International J. of Pure & Engg. Mathematics (IJPEM)
ISSN 2348-3881, Vol. 4 No. I (April, 2016), pp. 31-43

UNRAMIFIED EXTENSIONS OVER QUADRATIC FIELDS

AHMED ASIMI
Departement of Mathematics, Faculty of Sciences
University Ibnou Zohr, B. P. 8106 Agadir, Morroco
E-mail: asimiahmed2008@gmail.com, asimiahmed@yahoo.fr

Abstract

Let n be a given integer greater than 3, $P(X) = X^n - aX + b$ a polynomial in $\mathbb{Z}[X]$, where nb and $(n-1)a$ are relatively prime, and d be its discriminant. It was shown by Uchida [8] that the splitting field of $P(X)$ is unramified over $\mathbb{Q}(\sqrt{d})$.
In this paper we show in the situation above that we necessarily have $d \equiv 1 \bmod 4$ for all n and that the converse is not true. In this case we show that there are infinitely many square free integers $d \equiv 1 \bmod 4$ that are not discriminant of polynomials of type $P(X)$. At the same time we get infinite quadratic fields whose class numbers are divisible by a given prime number p (theorem 2.1). And at the end of this paper we construct Hilbert's fields of quadratic fields when $n = 3$. Unramified means that every finite prime is unramified, and Hilbert's field of a field means the maximal unramified abelian extension of this field.

1. Introduction and Notations

Let $\mathbf{K}$ be a number field and $\mathbf{L}$ a subfield of $\mathbf{K}$. Throughout this paper we denote :

$\mathbf{Tr}_{\mathbf{K/L}}$: The trace of $\mathbf{K}$/L.

$\mathbf{N}_{\mathbf{K/L}}$: The norm of $\mathbf{K}$/L.

$h(\mathbf{K})$: the class number of $\mathbf{K}$.

This work is a continuation of a work done by Uchida [8] who determined all splitting fields of $P(X) = X^n - aX + b$, a polynomial in $\mathbb{Z}[X]$ where nb and $(n-1)a$ are relatively prime and d be its discriminant for every number n greater than 3, and it turned out they are unramified over $\mathbb{Q}(\sqrt{d})$.

In this paper we show in the situation above that we necessarily have $d \equiv 1 \bmod 4$ for all n and that the converse is not true. In this case we show that there are infinitely many square free integers $d \equiv 1 \bmod 4$ that are not discriminant of polynomials of type $P(X)$. At the same time we get infinite quadratic fields whose class numbers are divisible by a given prime number p (theorem 2.1). And at the end of this paper we construct Hilbert's fields of quadratic fields when $n = 3$. Unramified means that every finite prime is unramified, and Hilbert's field of a field means the maximal unramified abelian extension of this field.

2. Unramified Extensions Over Quadratic Fields

Proposition 2.1 : Let d be an integer, and assume that there exist $n \geq 2$, a, b in $\mathbb{Z}$ such that $d = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} - (n-1)^{n-1}a^n)$ with nb and $(n-1)a$ relatively prime, we then get :

$$d \equiv \begin{cases} (-1)^{\frac{n(n-1)}{2}}(1-n), & \text{mod } 8 \text{ if } n \text{ is an even number and } n \geq 4. \\ (-1)^{\frac{n(n-1)}{2}}n, & \text{mod } 8 \text{ if } n \text{ is an odd number and } n \geq 4. \\ 5 + 4a^3, & \text{mod } 8 \text{ if } n = 3. \\ -4b + a^2, & \text{mod } 8 \text{ if } n = 2. \end{cases}$$

Proof : If $n = 2$, then $d = -4b + a^2$.

If $n = 3$, then $d = 4a^3 - 27b^2$ with $2a$ and $3b$ relatively prime, therefore $b^2 \equiv 1 \bmod 8$, so $d \equiv 5 + 4a^3 \bmod 8$.

If $n \geq 4$, we then have $n \equiv 1$ or $0 \bmod 2$.

- Assume $n \equiv 1 \bmod 2$, then $n - 1 \equiv 0 \bmod 2$ and $b \equiv 1 \bmod 2$, so $b^{n-1} \equiv 1 \bmod 8$ because $n - 1 \geq 3$, hence $d \equiv (-1)^{\frac{n(n-1)}{2}} n^n \bmod 8$.

  Since $n^n \equiv 1 \bmod 8$ because n and 8 are relatively prime, then $d \equiv (-1)^{\frac{n(n-1)}{2}} n \bmod 8$.

- Assume $n \equiv 0 \bmod 2$, then $a \equiv 1 \bmod 2$, so $a^n \equiv 1 \bmod 8$, $n^n \equiv 0 \bmod 8$ and $(n-1)^{n-1} \equiv n - 1 \bmod 8$ because $n \geq 4$ and $n - 1$ and 8 are relatively prime, therefore $d \equiv (-1)^{\frac{n(n-1)}{2}}(1-n) \bmod 8$.

Corollary 1 : Let d be an integer, and assume that there exist $n \geq 2$, a, b integers such that $d = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} - (n-1)^{n-1}a^n)$ with nb and $(n-1)a$ relatively prime, we then get $d \equiv 1 \bmod 4$.

Proof : If $n = 2$ or $n = 3$, then $d \equiv -4b + a^2 \equiv 1$ or $d \equiv 5 + 4a^3 \equiv 1 \bmod 4$ respectively (Proposition 2.1).

If $n \equiv 0 \bmod 4$ and $n \geq 4$, then $(-1)^{\frac{n(n-1)}{2}} = 1$ and $1 - n \equiv 1 \bmod 4$, therefore $d \equiv 1 \bmod 4$ (Proposition 2.1).

If $n \equiv 2 \bmod 4$ and $n \geq 4$, then $(-1)^{\frac{n(n-1)}{2}} = -1$ and $1 - n \equiv -1 \bmod 4$, therefore $d \equiv 1 \bmod 4$ (Proposition 2.1).

If $n \equiv 1 \bmod 4$ and $n \geq 4$, then $(-1)^{\frac{n(n-1)}{2}} = 1$, therefore $d \equiv 1 \bmod 4$ (Proposition 2.1).

If $n \equiv -1 \bmod 4$ and $n \geq 4$, then $(-1)^{\frac{n(n-1)}{2}} = -1$, therefore $d \equiv 1 \bmod 4$ (Proposition 2.1).

Corollary 2 : Let d be an integer, and assume that there exist $n \geq 3$, a, b in $\mathbb{Z}$ such that $d = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} - (n-1)^{n-1}a^n)$ with nb and $(n-1)a$ relatively prime, we then get :

(1) $d \equiv 1 \bmod 8 \iff$ ($n \equiv \pm 1$ or 0 or $2 \bmod 8$ if $n \geq 4$) or ($a \equiv 1 \bmod 2$ if $n = 3$).

(2) $d \equiv 5 \bmod 8 \iff$ ($n \equiv \pm 5$ or 4 or $6 \bmod 8$ if $n \geq 4$) or ($a \equiv 0 \bmod 2$ if $n = 3$).

Proof : Assume that $n = 3$.

From proposition 2.1, we then deduce :

$$\begin{aligned}
d \equiv 5 \bmod 8 \quad &\iff \quad 4a^3 \equiv 0 \quad \bmod 8 \\
&\iff \quad a^3 \equiv 0 \quad \bmod 2 \\
&\iff \quad a \equiv 0 \quad \bmod 2 \\
d \equiv 1 \bmod 8 \quad &\iff \quad 4a^3 \equiv -4 \quad \bmod 8 \\
&\iff \quad 4a^3 \equiv 4 \quad \bmod 8 \\
&\iff \quad a^3 \equiv 1 \quad \bmod 2 \\
&\iff \quad a \equiv 1 \quad \bmod 2
\end{aligned}$$

Assume that $n \geq 4$ and $d \equiv 1 \bmod 8$, from proposition 2.1, we then deduce :

- If $n \equiv 1 \bmod 4$, then $(-1)^{\frac{n(n-1)}{2}} = 1$, $n \equiv 1$ or $5 \bmod 8$ and $d \equiv n \bmod 8$, therefore $n \equiv 1 \bmod 8$.
- If $n \equiv 3 \bmod 4$, then $(-1)^{\frac{n(n-1)}{2}} = -1$, $n \equiv 3$ or $-1 \bmod 8$ and $d \equiv -n \bmod 8$, therefore $n \equiv -1 \bmod 8$.

- If $n \equiv 0 \bmod 4$, then $(-1)^{\frac{n(n-1)}{2}} = 1$, $n \equiv 0$ or $4 \bmod 8$ and $d \equiv 1 - n \bmod 8$, therefore $n \equiv 0 \bmod 8$.
- If $n \equiv 2 \bmod 4$, then $(-1)^{\frac{n(n-1)}{2}} = -1$, $n \equiv 2$ or $6 \bmod 8$ and $d \equiv n - 1 \bmod 8$, therefore $n \equiv 2 \bmod 8$.

The converse is trivial.
Assume that $n \geq 4$ and $d \equiv 5 \bmod 8$, from Proposition 2.1, we then deduce :

- If $n \equiv 1 \bmod 4$, then $(-1)^{\frac{n(n-1)}{2}} = 1$, $n \equiv 1$ or $5 \bmod 8$ and $d \equiv n \bmod 8$, therefore $n \equiv 5 \bmod 8$.
- If $n \equiv 3 \bmod 4$, then $(-1)^{\frac{n(n-1)}{2}} = -1$, $n \equiv 3$ or $-1 \bmod 8$ and $d \equiv -n \bmod 8$, therefore $n \equiv 3 \bmod 8$.
- If $n \equiv 0 \bmod 4$, then $(-1)^{\frac{n(n-1)}{2}} = 1$, $n \equiv 0$ or $4 \bmod 8$ and $d \equiv 1 - n \bmod 8$, therefore $n \equiv 4 \bmod 8$.
- If $n \equiv 2 \bmod 4$, then $(-1)^{\frac{n(n-1)}{2}} = -1$, $n \equiv 2$ or $6 \bmod 8$ and $d \equiv n - 1 \bmod 8$, therefore $n \equiv 6 \bmod 8$.

The converse is trivial.
If $d \equiv 1 \bmod 4$, then $d = 1 - 4b$ with $b \in \mathbb{Z}$, therefore d is a discriminant of the polynomial $P(X) = X^2 - X + b$, and we have for all integers b, $2b$ and $a = 1$ are relatively prime.
Henceforth we assume that $n \geq 3$. And we wonder : " If for every square free integer $d \equiv 1 \bmod 4$, there exist $n \geq 3$, a and $b \in \mathbb{Z}$ where nb and $(n-1)a$ are relatively prime such that $d = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} - (n-1)^{n-1} a^n)$? "
Lemma 2.1 : Let $P(X) = X^n - aX + b$ be a polynomial in $\mathbb{Z}[X]$, with nb and $(n-1)a$ relatively prime, d an integer such that $\sqrt{d} \notin \mathbb{Z}$, and $\alpha_1, ..., \alpha_n$ the roots of $P(X)$.
If $P(X)$ splits completely in $\mathbb{Q}(\sqrt{d})$, then for every root α_i that doesnot belong to $\mathbb{Q}$, there exists only one $j \in \{1, ..., n\}$ such that $\alpha_i + \alpha_j \in \mathbb{Z}$ and $\alpha_i \alpha_j \in \mathbb{Z}$.
Proof : Since nb and $(n-1)a$ are relatively prime, then $\alpha_i \neq \alpha_j$ for all $i \neq j$. Let σ be the $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{d})$ such that $\sigma(\sqrt{d}) = -\sqrt{d}$, and since $P(X) \in \mathbb{Z}[X]$, then $\sigma(\alpha_i) \in \{\alpha_1, ..., \alpha_n\}$ for all $i \in \{1, ..., n\}$, so there exists only one $j \in \{1, ..., n\}$ such that $\sigma(\alpha_i) = \alpha_j$; therefore $\mathbf{N}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha_i) = \alpha_i \sigma(\alpha_i) = \alpha_i \alpha_j \in \mathbb{Z}$ and $\mathbf{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha_i) = \alpha_i + \sigma(\alpha_i) = \alpha_i + \alpha_j \in \mathbb{Z}$.

Corollary 3 : Let $P(X) = X^n - aX + b$ be a polynomial in $\mathbb{Z}[X]$, with nb and $(n-1)a$ relatively prime and d be an integer.
If n is an odd number and $P(X)$ splits completely in $\mathbb{Q}(\sqrt{d})$, then $P(X)$ has at least one root in $\mathbb{Z}$, dividing b.
Proof : If $\sqrt{d} \in \mathbb{Z}$, the result is trivial.
Assume that $\sqrt{d} \notin \mathbb{Z}$, and since n is an odd number and $P(X)$ has all roots α_1, ..., α_n that are all distinct, then $P(X)$ has an odd number of roots. From Lemma 2.1, we deduce there exits $i \in \{1, ..., n\}$ such that $\sigma(\alpha_i) = \alpha_i$ (with $\sigma(\sqrt{d}) = -\sqrt{d}$), hence $\alpha_i \in \mathbb{Q}$, so $\alpha_i \in \mathbb{Z}$ because α_i is a root of $P(X) \in \mathbb{Z}[X]$.
But $\alpha_i(\alpha_i^{n-1} - a) = b$ and $\alpha_i \in \mathbb{Z}$, then α_i divides b.
Lemma 2.2 : Let d be an integer such that $\sqrt{d} \notin \mathbb{Z}$, and there exit $n \geq 3$, $a, b \in \mathbb{Z}$ such that $d = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} - (n-1)^{n-1}a^n)$ where nb and $(n-1)a$ are relatively prime, and $P(X)$ has all roots α_1, ..., α_n in $\mathbb{Q}(\sqrt{d})$ we then get :

(1) All roots are in $\mathbb{Z}$ except two of them, say α_1, α_2.

(2) $\alpha_1 - \alpha_i \neq c(\alpha_1 - \alpha_j)$ for all $i \neq j$ and $i, j \in \{2, ..., n\}$, and $c \in \mathbb{Q}(\sqrt{d})$.

(3) $\alpha_2 - \alpha_i \neq c(\alpha_2 - \alpha_j)$ for all $i \neq j$ and $i, j \in \{2, ..., n\}$.

(4) $\prod_{3 \leq j}(\alpha_2 - \alpha_j)^2(\alpha_1 - \alpha_j)^2 = 1$.

(5) $\alpha_i - \alpha_j = \pm 1$ for all $2 < i < j$ if $n \geq 4$.

(6) $\alpha_1 - \alpha_2 = \mp\sqrt{d}$.

Proof : Let σ be a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{d})$ such that $\sigma(\sqrt{d}) = -\sqrt{d}$. We assume that $\alpha_i \notin \mathbb{Q}$ for all $i \in \{1, ..., m\}$ (m is an even number : $m = 2m'$) and $\alpha_i \in \mathbb{Q}$ for all $i \in \{m+1, ..., n\}$ with $m \leq n$ and $\{m+1, ..., n\} = \emptyset$ if $m = n$.
From lemma 2.1, we get for all $i \in \{1, ..., m'\}$ $s_i = \alpha_i + \alpha_{i+m'} \in \mathbb{Z}$ and $p_i = \alpha_i\alpha_{i+m'} \in \mathbb{Z}$, then $\alpha_i = \frac{-s_i + \sqrt{s_i^2 - 4p_i}}{2}$ and $\alpha_{i+m'} = \frac{s_i + \sqrt{s_i^2 - 4p_i}}{2}$. But $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\alpha_i) = \mathbb{Q}(\sqrt{s_i^2 - 4p_i})$, then $2\sqrt{s_i^2 - 4p_i} = n_i + m_i\sqrt{d}$ with n_i and $m_i \neq 0$ are two numbers of the same parity, so $4(s_i^2 - 4p_i) = n_i^2 + 2n_i m_i\sqrt{d} + dm_i^2$, hence $n_i m_i = 0$, therefore $n_i = 0$, and $\sqrt{s_i^2 - 4p_i} = m_i'\sqrt{d}$ with $m_i' \in \mathbb{Z}$.
But for all $i \in \{1, ..., m'\}$, we have $\alpha_i - \alpha_{i+m'} = \sqrt{s_i^2 - 4p_i} = m_i'\sqrt{d}$.

Since d is the discriminant of $P(X)$, and let $H=\{(i,i+m'), i=1,...,m'\}$, then from [8] we get :

$$\begin{aligned} d &= \prod_{i<j}(\alpha_i-\alpha_j)^2 \\ &= \prod_{i=1}^{i=m'}(\alpha_i-\alpha_{i+m'})^2 \prod_{\substack{i<j\\(i,j)\notin H}}(\alpha_i-\alpha_j)^2 \\ &= \prod_{i=1}^{i=m'} m_i'^2 d \prod_{\substack{i<j\\(i,j)\notin H}}(\alpha_i-\alpha_j)^2 \\ &= d^{m'} \underbrace{\prod_{i=1}^{i=m'} m_i'^2}_{\in\mathbb{Z}} \underbrace{\prod_{\substack{i<j\\(i,j)\notin H}}(\alpha_i-\alpha_j)^2}_{\in\mathbb{Z}} \end{aligned}$$

then $m'=1$ and $m_1^2=1$, therefore we deduce (1), (4), (5) and (6).

(2) If there exist $c\in\mathbb{Q}(\sqrt{d})$ and $2<i<j$ such that $\alpha_1-\alpha_i=c(\alpha_1-\alpha_j)$ we then get $\alpha_i=\alpha_j$ if $c=1$ otherwise we have $\alpha_1\in\mathbb{Q}$. The proof of (3) is similar to (2).

Proposition 2.2 : Let d be a square free integer such that $h(\mathbb{Q}(\sqrt{d}))=1$, then the equality $d=(-1)^{\frac{n(n-1)}{2}}(n^nb^{n-1}-(n-1)^{n-1}a^n)$ does not hold for every integer $n\geq 5$, a, b in $\mathbb{Z}$ with nb and $(n-1)a$ relatively prime.

Proof : Assume there exist $n\geq 5$, a, b in $\mathbb{Z}$ such that $d=(-1)^{\frac{n(n-1)}{2}}(n^nb^{n-1}-(n-1)^{n-1}a^n)$ with nb and $(n-1)a$ relatively prime, then d is the discriminant of $P(X)=X^n-aX+b$, $d=\prod\limits_{i<j}(\alpha_i-\alpha_j)^2$ where α_i are the roots of $P(X)$ for all $i\in\{1,...,n\}$ and the splitting field $\mathbb{Q}(\alpha_1,...,\alpha_n)$ of a polynomial $P(X)=X^n-aX+b$ is an unramified extension over $\mathbb{Q}(\sqrt{d})$.

Since $h(\mathbb{Q}(\sqrt{d}))=1$, then $\mathbb{Q}(\alpha_1,...,\alpha_n)=\mathbb{Q}(\sqrt{d})$, so $P(X)$ splits completely in $\mathbb{Q}(\sqrt{d})$.

If $n\geq 5$, from Lemma 2.2 we then get (for example) :

$$\begin{cases} \alpha_3-\alpha_4=-1 & (1)\\ \alpha_3-\alpha_5=-1 & (2)\\ \alpha_4-\alpha_5=1 & (3)\end{cases}$$

because $\alpha_i\neq\alpha_j$ and $\alpha_i-\alpha_j=\pm 1$ for all $2<i<j$.

$(1)-(2)\Longleftrightarrow \alpha_4-\alpha_5=2\Longleftrightarrow 2=-1$ which is impossible.

Proposition 2.3 : Let d be the discriminant of the equation $P(X)=X^n-aX+b$ where nb and $(n-1)a$ are relatively prime, we then get :

$\sqrt{d}\in\mathbb{Q}\Longleftrightarrow P(X)$ splits completely in $\mathbb{Q}$.

Proof : Since d is the discriminant of the equation $P(X) = X^n - aX + b$ where nb and $(n-1)a$ are relatively prime, we then get $d = \prod_{i<j}(\alpha_i - \alpha_j)^2$ where α_i are the roots of $P(X)$ for all $i \in \{1, ..., n\}$ and $\mathbb{Q}(\alpha_1, ..., \alpha_n)$ is an unramified extension of $\mathbb{Q}(\sqrt{d})$ [8].
If $\sqrt{d} \in \mathbb{Q}$, then $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$, so $\mathbb{Q}(\alpha_1, ..., \alpha_n) = \mathbb{Q}$, therefore $\alpha_i \in \mathbb{Q}$ for all $i \in \{1, ..., n\}$. The converse is trivial.

Lemma 2.3 : Let d be an integer, $n \geq 3$, and p a prime number.
If p is a common divisor of n and d, then there are no a, b in $\mathbb{Z}$ such that $d = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} - (n-1)^{n-1}a^n)$ where nb and $(n-1)a$ are relatively prime.

Proof : Assume that there exist $n \geq 3$, a, b in $\mathbb{Z}$ such that $d = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} - (n-1)^{n-1}a^n)$ where nb and $(n-1)a$ are relatively prime. Since p divides n and d, then p^n divides n^n, so p divides a^n because p is relatively prime with $n-1$, hence p divides a, this is a contradiction with nb and $(n-1)a$ relatively prime.

Remark 1 : If $d = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} - (n-1)^{n-1}a^n)$ where nb and $(n-1)a$ are relatively prime, then d is relatively prime with n, $n-1$, a and b.

Proposition 2.4 : Let $P(X) = X^n - aX + b \in \mathbb{Z}[X]$ where nb and $(n-1)a$ are relatively prime, d the discriminant of $P(X)$, and α_1,..., α_n the roots of $P(X)$, we then get :

(1) $P(X)$ has at most two roots in $\mathbb{Z}$ dividing b. If $P(X)$ has two roots (for example α_1 and α_2), then $\alpha_1 - \alpha_2 = \pm 1$.

(2) $P(X)$ does not have roots in $\mathbb{Q}(\sqrt{d})$ or it has exactly two roots in $\mathbb{Q}(\sqrt{d}) - \mathbb{Q}$ (for example α_1 and α_2), in this case we then get :

$$\prod_{\substack{i<j \\ (i,j)\neq(1,2)}} (\alpha_i - \alpha_j)^2 = 1.$$

$$\alpha_1 - \alpha_2 = \mp\sqrt{d}.$$

The proof of this proposition relies on Lemma 2.2.

Corollary 4 : Let d be a discriminant of a polynomial $P(X) = X^4 - aX + b$ in $\mathbb{Z}[X]$ where $4b$ and $3a$ are relatively prime, then $P(X)$ does not have roots in $\mathbb{Q}(\sqrt{d})$ or has exactly one root in $\mathbb{Z}$.

Proof : Assume that $P(X)$ has a root in $\mathbb{Q}(\sqrt{d})-\mathbb{Q}$, then $P(X)$ has two roots in $\mathbb{Q}(\sqrt{d})-\mathbb{Q}$ (for example α_1 and α_2) and two roots in $\mathbb{Z}$ dividing b (for example α_3 and α_4) such that $\prod_{3\leq j\leq 4}((\alpha_1-\alpha_j)(\alpha_2-\alpha_j))^2=1$ (Proposition 2.4). But α_1 and α_2 are conjugate, then $\alpha_1-\alpha_j$ and $\alpha_2-\alpha_j$ are conjugate too and are integers in $\mathbb{Q}(\sqrt{d})$, therefore $(\alpha_1-\alpha_j)(\alpha_2-\alpha_j)=\alpha_j^2-(\alpha_1+\alpha_2)\alpha_j+\alpha_1\alpha_2=\pm 1$, hence α_j (for $j=3$ and $j=4$) are solutions of the equation $X^2-(\alpha_1+\alpha_2)X+\alpha_1\alpha_2-(\pm 1)=0$, and since α_1 and α_2 are solutions of the equation $X^2-(\alpha_1+\alpha_2)X+\alpha_1\alpha_2=0$, then $\alpha_1+\alpha_2=\alpha_3+\alpha_4$, $\alpha_1\alpha_2-(\pm 1)=\alpha_3\alpha_4$ and

$$\begin{array}{rcl} P(X) & = & (X^2-(\alpha_1+\alpha_2)X+\alpha_1\alpha_2)(X^2-(\alpha_1+\alpha_2)X+\alpha_1\alpha_2-(\pm 1)) \\ & = & X^4-2(\alpha_1+\alpha_2)X^3+(2\alpha_1\alpha_2-(\pm 1)+(\alpha_1+\alpha_2)^2)X^2 \\ & - & (\alpha_1+\alpha_2)(2\alpha_1\alpha_2-(\pm 1))X+\alpha_1\alpha_2(\alpha_1\alpha_2-(\pm 1)) \end{array}$$

we deduce that :

$$\begin{cases} \alpha_1+\alpha_2=0 & (1) \\ 2\alpha_1\alpha_2-(\pm 1)+(\alpha_1+\alpha_2)^2=0 & (2) \\ \alpha_1+\alpha_2)(2\alpha_1\alpha_2-(\pm 1)=4 & (3) \\ \alpha_1\alpha_2(\alpha_1\alpha_2-(\pm 1))=b & (4) \end{cases}$$

From (1) we have $\alpha_1=-\alpha_2$, we then substitute in (2), we obtain $\alpha_1^2=\pm\frac{1}{2}$, which is in contradiction with α_1 integer in $\mathbb{Q}(\sqrt{d})$. We deduce that $P(X)$ does not have roots in $\mathbb{Q}(\sqrt{d})$.

Since $deg(P)=4$, then by Proposition 2.4, we get $P(X)$ has two roots in $\mathbb{Q}(\sqrt{d})-\mathbb{Q}$ if only if $P(X)$ has two roots in $\mathbb{Z}$.

Proposition 2.5 : Let p be a prime number, n be an integer such that $p\equiv 1 \bmod n-1$ and $P(X)=X^n-aX+b$ a polynomial in $\mathbb{Z}[X]$ where nb and $(n-1)a$ are relatively prime, we then get :

(1) If p divides b and the order of a is $n-1$ modulo p, then $P(X)$ is either irreducible over $\mathbb{Q}$ or has irreducible factors of degree 1 and degree $(n-1)$, in such case it is reducible over $\mathbb{Q}$.

(2) If p is relatively prime with b, $n=p$ and $a\equiv 1 \bmod p$, then $P(X)$ is irreducible over $\mathbb{Q}$.

Proof : (1) If p divides b, we then get :

$$P(X)=X^n-aX+b\equiv X(X^{n-1}-a) \bmod p$$

Recall that $\mathbb{Z}/p\mathbb{Z}$ contains all $(n-1)$-th roots of unity, because p is a prime number such that $n-1$ divides $p-1$. But, $X^{n-1}-a$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$ if and only if

a is a primitive root mod p (Kummer's theorem). In our case we have a relatively prime with p because p divides b, and nb and $(n-1)a$ are relatively prime, hence a is a primitive root mod p, then $X^{n-1} - a$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$. Therefore we get 1).

(2) We assume that p is relatively prime with b and $a \equiv 1 \bmod p$, then $P(X) \equiv X^p - X + b \bmod p$. By Artin Schreier's theorem [5], we deduce that $P(X)$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$ if and only if $P(X)$ does not have roots in $\mathbb{Z}/p\mathbb{Z}$. In our case, it is easy to see that $P(X)$ does not have roots in $\mathbb{Z}/p\mathbb{Z}$, therefore $P(X)$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$, and then over $\mathbb{Q}$.

Proposition 2.6 : Let p be a prime number, d a discriminant of a polynomial $P(X) = X^p - aX + b$ in $\mathbb{Z}[X]$ where pb and $(p-1)a$ are relatively prime, and $h(\mathbb{Q}(\sqrt{d})) = p$. $P(X)$ is reducible over $\mathbb{Q}(\sqrt{d})$ if only if $P(X)$ splits completely in $\mathbb{Q}(\sqrt{d})$.

Proof : $\Longleftarrow$) Is trivial.

$\Longrightarrow$) Let α_1,..., α_p be the roots of $P(X) = X^p - aX + b$. Assume that there exists $i \in \{1, ..., p\}$ such that $\alpha_i \notin \mathbb{Q}(\sqrt{d})$. Since $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\sqrt{d}, \alpha_i) \subset \mathbb{Q}(\alpha_1, ..., \alpha_p)$, $\mathbb{Q}(\alpha_1, ..., \alpha_p)$ is an unramified extension over $\mathbb{Q}(\sqrt{d})$, and $[\mathbb{Q}(\sqrt{d}, \alpha_i) : \mathbb{Q}(\sqrt{d})] > 1$ divides p, then $[\mathbb{Q}(\sqrt{d}, \alpha_i) : \mathbb{Q}(\sqrt{d})] = p$, so $P(X)$ is a minimal polynomial of α_i over $\mathbb{Q}(\sqrt{d})$, therefore $P(X)$ is irreducible over $\mathbb{Q}(\sqrt{d})$.

Corollary 5 : Let p be a prime number, d a discriminant of a polynomial $P(X) = X^p - aX + b$ in $\mathbb{Z}[X]$ where pb and $(p-1)a$ are relatively prime, and $h(\mathbb{Q}(\sqrt{d})) = p$, then $P(X)$ is irreducible over $\mathbb{Q}$ or $P(X)$ splits completely in $\mathbb{Q}(\sqrt{d})$.

Corollary 6: Let d be a discriminant of a polynomial $P(X) = X^n - aX + b$ in $\mathbb{Z}[X]$ where nb and $(n-1)a$ are relatively prime, we then get :

If $n \geq 4$ then $h(\mathbb{Q}(\sqrt{d})) \geq 2$.

The proof of this corollary relies on Proposition 2.4 and Corollary 4.

Proposition 2.7 : Let $P(X) = X^3 - aX + b$ be a polynomial in $\mathbb{Z}[X]$ where $3b$ and $2a$ are relatively prime, and d be its discriminant, we then get :

If $P(X)$ has a root t in $\mathbb{Z}$, then

$$\begin{cases} 9t^2 - d & = & \pm 4 \\ t(a - t^2) & = & b \\ -3t^2 + 4a & = & d \end{cases}$$

Proof : If $P(X)$ has a root t in $\mathbb{Z}$, we then deduce from proposition 2.4 and 2.5 that

$P(X)$ has two roots α_1 and α_2 in $\mathbb{Q}(\sqrt{d})-\mathbb{Q}$ such that

$$\begin{cases} \alpha_1-\alpha_2=\pm\sqrt{d} \\ (t-\alpha_1)(t-\alpha_2)=\pm 1 \\ P(X)=(X-t)(X^2+tX+t^2-a) \\ -3t^3+4a=d \\ t(a-t^2)=b \end{cases}$$

Therefore α_1 and α_2 are roots of the equation $X^2+tX+t^2-a=0$, so $\alpha_1=\frac{-t+\sqrt{d}}{2}$ and $\alpha_2=\frac{-t-\sqrt{d}}{2}$, hence

$$\begin{array}{rcl} (t-\alpha_1)(t-\alpha_2)=\pm 1 & \Longleftrightarrow & \frac{3t-\sqrt{d}}{2}\frac{3t+\sqrt{d}}{2}=\pm 1 \\ & \Longleftrightarrow & 9t^2-d=\pm 4 \end{array}$$

We then deduce that

$$\begin{cases} 9t^2-d & = & \pm 4 \\ t(a-t^2) & = & b \\ -3t^2+4a & = & d \end{cases}$$

Corollary 7 : Let $P(X)=X^3-aX+b$ be a polynomial in $\mathbb{Z}[X]$ where $3b$ and $2a$ are relatively prime, and d be its discriminant, we then get :
If $h(\mathbb{Q}(\sqrt{d}))=1$, then $d\equiv 5 \bmod 8$ and is a prime number.
Proof : Assume that $h(\mathbb{Q}(\sqrt{d}))=1$. Since d is the discriminant of the polynomial $P(X)=X^3-aX+b\in\mathbb{Z}[X]$ where $3b$ and $2a$ are relatively prime, then $P(X)$ splits completely in $\mathbb{Q}(\sqrt{d})$. From Proposition 2.4 and 2.6, there exists an odd number t such that $9t^2-d=\pm 4$. As t is an odd number, then $t^2\equiv 1 \bmod 8$. By the formula $9t^2-d=\pm 4$ we deduce $d\equiv 1-(\pm 4)\equiv 5 \bmod 8$.
If d is not a prime number, then by [3], we get $h(\mathbb{Q}(\sqrt{d}))>1$.
Corollary 8 : Let $d\equiv 1 \bmod 4$ be a square free integer for which there exist a and b in $\mathbb{Z}$ such that $d=4a^3-27b^2$ where $3b$ and $2a$ are relatively prime.
If $h(\mathbb{Q}(\sqrt{d}))=1$ then $d=5$ or there exists an odd number t such that

$$\begin{cases} 9t^2+4 & = & d \\ t(a-t^2) & = & b \\ -3t^2+4a & = & d \end{cases}$$

Proof : Let $d\equiv 1 \bmod 4$ be a square free integer such that $h(\mathbb{Q}(\sqrt{d}))=1$. We assume that there exist a and b in $\mathbb{Z}$ such that $d=4a^3-27b^2$ where $3b$ and $2a$ are relatively prime. We refer to Proposition 2.6 and Corollary 7, we then get :

d is a prime number and there exists an odd number t such that

$$\begin{cases} 9t^2 + (\pm 4) & = & \pm d \\ t(a - t^2) & = & b \\ -3t^2 + 4a & = & d \end{cases}$$

But we have :

$$\begin{cases} 9t^2 - 4 = d & \Longleftrightarrow & (3t-2)(3t+2) = d \\ & \Longleftrightarrow & (3t - 2 = 1 \text{ and } 3t + 2 = d) \text{ or } (3t - 2 = -d \text{ and } 3t + 2 = -1) \\ & \Longleftrightarrow & d = 5 \end{cases}$$

Remark 2 : The converse of Corollary 8 is not in general true : There exist a square free integer d, a and b in $\mathbb{Z}$ such that $d = 4a^3 - 27b^2$ where $3b$ and $2a$ are relatively prime, and an odd number t such that

$$\begin{cases} 9t^2 + 4 & = & d \\ t(a - t^2) & = & b \\ -3t^2 + 4a & = & d \end{cases}$$

But $h(\mathbb{Q}(\sqrt{d})) > 1$.

Example 1 : We refer to [4] and we use the Maple's software, to deduce the following examples :

$a = 76, b = 255, t = 5, d = 229, P(X) = (X-5)(X^2 + 5X - 51), h(\mathbb{Q}(\sqrt{229})) = 3$

$a = 244, b = 1467, t = 9, d = 733, P(X) = (X-9)(X^2 + 9X - 163), h(\mathbb{Q}(\sqrt{229})) = 3$

$a = 364, b = 2673, t = 11, d = 1093, P(X) = (X-11)(X^2 + 11X - 243),$

$h(\mathbb{Q}(\sqrt{229})) = 5$

Corollary 9 : For all non prime square free integers $d \equiv 1 \bmod 8$ or $d \equiv 5 \bmod 8$ such that $h(\mathbb{Q}(\sqrt{d})) = 1$, the equality $d = (-1)^{\frac{n(n-1)}{n}}(n^n b^{n-1} - (n-1)^{n-1} a^n)$ does not hold for $n \geq 3$, a and b in $\mathbb{Z}$ where nb and $(n-1)a$ are relatively prime.

The proof of this corollary relies on Corollary 7.

Theorem 2.1 : Let p be a prime number, then there exist infinitely many quadratic fields $\mathbb{Q}(\sqrt{d})$ with class number divisible by p, where $d = (-1)^{\frac{p(p-1)}{2}}(p^p - (p-1)^{(p-1)} a^p)$ and p is relatively prime with a if $p \neq 2$.

Proof : If $p = 2$, we consider the quadratic field $\mathbb{Q}(\sqrt{qq'})$ where q and q' are two distinct prime numbers such that $q \equiv q' \equiv 1 \bmod 4$. It is easy to see that $\mathbb{Q}(\sqrt{q}, \sqrt{q'})$ is an unramified extension over $\mathbb{Q}(\sqrt{qq'})$, therefore there exist infinitely many quadratic fields with class number divisible by 2.

If $p>2$, we consider $P(X)=X^p-aX+1\in\mathbb{Z}[X]$ with $a\equiv 1 \bmod p$, then $(p-1)a$ and p are relatively prime, and $P(X)=X^p-X+1$ in $\mathbb{Z}/p\mathbb{Z}[X]$. By Artin Schreier's theorem, we deduce that $P(X)$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$ if and only if $P(X)$ does not have roots in $\mathbb{Z}/p\mathbb{Z}$. In our case, it is easy to see that $P(X)$ does not have roots in $\mathbb{Z}/p\mathbb{Z}$, therefor p is unramified in the splitting field denoted $\mathbf{K}$ of a polynomial $P(X)$ and divides the residue class degree of p in $\mathbf{K}/\mathbb{Q}$. Since p is an odd number, $\mathbb{Q}(\sqrt{d})\subset\mathbf{K}$ where d is the discriminant of $P(X)$ and $\mathbf{K}$ is an unramified extension over $\mathbb{Q}(\sqrt{d})$ [8], therefore p divides the class number of $\mathbb{Q}(\sqrt{d})$.

It seems that there exist infinitely many numbers $a\equiv 1 \bmod p$ such that p divides the class number of $\mathbb{Q}(\sqrt{d})$ with d is a discriminant of $P(X)=X^p-aX+1$. Let a_0 be one of such numbers, and d_0 be a discriminant of $P(X)=X^p-a_0X+1$. We claim that there are only finite numbers of a's with $\mathbb{Q}(\sqrt{d})=\mathbb{Q}(\sqrt{d_0})$. Indeed, since $\mathbb{Q}(\sqrt{d})=\mathbb{Q}(\sqrt{d_0})$, then there exist an integer m such that $d=m^2d_0$, hence $m^2(p^p-(p-1)^{p-1}a_0^p)=p^p-(p-1)^{p-1}a^p$, therefore the pair (m,a) is an integral solution of the Diophantine equation

$$(p^p-(p-1)^{p-1}a_0^p)Y^2=-(p-1)^{p-1}X^p+p^p. \tag{1}$$

Since there exist only a finite number of integral solutions of (1) by Siegel's theorem, therefore there exist infinitely many quadratic fields with class number divisible by p.

In the two cases we have shown that for every prime number p there exist infinitely many quadratic fields with class number divisible by p.

Remark 3 : Theorem 2.1 is considered as a sort of generalization of Honda [2], where the case $p=3$ is treated.

Theorem 2.2 : Let n be a given a number greater than 2, then there exist infinitely many quadratic fields with class number divisible by n.

Proof : If $n=2$, Theorem 2.1.

If $n>2$, we refer to Dirichlet's theorem [9], we deduce that there exists a prime number p such that $p\equiv 1 \bmod 2n$. We consider $P(X)=X^p-aX+b\in\mathbb{Z}[X]$ with p divides b, $(p-1)a$ and pb are relatively prime, d its discriminant and the order of a is equal to $p-1$. From Proposition 2.5 we get $P(X)=X(X^{p-1}-a)$ in $\mathbb{Z}/p\mathbb{Z}[X]$, $X^{p-1}-a$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$, therefore p is unramified in the splitting field denoted $\mathbf{K}$ of a polynomial $P(X)$ and $p-1$ divides the residue class degree of p in $\mathbf{K}/\mathbb{Q}$. Since $2n$ divides $p-1$, hence $2n$ divides the residue class degree of p in $\mathbf{K}/\mathbb{Q}$. But we have

$\mathbb{Q}(\sqrt{d}) \subset \mathbf{K}$ where d is the discriminant of $P(X)$, $\mathbf{K}$ is an unramified extension over $\mathbb{Q}(\sqrt{d})$ [8] and $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] = 2$, then n divides the class number of $\mathbb{Q}(\sqrt{d})$.
The proof of the infiniteness of the number of quadratic number fields for every natural number n is similar Theorem 2.1.

3. Construction of Hilbert's Fields of Quadratic Fields

Let $P(X) = X^n - aX + b$ be a polynomial over $\mathbb{Z}$ such that nb and $(n-1)a$ are relatively prime, d be its discriminant, $h(\mathbb{Q}(\sqrt{d})) = h$ be the class number of $\mathbb{Q}(\sqrt{d})$ and $\mathbf{H}$ be the Hilbert's field of a quadratic field $\mathbf{k} = \mathbb{Q}(\sqrt{d})$.
We refer to [4] and we use the Maple's software, to get the following examples for $n = 3$ and for small integers a and b :

$$a = 1, b = 1, d = -23, h = 3, P(X) = X^3 - X + 1,\ \mathbf{H} = \mathbf{k}\left(\sqrt[3]{108 + 12\sqrt{69}})\right)$$
$$a = 4, b = 1, d = 229, h = 3, P(X) = X^3 - 4X + 1,\ \mathbf{H} = \mathbf{k}\left(\sqrt[3]{-108 + 12\sqrt{-687}}\right)$$
$$a = 5, b = 1, d = 473, h = 3, P(X) = X^3 - 5X + 1,\ \mathbf{H} = \mathbf{k}\left(\sqrt[3]{-108 + 12\sqrt{-1419}}\right)$$
$$a = 2, b = 3, d = -211, h = 3, P(X) = X^3 - 2X + 3,\ \mathbf{H} = \mathbf{k}\left(\sqrt[3]{324 + 12\sqrt{633}}\right)$$
$$a = 5, b = 3, d = 257, h = 3, P(X) = X^3 - 8X + 9,\ \mathbf{H} = \mathbf{k}\left(\sqrt[3]{324 + 12\sqrt{417}}\right)$$
$$a = 8, b = 9, d = -139, h = 3, P(X) = X^3 - 7X + 3,\ \mathbf{H} = \mathbf{k}\left(\sqrt[3]{972 + 12\sqrt{417}}\right).$$

References

[1] Cassels J. W.S. and Fröhlich A., Algebraic Number Theory, Academic Press, (1967).

[2] Honda T., On real quadratic fields whose class numbers are multiples of 3, J, Reine Angew. Math. 233 (1968), 101-102.

[3] Kaplan P., Sur le 2-groupe des classes d'idéaux des corps quadratiques, J, Reine Angew. Math., 283/284 (1976), 313-363.

[4] Oriat B., Table des groupes des classes des corps quadratiques réels $\mathbb{Q}(\sqrt{d})$ et imaginaires $\mathbb{Q}(\sqrt{-d})$, $d < 10000$, Faculté des Sciences de Besançon, (1974-1975).

[5] Ribenboim P.,, L'Arithmétique des corps, Hermann, Paris, (1972).

[6] Samuel P., Théorie algébrique des nombres, Hermann, Paris, (1971).

[7] Siegel C. L., Über einige anvendungen diophantisher aproximationen, Gesammelte abhandlungen band I, 209-266.

[8] Uchida, Unramified extensions of quadratic number fields, I, Tôhoku Math. J., 22 (1970).

[9] Washington L. C., Introduction to Cyclotomic Fields, Graduate Texts in Mathematics, 83 (1982), Springer-Verlag, New York.