt{mn}}{2} + a_2\sqrt{dn} + a_3\frac{\sqrt{dm}+\sqrt{dn}}{2}\\ &= A_0 + A_1\sqrt{dm} + A_2\sqrt{dn} + A_3\sqrt{mn},\end{aligned}$$

where in this case: $\begin{cases} A_0 = \dfrac{2a_0 + a_1\left(1-\delta\right)}{2}, \\ A_1 = \dfrac{a_3}{2}, \\ A_2 = \dfrac{2a_2 + a_3}{2}, \\ A_3 = \dfrac{2^{\delta}a_1}{2}. \end{cases}$,

And we get:

$$\begin{aligned}\alpha_1 &= a_0 + a_1\left(1-\delta\right) - a_1\frac{1-\delta+2^{\delta}\sqrt{mn}}{2} - \left(a_2 + a_3\right)\sqrt{dn} + a_3\frac{\sqrt{dm}+\sqrt{dn}}{2}\\ &= A_0 + A_1\sqrt{dm} - A_2\sqrt{dn} - A_3\sqrt{mn};\end{aligned}$$

$$\begin{aligned}\alpha_2 &= a_0 + a_1\left(1-\delta\right) - a_1\frac{1-\delta+2^{\delta}\sqrt{mn}}{2} + \left(a_2 + a_3\right)\sqrt{dn} - a_3\frac{\sqrt{dm}+\sqrt{dn}}{2}\\ &= A_0 - A_1\sqrt{dm} + A_2\sqrt{dn} - A_3\sqrt{mn};\end{aligned}$$

$$\begin{aligned}\alpha_3 &= a_0 + a_1\frac{1-\delta+2^{\delta}\sqrt{mn}}{2} - a_2\sqrt{dn} - a_3\frac{\sqrt{dm}+\sqrt{dn}}{2}\\ &= A_0 - A_1\sqrt{dm} - A_2\sqrt{dn} + A_3\sqrt{mn}.\end{aligned}$$

3. Splitting Fields and Decomposition Modulo p Characterization Theorems for Biquadratic Fields

Under these notations we get the following main theorem:

Proposition 3.1. *Let* $f(X)=X^4+a_3X^3+a_2X^2+a_1X+a_0\in\mathbb{Z}[X]$ *be an irreducible polynomial, and* Σ_f *its splitting fields. Then there is an implication from proposition* (i) *to proposition* (ii):

(i) $\Sigma_f=\mathbb{Q}\left(\sqrt{dm},\sqrt{dn}\right)$.

(ii) *For every prime number* $p\in\mathbb{N}$, *the polynomial* $\overline{f_p}(X)=X^4+\overline{a_3}X^3+\overline{a_2}X^2+\overline{a_1}X+\overline{a_0}$, *is always reducible in* $\mathbb{F}_p[X]$.

Proof 3.1. • *Let's show that* (i) $\Rightarrow$ (ii).

The hypothesis (i) *implies that* $f(X)=\prod_{i=0}^{3}(X-\alpha_i)$, *with the* $\alpha_i\in\mathbb{Z}_{\mathbb{Q}\left(\sqrt{dm},\sqrt{dn}\right)}$.

Let's solve simultaneously, the both cases $dm\equiv dn\equiv 1\pmod 4$ *and* $dm\equiv dn\equiv -1$ *or* $2\pmod 4$.

So from Proposition 2.2. & 2.3., *we know that there exists* $A_0,A_1,A_2,A_3\in\mathbb{Q}$ *such that*:

$$\begin{aligned}\alpha_0&=A_0+A_1\sqrt{dm}+A_2\sqrt{dn}+A_3\sqrt{mn},\\ \alpha_1&=A_0+A_1\sqrt{dm}-A_2\sqrt{dn}-A_3\sqrt{mn},\\ \alpha_2&=A_0-A_1\sqrt{dm}+A_2\sqrt{dn}-A_3\sqrt{mn},\\ \alpha_3&=A_0-A_1\sqrt{dm}-A_2\sqrt{dn}+A_3\sqrt{mn}.\end{aligned}$$

Let's consider the following six polynomials, having noticed that:

$$(\alpha_0+\alpha_1,\alpha_0\alpha_1)\ \text{and}\ (\alpha_2+\alpha_3,\alpha_2\alpha_3)\in\mathbb{Z}_{\mathbb{Q}\left(\sqrt{dm^\star}\right)},$$

$$(\alpha_0+\alpha_2,\alpha_0\alpha_2)\ \text{and}\ (\alpha_1+\alpha_3,\alpha_1\alpha_3)\in\mathbb{Z}_{\mathbb{Q}\left(\sqrt{dn^\star}\right)},\ \text{And}$$

$$(\alpha_0+\alpha_3,\alpha_0\alpha_3)\ \text{and}\ (\alpha_1+\alpha_2,\alpha_1\alpha_2)\in\mathbb{Z}_{\mathbb{Q}\left(\sqrt{mn^\star}\right)}:$$

• $$\begin{aligned}g_1(X)&=(X-\alpha_0)(X-\alpha_1)\in\mathbb{Z}_{\mathbb{Q}\left(\sqrt{dm^\star}\right)}[X]\\&=X^2-2\left(A_2+A_1\sqrt{dm}\right)X+\left(A_0^2+A_1^2dm-A_2^2dn-A_3^2mn\right.\\&\quad\left.+2\left(A_0A_1-A_2A_3n\right)\sqrt{dm}\right)\\&=X^2-B_1X+B_2=X^2-\left(b_{10}+b_{11}\sqrt{dm^\star}\right)X+\left(b_{20}+b_{21}\sqrt{dm^\star}\right)\end{aligned},$$

with $b_{ij}\in\mathbb{Z}$;

And:

$$\begin{aligned}h_1(X)&=(X-\alpha_2)(X-\alpha_3)\in\mathbb{Z}_{\mathbb{Q}\left(\sqrt{dm^\star}\right)}[X]\\&=X^2-2\left(A_0-A_1\sqrt{dm}\right)X-\left(A_0^2+A_1^2dm-A_2^2dn-A_3^2mn\right.\\&\quad\left.-2\left(A_0A_1-A_2A_3n\right)\sqrt{dm}\right),\\&=X^2-\overline{B_1}X+\overline{B_2}=X^2-\left(b_{10}+b_{11}\sqrt{dm^\star}\right)X+\left(b_{20}+b_{21}\sqrt{dm^\star}\right).\end{aligned}$$

Similarly consider:

$$\begin{aligned} g_2(X) &= (X-\alpha_0)(X-\alpha_2) \in \mathbb{Z}_{\mathbb{Q}\left(\sqrt{dn^\star}\right)}[X] \\ &= X^2 - 2\left(A_0 + A_2\sqrt{dn}\right)X + \left(A_0^2 + A_2^2 dn - A_1^2 dm - A_3^2 mn\right. \\ &\left. + 2\left(A_0A_2 - A_1A_3 m\right)\sqrt{dn}\right) \\ &= X^2 - C_1X + C_2 = X^2 - \left(c_{10} + c_{11}\sqrt{dn^\star}\right)X + \left(c_{20} + c_{21}\sqrt{dn^\star}\right) \end{aligned}$$

•

with $c_{ij} \in \mathbb{Z}$;

And:

$$\begin{aligned} h_2(X) &= (X-\alpha_1)(X-\alpha_3) \in \mathbb{Z}_{\mathbb{Q}\left(\sqrt{dn^\star}\right)}[X] \\ &= X^2 - 2\left(A_0 - A_2\sqrt{dn}\right)X + \left(A_0^2 + A_2^2 dn - A_1^2 dm - A_3^2 mn\right. \\ &\left. - 2\left(A_0A_2 - 2A_1A_3 m\right)\sqrt{dn}\right) \\ &= X^2 - \overline{C_1}X + \overline{C_2} = X^2 - \left(c_{10} + c_{11}\overline{\sqrt{dn^\star}}\right)X + \left(c_{20} + c_{21}\overline{\sqrt{dn^\star}}\right). \end{aligned}$$

And, to finish similarly consider:

$$\begin{aligned} g_3(X) &= (X-\alpha_0)(X-\alpha_3) \in \mathbb{Z}_{\mathbb{Q}\left(\sqrt{mn^\star}\right)}[X] \\ &= X^2 - 2\left(A_0 + A_3\sqrt{mn}\right)X + \left(A_0^2 + A_3^2 mn - A_1^2 dm - A_2^2 dn\right. \\ &\left. + 2\left(A_0A_3 - A_1A_2 d\right)\sqrt{mn}\right) \\ &= X^2 - D_1X + D_2 = X^2 - \left(d_{10} + d_{11}\sqrt{mn^\star}\right)X + \left(d_{20} + d_{21}\sqrt{mn^\star}\right) \end{aligned}$$

with $d_{ij} \in \mathbb{Z}$;

And:

$$\begin{aligned} h_3(X) &= (X-\alpha_1)(X-\alpha_2) \in \mathbb{Z}_{\mathbb{Q}\left(\sqrt{mn^\star}\right)}[X] \\ &= X^2 - 2\left(A_0 - A_3\sqrt{mn}\right)X - \left(A_0^2 + A_3^2 mn - A_1^2 dm - A_2^2 dn\right. \\ &\left. - 2\left(A_0A_3 - A_1A_2 d\right)\sqrt{mn}\right) \\ &= X^2 - \overline{D_1}X + \overline{D_2} = X^2 - \left(d_{10} + d_{11}\overline{\sqrt{mn^\star}}\right)X + \left(d_{20} + d_{21}\overline{\sqrt{mn^\star}}\right). \end{aligned}$$

We deduce the factorization:

$$g_j \times h_j = f \text{, with } \deg\left(g_j\right) = \deg\left(h_j\right) = 2, \forall j = 1,2,3;$$

And this: *Respectively in* $\mathbb{Z}\left[\sqrt{dm^\star}\right][X]$, $\mathbb{Z}\left[\sqrt{dn^\star}\right][X]$ *and* $\mathbb{Z}\left[\sqrt{mn^\star}\right][X]$.

These factorizations will lead to non-trivial factorizations of $\overline{\alpha_p}(f) = \overline{f_p}$ *in* $\mathbb{F}_p\left[\sqrt{a^*}\right][X] = \mathbb{F}_p[X]$, *for all prime number p*. (*cf. Remarks* 2.2.). *To prove it, it suffices to show that the propositions of Lemma* 2.1. *is holding.*

Let's prove it effectively:

A) *Suppose that* $p \nmid dmn$.

1) $p \neq 2$.

a) *If* $p \nmid d$ *then* $p \nmid dm$ (*and* $p \nmid dn$) *then* $\sqrt{dm} = 0_{\mathbb{F}_p}$ (*and*

$\sqrt{dn}=0_{\mathbb{F}_p}$).

We have $\sqrt{dm^*}=\begin{cases}2^{-1} \text{ if } dm\equiv 1(\bmod 4)\\ 0_{\mathbb{F}_p}, \text{ if } dm\equiv -1 \text{ or } 2(\bmod 4)\end{cases}\in\mathbb{F}_p$.

(*Resp. similarly for* $\sqrt{dn^*}$).

We can choose to factorize in $\mathbb{Z}\left[\sqrt{dm^*}\right][X]$:

$f=g_1\times h_1$, *lies modulo p in* $\mathbb{F}_p[X]$, *so we get the following factorization of* $\overline{f_p}$:

For details:

- *In the case*: $dm\equiv dn\equiv 1(\bmod(4))$:

$$\begin{aligned}\overline{f_p}(X)&=\left(\overline{(g_1)_p}(X)\right)\times\left(\overline{(h_1)_p}(X)\right)\\&=\left(X^2-\left(b_{10}+\left(\overline{2}^{-1}\right)b_{11}\right)X+b_{20}+\left(\overline{2}\right)^{-1}b_{21}\right)\\&\quad\times\left(X^2-\left(b_{10}-\left(\overline{2}\right)^{-1}b_{11}\right)X+b_{20}-\left(\overline{2}\right)^{-1}b_{21}\right).\end{aligned}$$

- *And in the case* $dm\equiv dn\equiv -1$ *or* $2(\bmod(4))$ *we get*:

$$\overline{f_p}(X)=\left(\overline{(g_1)_p}(X)\right)\times\left(\overline{(h_1)_p}(X)\right)=\left(X^2-b_{10}X+b_{20}\right)^2.$$

b) *If* $p\nmid m$ *then* $\sqrt{dm}=0_{\mathbb{F}_p}$, *and* $\sqrt{mn}=0_{\mathbb{F}_p}$. *We can choose to factorize in* $\mathbb{Z}\left[\sqrt{dm^*}\right][X]$, *we get for* $\overline{f_p}$ *the same factorization.*

c) *If* $p\nmid n$ *then* $\sqrt{dn}=0_{\mathbb{F}_p}$, *and* $\sqrt{mn}=0_{\mathbb{F}_p}$. *We can choose to factorize in* $\mathbb{Z}\left[\sqrt{dn^*}\right][X]$, *we get for* f_p *a factorization via* $\mathbb{Z}\left[\sqrt{dn^*}\right][X]$:

For details:

In the case: $dm\equiv dn\equiv 1(\bmod(4))$

$$\begin{aligned}\left(\overline{(f_p)}(X)\right)&=\left(\overline{(g_2)_p}(X)\right)\times\left(\overline{(h_2)_p}(X)\right)\\&=\left(X^2-\left(c_{10}+\left(\overline{2}\right)^{-1}c_{11}\right)X+c_{20}+\left(\overline{2}\right)^{-1}c_{21}\right)\\&\quad\times\left(X^2-\left(c_{10}-\left(\overline{2}\right)^{-1}c_{11}\right)X+c_{20}-\left(\overline{2}\right)^{-1}c_{21}\right).\end{aligned}$$

And in the case $dm\equiv dn\equiv -1$ *or* $2(\bmod(4))$ *we get*:

$$\overline{f_p}(X)=\left(\overline{(g_2)_p}(X)\right)\times\left(\overline{(h_2)_p}(X)\right)=\left(X^2-c_{10}X+c_{20}\right)^2.$$

2) *If* $p=2\nmid dmn$, *necessarily* $2\nmid d$ (*cf. Remarks* 2.2. 1)), *then* $\sqrt{dm}=0_{\mathbb{F}_2}$ *and* $\sqrt{dn}=0_{\mathbb{F}_2}\Rightarrow X^2-dm=X^2$ *and* $X^2-dn=X^2$ *and the factorization of f, in* $\mathbb{Z}\left[\sqrt{dm}\right][X]$ *and in* $\mathbb{Z}\left[\sqrt{dn}\right][X]$ *given by*: $f=g_1\times h_1$ *and* $f=g_2\times h_2$ *are in fact modulo* 2 *in* $\mathbb{F}_2[X]$, *so we get two factorisations for* $\overline{f_2}$, *that are* $\overline{f_2}=\overline{(g_1)_2}\times\overline{(h_1)_2}$ *and* $\overline{f_2}=\overline{(g_2)_{p=2}}\times\overline{(h_2)_{p=2}}$.

B) *Let p prime such that* $p\nmid dmn$.

1) *First assume* $p\neq 2$.

Then necessarily exactly one, or all, of the $\left(\frac{dm}{p}\right)$, $\left(\frac{dn}{p}\right)$, $\left(\frac{mn}{p}\right)$ *are equal*

to 1. *Otherwise*: $\left(\frac{d^2m^2n^2}{p}\right)=-1$ *that is absurd.*

Suppose that it is $\left(\frac{dm}{p}\right)=1$ (*The other cases are done equivalently*).

The conditions of the Lemma 2.1. (ii) *are realized, so*:

The factorization: $f=g_1\times h_1$ *in* $\mathbb{Z}\left[\sqrt{dm^*}\right][X]$.

Induces the factorization $\alpha_p(f)=\overline{\alpha_p}(g_1)\times\overline{\alpha_p}(h_1)$, *in* $\mathbb{F}_p\left[\sqrt{dm^*}\right][X]=\mathbb{F}_p[X]$.

But in one hand, the left side gives $\overline{\alpha_p}(f)=\overline{f_p}$, *and in the other hand, the right side give*: $\overline{\alpha_p}(g_1)=\overline{(g_1)_p}$ *and* $\overline{\alpha_p}(h_1)=\overline{(h_1)_p}$, *and the factorization* $\overline{f_p}=\overline{(g_1)_p}\times\overline{(h_1)_p}$ *lies to* $\mathbb{F}_p[X]$, *so f is reducible* $\bmod(p)$ *for any such prime p.*

2) *Assume now* $p=2$ (*recall that* $2\nmid dmn$).

a) *In case* $dm\equiv 3(\bmod 4)$ *then* $X^2-dm=(X+1)^2$ *in* $\mathbb{F}_2[X]$ $\Rightarrow$ $\sqrt{dm^*}=\sqrt{dm}=1\in\mathbb{F}_2$ $\Rightarrow$ $\overline{f_2}$ *is reducible in* $\mathbb{F}_2[X]$, *via the factorization* $f=g_1\times h_1$ *in* $\mathbb{Z}\left[\sqrt{dm}\right][X]$, *which implies*: $\overline{f_2}=\overline{(g_1)_2}\times\overline{(h_1)_2}$.

b) *In case* $dm\equiv 1(\bmod 4)$ *let's note that we get also* $dn\equiv mn\equiv 1(\bmod(4))$.

b_1) *If* $dm\equiv 1(\bmod 8)$ *or* $dn\equiv 1(\bmod 8)$ *or* $mn\equiv 1(\bmod 8)$ *then in* $\mathbb{F}_2[X]$:

$$X^2-X+\frac{1-dm}{4}=X^2-X\Rightarrow\sqrt{dm^*}=\frac{1+\sqrt{dm}}{2}\in\left\{0_{\mathbb{F}_p},1\right\}\subset\mathbb{F}_2,$$

or $\sqrt{dn^*}=\frac{1+\sqrt{dn}}{2}\in\left\{0_{\mathbb{F}_p},1\right\}\subset\mathbb{F}_2$, *or* $\sqrt{mn^*}=\frac{1+\sqrt{mn}}{2}\in\left\{0_{\mathbb{F}_p},1\right\}\subset\mathbb{F}_2$.

So $\overline{f_2}$ *is reducible in* $\mathbb{F}_2[X]$ *via the factorisations*:

$$f=g_1\times h_1 \text{ in } \mathbb{Z}\left[\frac{1+\sqrt{dm}}{2}\right][X];$$

(*or* $f=g_2\times h_2$ *in* $\mathbb{Z}\left[\frac{1+\sqrt{dn}}{2}\right][X]$ *or* $f=g_3\times h_3$ *in* $\mathbb{Z}\left[\frac{1+\sqrt{mn}}{2}\right][X]$).

Equalities that lead to:

$$\overline{f_2}=\overline{(g_1)_2}\times\overline{(h_1)_2};$$

(*Or* $\overline{f_2}=\overline{(g_2)_{p=2}}\times\overline{(h_2)_{p=2}}$; *or* $\overline{f_2}=\overline{(g_3)_2}\times\overline{(h_3)_2}$)

b_2) *Now to close the proof, it remains the case* $dm\equiv dn\equiv mn\equiv 5(\bmod(8))$.

But this case don't exist for biquadratic fields $\mathbb{Q}\left(\sqrt{dm},\sqrt{dn}\right)$, *because*:

$dm\equiv dn\equiv 5(\bmod 8)$ $\Rightarrow$ $dm\times dn\equiv mn\equiv 1(\bmod 8)$ *which is absurd.*

In conclusion, we have prooved that:

Once $\Sigma_f=\mathbb{Q}\left(\sqrt{dm},\sqrt{dn}\right)$, *then* $\overline{f_p}(X)=X^4+\overline{a_3}X^3+\overline{a_2}X^2+\overline{a_1}X+\overline{a_0}$ *is reducible over* $\mathbb{F}_p[X]$, *for any prime p.*

We deduce the following theorem which is the goal of this paper:

3.1. Main Theorem

Theorem 3.1. *Let* $\mathcal{M}=\left\{K=\mathbb{Q}\left(\sqrt{dm},\sqrt{dn}\right)/\exists\theta\in\mathbb{Z}_K \text{ such that } \mathbb{Z}_K=\mathbb{Z}[\theta]\right\}$,

cf. Definition 1.3., *then all the fields of* $\mathcal{M}$, *do not admit any prime number* $p \in \mathbb{Z}$ *which are inert there.*

Proof 3.2. *Let* $K \in \mathcal{M}$, *and* $\theta \in \mathbb{Z}_K$ *such that* $\mathbb{Z}_K = \mathbb{Z}[\theta]$. *Then its irreducible polynomial* $f(X)$ *is such that* $K = \mathbb{Q}(\sqrt{dm}, \sqrt{dn}) = \Sigma_f$, *and that* $\overline{f_p}(X) = X^4 + \overline{a_3}X^3 + \overline{a_2}X^2 + \overline{a_1}X + \overline{a_0}$ *is reducible over* $\mathbb{F}_p[X]$ (*cf. Proposition* 3.1.) *but then for any prime p, we get* (*cf. Proposition* 1.1.):

$p\mathbb{Z}[\theta] = \prod_{i=1}^{g}\left(p\mathbb{Z}[\theta] + f_{i,p}(\theta)\mathbb{Z}[\theta]\right)^e$, *with necessarly* $g \neq 1$, *because* $\overline{f_p}(X) = \overline{f_{1,p}}(X)$ *is impossible otherwise* $\overline{f_p}(X)$ *would be irreducible. So p is inert in K.*

3.2. Application to Cubic Resolvents

From [3] & [5], we deduce this corollary.

Let's put: $r(X) = X^3 - a_2X^2 - (a_3a_1 - 4a_4)X - (a_3^2a_0 - 4a_2a_0 + a_1) \in \mathbb{Z}[X]$, known as a cubic resolvent of $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{Z}[X]$, then:

Corollary 3.1. *Let* $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{Z}[X]$ *be an irreducible polynomial.*

Then there is an implication from proposition (i) *to proposition* (ii):

(i) $r(X) = X^3 - a_2X^2 - (a_3a_1 - 4a_4)X - (a_3^2a_0 - 4a_2a_0 + a_1)$ *admits* 3 *distinct roots in* $\mathbb{Q} \setminus \mathbb{Q}^2$.

(ii) *For every prime number p, each polynomial* $\overline{f_p}(X) = X^4 + \overline{a_3}X^3 + \overline{a_2}X^2 + \overline{a_1}X + \overline{a_0}$, *is reducible in* $\mathbb{F}_p[X]$.

Remarks 3.1. 1) *The proof comes from that* [3] *&* [5]: (i) $\Leftrightarrow$ $\Sigma_f = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ *is a biquadratic field.*

2) *Since there are other resolvents* $R(X)$ *of* $f(X)$, *we can replace, without changing the goal of the corollary, the polynomial* $r(X)$ *by these ones.*

4. Conclusions

The conclusive results of our study raise in a relevant way the question of the existence of algebraic fields without inert prime numbers, in relation to their monogeneity or not.

This encourages the search for other examples of families of such fields, possessing this property. We can think of well-known families in number theory.

Thanks

I thank Prof. F. Pappalardi, from Roma 3 University, for suggesting this topic.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Samuel, P. (1967) Théorie algébrique des nombres. Hermann, Paris.

[2] Gras, M.-N. and Tanoé, F. (1995) Corps biquadratiques monogènes. Manuscripta Mathematica, 86, 63-79. https://doi.org/10.1007/BF02567978

[3] Kappe, L.C. and Warren, B. (1989) An Elementary Test for the Galois Group of a Quartic Polynomial. *The American Mathematical Monthly*, **96**, 133-137. https://doi.org/10.1080/00029890.1989.11972158

[4] Motoda, Y. (1975) On Biquadratic Fields. *Memoirs of the Faculty of Science, Kyushu University. Series A, Mathematics*, **29**, 263-268. https://doi.org/10.2206/kyushumfs.29.263

[5] Nagell, T. (1961) Sur quelques questions dans la théorie des corps biquadratiques. *Arkiv för Matematik*, **4**, 347-362. https://doi.org/10.1007/BF02591510