An elementary computation of the Galois groups of symmetric sextic trinomials

ALBERTO CAVALLO

Max Planck Institute for Mathematics,
Bonn 53111, Germany
cavallo@mpim-bonn.mpg.de

Abstract

We compute the Galois group of the splitting field $F$ of any irreducible and separable polynomial $f(x) = x^6 + ax^3 + b$ with $a, b \in K$, a field with characteristic different from two. The proofs require to distinguish between two cases: whether or not the cubic roots of unity belong to $K$.

We also give a criterion to determine whether a polynomial as $f(x)$ is irreducible, when $F$ is a finite field. Moreover, at the end of the paper we also give a complete list of all the possible subfields of $F$.

1 Introduction

The computation of the Galois group of the splitting field of polynomials as $x^4 + cx^2 + d$ is a standard exercise in Galois theory, see [3]. On the other hand, the solution of the similar problem for sextic trinomials $f(x) = x^6 + ax^3 + b$, although it may be known to experts ([2, 4, 5, 7, 8, 9, 10]), cannot be found easily in literature; specially in the general case when the coefficients of $f(x)$ are taken in a generic field $K$. This was our main motivation for writing this paper.

Here, we determine the Galois group of $F$, the splitting field of $f(x)$, whenever $f(x) \in K[x]$ is irreducible and separable over $K$, where $K$ is every possible field with characteristic different from two. More specifically, we prove the following theorem. Note that when we write that the element $\sqrt[3]{b}$ is not in the field $K$ we mean that none of the three cubic roots of $b$ belongs to $K$.

Theorem 1.1. Suppose that $f(x) = x^6 + ax^3 + b$ is an irreducible and separable polynomial over the field $K$, where $\text{char}(K) \neq 2$; moreover, consider $\Delta = a^2 - 4b$ and denote with $F$ the splitting field of $f(x)$. Then we have that

1. when $\zeta_3 \notin K$, where $\zeta_3$ is a primitive cubic root of unity, and $-3\Delta$ is not a square in $K$:
   - if $\sqrt[3]{b} \in K$ or $R(x) = x^3 - 3bx + ab$ is reducible over $K$ then $\text{Gal}(\overline{F}/K) \cong D_6$, the Dihedral group of order 12;
   - if $\sqrt[3]{b} \notin K$ and $R(x)$ is irreducible over $K$ then $\text{Gal}(\overline{F}/K) \cong S_3 \times S_3$, the direct product of two symmetric groups over 3 nodes.

2. When $\zeta_3 \notin K$ and $-3\Delta$ is a square in $K$:
   - if $\sqrt[3]{b} \in K$ and $R(x)$ is irreducible over $K$ then $\text{Gal}(\overline{F}/K) \cong C_6$, the cyclic group of order 6;
• if $\sqrt[3]{b} \notin \mathbb{K}$ and $R(x)$ is reducible over $\mathbb{K}$ then $\text{Gal} \left( \mathbb{F} : \mathbb{K} \right) \cong S_3$;
• if $\sqrt[3]{b} \notin \mathbb{K}$ and $R(x)$ is irreducible over $\mathbb{K}$ then $\text{Gal} \left( \mathbb{F} : \mathbb{K} \right) \cong C_3 \times S_3$.

3. When $\zeta_3 \in \mathbb{K}$:
• if $\sqrt[3]{b} \in \mathbb{K}$ and $R(x)$ is irreducible over $\mathbb{K}$ then $\text{Gal} \left( \mathbb{F} : \mathbb{K} \right) \cong S_3$;
• if $\sqrt[3]{b} \notin \mathbb{K}$ and $R(x)$ is reducible over $\mathbb{K}$ then $\text{Gal} \left( \mathbb{F} : \mathbb{K} \right) \cong C_6$;
• if $\sqrt[3]{b} \notin \mathbb{K}$ and $R(x)$ is irreducible over $\mathbb{K}$ then $\text{Gal} \left( \mathbb{F} : \mathbb{K} \right) \cong C_3 \times S_3$.

These are all the possible cases.

Such computations agree with the ones of Harrington and Jones in [6] in the case $\mathbb{K} = \mathbb{Q}$ and $b$ is a cube in $\mathbb{Q}$.

We present an infinite family of polynomials whose Galois group is $G$ for every $G$ appearing in Theorem 1.1 Using Galois correspondence, we are also able to explicitly determine all the possible extensions of $\mathbb{K}$ which are subfields of $\mathbb{F}$. Furthermore, we apply the results in Theorem 1.1 to finite fields; we obtain necessary and sufficient conditions for a polynomial $f(x)$ of the given form to be irreducible.

**Theorem 1.2.** Suppose that $f(x) = x^6 + ax^3 + b \in \mathbb{F}_{p^k}[x], \text{ where } p \neq 2$. Then we have that

1. when $p^k \not\equiv 1 \mod 3$ and $p \neq 3$ the polynomial $f(x)$ is irreducible if and only if $R(x) = x^3 - 3bx + ab$ is irreducible over $\mathbb{F}_{p^k}$;
2. when $p^k \equiv 1 \mod 3$ the polynomial $f(x)$ is irreducible if and only if $\sqrt[3]{b}, \sqrt{\Delta} \notin \mathbb{F}_{p^k}$;
3. when $p = 3$ the polynomial $f(x)$ is never irreducible.

We apply this result to prove that some polynomials are irreducible over the rational numbers, see Corollaries 3.5 and 3.9.

The paper is organized as follows. In Section 2 we set the notation and we prove some preliminary results. Moreover, we determine what are the possible degrees $[\mathbb{F} : \mathbb{K}]$ for the splitting field of $f(x)$ over $\mathbb{K}$. In Section 3 we prove Theorem 1.1 and finally, in Section 4 we list all the intermediate extensions between $\mathbb{F}$ and $\mathbb{K}$.

**Acknowledgements** The author has a post-doctoral fellowship at the Max Planck Institute for Mathematics in Bonn.

## 2 Preliminaries

Let us consider our polynomial $f(x) = x^6 + ax^3 + b$ over the field $\mathbb{K}$. We suppose that $f(x)$ is irreducible, and also separable if $\text{char}(\mathbb{K}) = 3$, and the characteristic of $\mathbb{K}$ is not two. We also take $\Delta = a^2 - 4b$.

Since one has

$$x^3 = \frac{-a \pm \sqrt{\Delta}}{2},$$
the six roots of \( f(x) \) in the algebraic closure of \( K \), when \( \text{char}(K) \) is different from three, are \( \{ \alpha, \alpha \zeta_3, \alpha \zeta_3^2, \beta, \beta \zeta_3, \beta \zeta_3^2 \} \), where \( \zeta_3 \) is a primitive cubic root of unity; moreover, we have that

\[
\alpha = \sqrt[3]{\frac{-a + \sqrt{\Delta}}{2}} \quad \text{and} \quad \beta = \sqrt[3]{\frac{-a - \sqrt{\Delta}}{2}}.
\]

Otherwise, in the case of \( \text{char}(K) = 3 \) the roots are just \( \{ \alpha, \beta \} \), each one with multiplicity three. This is because in this kind of fields \( \zeta_3 \) does not exist and the only cubic root of unity is \( 1 \).

We observe that \( \alpha \beta = \sqrt[3]{b} \). Since once we fix \( \alpha \) there are three choices for \( \beta \), we have that \( \sqrt[3]{b} \) also depends on this selection. Although, when \( K = \mathbb{Q} \), it may seems more natural to take \( \alpha \) and \( \beta \) in the way that \( \sqrt[3]{b} \) is always real, in this paper we need to not make this assumption.

Furthermore, after an easy computation we note that

\[
\alpha^3 + \beta^3 = -a \quad \text{and} \quad \alpha^3 \beta^3 = b.
\]

**Lemma 2.1.** We have that \( \alpha \neq \beta \), where here we mean that none of the three values of \( \beta \) coincides with \( \alpha \).

**Proof.** Suppose for now that \( \text{char}(K) \neq 3 \) and assume that \( \alpha = \beta \). Since there is a double root one has

\[
\text{disc}(f(x)) = 729b^2 \Delta^3 = 0
\]

and this implies that \( \Delta \) or \( b \) is also zero. In both cases \( f(x) \) would be reducible.

Now we consider a field \( K \) with characteristic three. In this case \( \text{disc}(f(x)) \) is always zero, but from the equations we wrote before we obtain

\[
(2\alpha)^3 = (\alpha + \alpha)^3 = 2\alpha^3 = 2a,
\]

which means that

\[
\alpha^3 = a \quad \text{and} \quad \alpha^6 = b = a^2.
\]

Hence, in conclusion \( f(x) = x^6 - 2ax^3 + a^2 = (x^3 - a)^2 \) and this is a contradiction because \( f(x) \) is irreducible.

The splitting field of \( f(x) \) is clearly \( F = K(\zeta_3, \sqrt[3]{b}) = K(\zeta_3, \alpha, \sqrt[3]{b}) \). Denote with \( L \) the subfield \( K(\zeta_3, \sqrt[3]{b}) \cap K(\alpha) \); we obtain the diagram of extensions in Figure 1. In the diagrams on the right we have that \( [K(\sqrt[3]{b}) : K] = 1,3 \) because, up to the choice of \( \alpha \) and \( \beta \), we can assume either \( \sqrt[3]{b} \in K \) or none of the three possible cubic roots of \( b \) belongs to \( K \). We can detect whether \( \zeta_3 \) belongs to \( K(\alpha) \) by using the following criterion.

**Lemma 2.2.** Suppose that \( K \) is a field with \( \text{char}(K) \neq 2,3 \) and \( \zeta_3 \notin K \). We have \( K(\zeta_3) \subset K(\alpha) \) if and only if \( \Delta = -3n^2 \), where \( n \in K \).
First we note that \( \text{Proof.} \) Suppose that \( \text{Lemma 2.3.} \)

\( K \) other transitive subgroup of \( K \) order twelve are \( D_{18} \) is faithful \([1]\). This group has a unique subgroup of order \( K \) subfield \( K \) 4 extension of \( K \) or the only if implication suppose that \( \Delta \neq -3n^2 \). Then \( K(\sqrt{\Delta}, i\sqrt{3}) \subset K(\alpha) \) should be a degree 4 extension of \( K \), but obviously 4 is not a divisor of 6.

When \( K(\zeta_3) \subset K(\alpha) \) the diagram on the right in Figure 1 tells us that \([F : K]\) is 6 or 18. Since the only transitive subgroup of \( S_6 \) of order 18 is \( C_3 \times S_3 \) \([1]\), we obtain that \( \text{Gal} \left( \frac{F}{K(\zeta_3, \sqrt{6})} \right) \) can be isomorphic to \( S_3, C_6 \) or \( C_3 \times S_4 \); we recall that \( C_n \) denotes the cyclic group of order \( n \).

On the other hand, if \( \zeta_3 \) is not in \( K(\alpha) \) then, since \( K(\zeta_3) \) is the only quadratic extension in \( K(\zeta_3, \sqrt{6}) \), we have that \([L : K]\) is equal to 1 or 3. Hence, the diagram on the left in Figure 1 implies \([F : K]\) is 12, 36.

Now if the degree of \( F \) is 12 then \( \text{Gal} \left( \frac{F}{K(\zeta_3)} \right) \cong D_6 \). In fact, the only transitive subgroups of \( S_6 \) of order twelve are \( D_6 \) and \( A_4 \), see \([1]\); the latter group does not have subgroups of order six and, under the Galois correspondence, this results in \( F \) not having a subfield of degree 2. This is not the case since \( K(\zeta_3) \subset F \).

**Lemma 2.3.** Suppose that \([F : K] = 36\) where the fields \( F \) and \( K \) are as before. Then we have that \( \text{Gal} \left( \frac{F}{K(\zeta_3)} \right) \cong S_3 \times S_3 \).

**Proof.** First we note that \( F \) has \( K(\zeta_3) \) and \( K(\sqrt{\Delta}) \) as distinct normal extension of degree 2 because \( K(\zeta_3) \not\subset K(\alpha) \), see Figure 1. We can already conclude that \( \text{Gal} \left( \frac{F}{K(\zeta_3)} \right) \cong S_3 \times S_3 \); in fact, the only other transitive subgroup of \( S_6 \) of order 36, up to isomorphism, is \((C_3 \times C_3) \rtimes_{\phi} C_4\), where the action \( \phi \) is faithful \([1]\). This group has a unique subgroup of order 18, while by Galois correspondence it should have at least two of them.

Note that \([F : K] = 36\) implies \( K(\sqrt{6}) \not\subset K(\alpha) \), which also means that \( K(\alpha) \neq K(\beta) \). Therefore, the subfield \( K(\alpha) \) is not a normal extension of \( K \) and then the isomorphism between \( \text{Gal} \left( \frac{F}{K(\alpha)} \right) \) and \( S_3 \times S_3 \) is not given by the diagram on the left in Figure 1 in the sense that the subfield that corresponds to \( \{0\} \times S_3 \) is not \( K(\alpha) \).
We conclude this section with the following useful lemma. As remarked before, we say that \( \sqrt{b} \) belongs to the field \( K \) if at least one of the three cubic roots of \( b \) is in \( K \).

**Lemma 2.4.** Consider \( f(x) = x^6 + ax^3 + b \) irreducible over a field \( K \) with \( \text{char}(K) \neq 2 \). Then we cannot have both \( \sqrt{b} \in K \) and \( R(x) = x^3 - 3bx + ab \) reducible over \( K \).

**Proof.** We can easily check that the three roots of \( R(x) \), in the algebraic closure of \( K \), are \( \{\alpha \beta(\alpha + \beta), \alpha \beta(\alpha \zeta_3 + \beta \zeta_3^2), \alpha \beta(\alpha \zeta_3^2 + \beta \zeta_3)\} \). Note that these roots are all distinct if \( \text{char}(K) \neq 3 \).

We can choose \( \alpha \) and \( \beta \) in the way that \( \alpha \beta(\alpha + \beta) \in K \) and there is an \( i \) such that \( \sqrt{b} = \alpha \beta \zeta_3^i \in K \). This tells us that \( \alpha \) is the root of a degree two polynomial over \( K(\zeta_3) \).

Since \( [K(\zeta_3) : K] \leq 2 \) we have that \( [K(\alpha) : K] \leq 4 \), but this is a contradiction because \( \alpha \) is the root of an irreducible polynomial of degree six over \( K \). \( \Box \)

### 3 The Galois groups

#### 3.1 Proof of Theorem 1.1: cubic roots of unity not in \( K \)

We recall that \( \text{char}(K) \) still cannot be equal to 2; and it is necessarily different from 3. Suppose for now that \( \Delta \neq -3n^2 \) for every \( n \in K \), which means that \( K(\zeta_3) \subset K(\alpha) \) from Lemma 2.2.

**Proposition 3.1.** If \( \sqrt[b]{b} \in K \) and \( \Delta \neq -3n^2 \) then \( \text{Gal}(\overline{F}/K) \cong D_6 \).

**Proof.** We have already seen in the previous section that, in this case, the order of the Galois group can be 12 or 36; depending on the degree of \( L = \{K(\zeta_3, \sqrt[b]{b}) \cap K(\alpha) : K\} \). Hence, since \( \sqrt[b]{b} \in K \) we have that \( [L : K] = 1 \) and this implies the thesis; in fact, we saw that \( D_6 \) is the only option when \( \{F : K\} = 12 \). \( \Box \)

From now on, we also suppose that \( \sqrt[b]{b} \notin K \). Moreover, we say that \( \text{Gal}(\overline{F}/K) \cong D_6 \) and study what happens to the coefficients \( a \) and \( b \).

First, we use Lemma 2.1 to ensure that \( \alpha \neq \beta \). Since \( [F : K] = 12 \) there is a cubic subfield of \( K(\zeta_3, \sqrt[b]{b}) \) inside \( K(\alpha) \). We take \( \beta \) such that
\[
\sqrt[b]{b} = \alpha \beta \in K(\alpha) = K(\beta).
\]

We can describe all twelve automorphisms in the Galois group. The set
\[
\mathcal{B} = \left\{ \alpha^i \zeta_3^j \mid i = 0, \ldots, 5; \ j = 1, 2 \right\}
\]
is a basis of \( F \) as a \( K \)-vector space. Then \( F \in \text{Gal}(\overline{F}/K) \) is determined by:
\[
F(\alpha) = \alpha \zeta_3^i \text{ or } \beta \zeta_3^j \quad i = 0, 1, 2; \ k = 0, 1, 2;
F(\zeta_3) = \zeta_3^j \quad j = 1, 2.
\]

These are all the possibilities, because \( \alpha \) is a root of \( f(x) \) and then \( F(\alpha) \) needs to be a root too; moreover, clearly a primitive root of unity will be send to another primitive root of the same order. We need to compute \( F(\beta) \) and \( F(\sqrt[b]{b}) \) for every \( F \) in the Galois group.

We denote the automorphisms with the following notation: we call \( F_{(i,j)} \) the map that sends \( \zeta_3 \) to \( \zeta_3^j \) for \( j = 1, 2, \alpha \) to \( \alpha \zeta_3^i \) for \( i = 0, 1, 2 \) and \( \alpha \) to \( \beta \zeta_3^3 \) for \( i = 3, 4, 5 \).

The map \( F_{(0,1)} \) is the Identity and then this case is easy. The subfield \( K(\zeta_3) \) is a normal quadratic extension of \( K \). Therefore, it is fixed by the characteristic subgroup of order six of \( D_6 \). This is because \( K(\zeta_3) \subset K(\zeta_3, \sqrt[b]{b}) \), which is a normal extension of \( K \) of degree six, and there is only one subgroup of \( D_6 \) of order six containing a normal subgroup of order two.
The previous argument tells us that \( \mathbb{K}(\zeta_3) \) is fixed by the automorphisms \( F_{i,1} \) for \( i = 0, \ldots, 5 \) and then \( F_{i,2} \) are the six symmetries of \( D_6 \).

Since \( [\mathbb{K}(\alpha) : \mathbb{K}] = 6 \) we have that \( F_{0,2} \) fixes \( \mathbb{K}(\alpha) \). Furthermore, the fact that \( \mathbb{K}(\alpha) = \mathbb{K}(\beta) \) implies that \( F_{0,2} \) also fixes \( \beta \), and consequently \( \sqrt[6]{b} \). In the same way, the map \( F_{3,2} \) is a symmetry and then it has order two. This means that \( F_{3,2}(\beta) = \alpha \). We can now prove the following lemma.

**Lemma 3.2.** If \( \alpha \) and \( \beta \) are taken as before then \( \mathbb{K}(\alpha + \beta) \subset \mathbb{K}(\sqrt[6]{b}) \).

**Proof.** We do some computations:

\[
(\alpha + \beta)^3 = \alpha^3 + \beta^3 + 3\alpha\beta(\alpha + \beta) = -a + 3\sqrt[6]{b}(\alpha + \beta)
\]

and then \( \alpha + \beta \) is a root of \( g(x) = x^3 - 3\sqrt[6]{b}x + a \in \mathbb{K}(\sqrt[6]{b})[x] \).

The polynomial \( g(x) \) does not have all three roots in \( \mathbb{K}(\sqrt[6]{b}) \) because

\[
\sqrt{\text{disc}(g(x))} = \sqrt{-27\Delta} = 3 \cdot i\sqrt{3} \cdot \sqrt{\Delta} \notin \mathbb{K}(\sqrt[6]{b}) .
\]

Furthermore, \( g(x) \) is not irreducible because otherwise 9 would divide 6.

At the end, we have that either \( \mathbb{K}(\alpha + \beta) \subset \mathbb{K}(\sqrt[6]{b}) \) or \( [\mathbb{K}(\alpha + \beta) : \mathbb{K}] = 6 \) and \( \mathbb{K}(\alpha + \beta) = \mathbb{K}(\alpha) \). In the latter case \( \alpha + \beta \) should only be fixed by \( F_{0,2} \); this is not true because \( F_{3,2}(\alpha + \beta) = \alpha + \beta \). \( \Box \)

Now we can study the other automorphisms. The maps \( F_{i,1} \) and \( F_{i,2} \) are in the cyclic subgroup \( H \) of order six of \( D_6 \). Since \( F_{i,1}^3(\alpha) = F_{i,2}^3(\alpha) = \alpha \), we have that they are the elements of order three of the Galois group. Let us compute \( F_{i,1}(\beta) \): it is easy to check that \( \alpha \neq \beta \) implies \( F_{i,1}(\beta) = \beta\zeta_3^i \), where \( j \) is not zero because \( F_{i,1} \) cannot fix \( \beta \). Moreover, if \( j = 2 \) then \( F_{1,1}(\beta) = 2 \beta \zeta_3^2 \) is impossible since \( \mathbb{K}(\sqrt[6]{b}) \) is a cubic extension of \( \mathbb{K} \) and then it is fixed by an order four subgroup of \( D_6 \). We conclude that \( F_{i,1}(\beta) = \beta\zeta_3 \) and, using the same proof, \( F_{i,2}(\beta) = \beta\zeta_3^2 \).

We now consider the other symmetries. Since their order is two we immediately obtain that \( F_{i,2}(\beta) = \alpha\zeta_3^i \) for \( i = 4, 5 \). On the other hand, as before we have that \( F_{i,2}(\beta) = \beta\zeta_3^i \) and \( j \) is not zero. Again, if \( j = 2 \) then \( F_{i,2}(\beta) = 2 \beta \zeta_3^2 \) is impossible since \( F_{0,2} \) and \( F_{3,2} \) are the only two symmetries that could fix \( \sqrt[6]{b} \). We have gotten that \( F_{i,2}(\beta) = \beta\zeta_3 \) and again the same proof also gives \( F_{i,2}(\beta) = \beta\zeta_3^2 \).

We have three automorphisms left to consider: \( F_{3,1}, F_{4,1} \) and \( F_{5,1} \). For Lemma 3.2 the order of \( F_{3,1} \) is two; in fact, it says that the order two element in \( H \) has to fix \( \alpha + \beta \). It is an easy check that this cannot happen if such an element is \( F_{4,1} \) or \( F_{5,1} \). In conclusion, one has \( F_{3,1}(\beta) = \alpha \).

The maps \( F_{4,1} \) and \( F_{5,1} \) are the two elements of order six in \( D_6 \). We know that these two maps send \( \beta \) to \( \alpha\zeta_3^i \) for some \( i \) because one has \( \alpha \neq \beta \); in order to determine \( i \) we use the following relation in \( D_6 \):

\[
r^k = sr^{6-k}s \quad \text{for} \quad k = 0, \ldots, 5 ,
\]

where \( s \) is a symmetry and \( r \) is an order six rotation. We use this equation with \( k = 5, r = F_{4,1} \) and \( s = F_{3,2} \) and we get

\[
\beta\zeta_3^2 = F_{5,1}(\alpha) = (F_{3,2} \circ F_{4,1} \circ F_{3,2})(\alpha) = \beta\zeta_3^{2i} ,
\]

which means that \( F_{4,1}(\beta) = \alpha\zeta_3^i = \alpha\zeta_3 \), and

\[
F_{5,1}(\beta) = (F_{3,2} \circ F_{4,1} \circ F_{3,2})(\beta) = \alpha\zeta_3^2 .
\]

This concludes the study of the automorphisms in \( \text{Gal} \left( F/\mathbb{K} \right) \). We summarize the results in the following table.  

\begin{center}
\begin{tabular}{|c|c|c|c|}
\hline
\( F_{i,1} \) & \( \alpha \) & \( \beta \) & \( \alpha + \beta \) \\
\hline
\( F_{i,2} \) & \( \alpha\zeta_3^i \) & \( \beta\zeta_3 \) & \( \beta\zeta_3^2 \) \\
\hline
\end{tabular}
\end{center}
\[
\begin{array}{|c|c|c|c|c|}
\hline
F_{(0,1)}(\beta) = \beta & F_{(0,1)}(\sqrt[3]{b}) = \sqrt[3]{b} & F_{(0,2)}(\beta) = \beta & F_{(0,2)}(\sqrt[3]{b}) = \sqrt[3]{b} \\
\hline
F_{(1,1)}(\beta) = \beta \zeta_3 & F_{(1,1)}(\sqrt[3]{b}) = \sqrt[3]{b} \zeta_3^2 & F_{(1,2)}(\beta) = \beta \zeta_3 & F_{(1,2)}(\sqrt[3]{b}) = \sqrt[3]{b} \zeta_3^2 \\
\hline
F_{(2,1)}(\beta) = \beta \zeta_3^2 & F_{(2,1)}(\sqrt[3]{b}) = \sqrt[3]{b} \zeta_3 & F_{(2,2)}(\beta) = \beta \zeta_3^2 & F_{(2,2)}(\sqrt[3]{b}) = \sqrt[3]{b} \zeta_3 \\
\hline
F_{(3,1)}(\beta) = \alpha & F_{(3,1)}(\sqrt[3]{b}) = \sqrt[3]{b} & F_{(3,2)}(\beta) = \alpha & F_{(3,2)}(\sqrt[3]{b}) = \sqrt[3]{b} \\
\hline
F_{(4,1)}(\beta) = \alpha \zeta_3 & F_{(4,1)}(\sqrt[3]{b}) = \sqrt[3]{b} \zeta_3^2 & F_{(4,2)}(\beta) = \alpha \zeta_3 & F_{(4,2)}(\sqrt[3]{b}) = \sqrt[3]{b} \zeta_3^2 \\
\hline
F_{(5,1)}(\beta) = \alpha \zeta_3^2 & F_{(5,1)}(\sqrt[3]{b}) = \sqrt[3]{b} \zeta_3 & F_{(5,2)}(\beta) = \alpha \zeta_3^2 & F_{(5,2)}(\sqrt[3]{b}) = \sqrt[3]{b} \zeta_3 \\
\hline
\end{array}
\]

Figure 2: The values of \( \beta \) and \( \sqrt[3]{b} \) for the twelve automorphisms of \( \text{Gal} \left( \mathbb{F}/\mathbb{K} \right) \cong D_6 \).

We have completely described the Galois group when \( \sqrt[3]{b} \notin \mathbb{K} \) and \( [\mathbb{F} : \mathbb{K}] = 12 \). This allows us to determine when \( \text{Gal} \left( \mathbb{F}/\mathbb{K} \right) \) is isomorphic to the Dihedral group \( D_6 \).

**Proposition 3.3.** Take a field \( \mathbb{K} \), not containing all the cubic roots of unity, such that \( \text{char}(\mathbb{K}) \neq 2 \) and an irreducible polynomial \( f(x) = x^6 + ax^3 + b \) over \( \mathbb{K} \). Suppose that \( \sqrt[3]{b} \notin \mathbb{K} \) and \( \Delta \neq -3n^2 \) for every \( n \in \mathbb{K} \).

Then \( \text{Gal} \left( \mathbb{F}/\mathbb{K} \right) \cong D_6 \) if and only if \( R(x) = x^3 - 3bx + ab \) is reducible over \( \mathbb{K} \), where \( \mathbb{F} \) is the splitting field of \( f(x) \).

**Proof.** We start with the only if implication. We have that \( \alpha \beta (\alpha + \beta) = c \in \mathbb{K} \) because is fixed by all the automorphisms in \( \text{Gal} \left( \mathbb{F}/\mathbb{K} \right) \), see Figure 2.

Then one has
\[
c^2 = \alpha^2 \beta^2 (\alpha + \beta)^2 = \alpha^2 \beta^2 (\alpha^2 + \beta^2) + 2b
\]

which implies that
\[
ab = b(\alpha^3 + \beta^3) = b(\alpha + \beta)(\alpha^2 - \alpha \beta + \beta^2) = c(c^2 - 2b - b) = c^3 - 3bc.
\]

Conversely, if \( R(x) \) is reducible over \( \mathbb{K} \) then, since \( \text{disc}(R(x)) = -27\Delta \) is not a square in \( \mathbb{K} \), we can choose \( \alpha \) and \( \beta \) in the way that \( \alpha \beta (\alpha + \beta) = c \in \mathbb{K} \). We recall that we observed in the previous section that the three roots of \( R(x) \) are \( \alpha \beta (\alpha + \beta), \alpha \beta (\alpha \zeta_3 + \beta \zeta_3^2) \) and \( \alpha \beta (\alpha \zeta_3^2 + \beta \zeta_3) \).

In other words, one has \( \alpha + \beta = \frac{a}{b} \sqrt[3]{b} \). Since \( \beta = -\frac{1}{b} \cdot \alpha^5 \sqrt[3]{b} = \frac{c^2}{b} \cdot \alpha^2 \sqrt[3]{b} \) we get
\[
bc^2 - \alpha^5 \sqrt[3]{b} - \alpha^2 \sqrt[3]{b} - c^3 \sqrt[3]{b} = 0 \tag{3.1}
\]

which is a non-trivial \( \mathbb{K} \)-linear combination between elements of
\[
C = \left\{ \alpha^i \beta^j \mid i = 0, \ldots, 5; j = 0, 1, 2 \right\}.
\]

Suppose that \( [\mathbb{F} : \mathbb{K}] = 36 \) then \( [\mathbb{K}(\sqrt[3]{b}, \alpha) : \mathbb{K}] = 18 \) and \( C \) is a basis of \( \mathbb{K}(\sqrt[3]{b}, \alpha) \); this is a contradiction because of Equation (3.1).

In particular, it follows that, under the hypothesis of Proposition 3.3, we can choose \( \alpha \) and \( \beta \) in the way that \( \alpha + \beta = \frac{c}{b} \sqrt[3]{b} \), where \( c \) is the rational root of \( R(x) \). Moreover, we have that \( \mathbb{K}(\sqrt[3]{b}) \) is the only cubic subfield of \( \mathbb{K}(\alpha) = \mathbb{K}(\beta) \).
Corollary 3.4. Suppose that \( \text{char}(\mathbb{F}) \neq 2 \), the field \( \mathbb{F} \) does not contain all the cubic roots of unity and \( \Delta \neq -3n^2 \).

We have that \( \text{Gal}(\mathbb{F}/\mathbb{K}) \cong S_3 \times S_3 \) if and only if \( \sqrt[3]{b} \notin \mathbb{K} \) and \( R(x) \) is irreducible over \( \mathbb{K} \).

Proof. It follows immediately from Lemma 2.4, Propositions 3.1 and 3.3.

We now give some examples of polynomials for which we can compute the Galois group.

Corollary 3.5. We consider infinite families of \( a, b \in \mathbb{Z} \) when \( f(x) = x^6 + ax^3 + b \in \mathbb{Q}[x] \) is irreducible over \( \mathbb{Q} \) and \( \Delta \neq -3n^2 \). Hence, in the following cases one has \( \text{Gal}(\mathbb{F}/\mathbb{Q}) \cong S_3 \times S_3 \):

1. \( b = 2 \) and \( a \equiv 1 \) mod 10;
2. \( b = 27(100n + 23)^3 + 1 \) with \( n \leq -1 \) and \( a \equiv 25 \) mod 30.

While in the following ones \( \text{Gal}(\mathbb{F}/\mathbb{Q}) \cong D_6 \):

3. \( b \equiv 10 \) mod 12 and \( a = 0 \);
4. \( b = -(5n + 1)^3 \) with \( n > 0 \) and \( a \equiv 3 \) mod 5.

Proof. Cases 1 and 2 follows applying Eisenstein criterion to \( R(x) \), while in Case 3 we observe that 0 is a root of \( R(x) \). Finally, for Case 4 we note that \( \sqrt[3]{b} = -5n - 1 \in \mathbb{Z} \).

From now on we suppose that \( \Delta = -3n^2 \) for some \( n \in \mathbb{K} \). This implies \( \mathbb{K}(\zeta_3) \subset \mathbb{K}(\alpha) \) for Lemma 2.2. From what we said in the previous section, see Figure 1, we have that

\[
[F:\mathbb{K}] = \begin{cases} 18 & \Rightarrow \text{Gal}(\mathbb{F}/\mathbb{K}) \cong C_3 \times S_3 \\ 6 & \Rightarrow \text{Gal}(\mathbb{F}/\mathbb{K}) \cong S_3 \text{ or } C_6. \end{cases}
\]

All these three cases can happen, here we give an example for each group over the rational numbers:

- \( C_3 \times S_3 \): \( x^6 + 3x^3 + 3 \);
- \( S_3 \): \( x^6 + 3 \);
- \( C_6 \): \( x^6 + x^3 + 1 \).

Proposition 3.6. Suppose that \( \mathbb{K} \) is a field without all the cubic roots of unity and such that \( \text{char}(\mathbb{K}) \neq 2 \). Moreover, we assume \( \Delta = -3n^2 \).

Then one has \( \text{Gal}(\mathbb{F}/\mathbb{K}) \cong C_6 \) if and only if \( \sqrt[3]{b} \in \mathbb{K} \).

Proof. We start with the if implication. Suppose \( \sqrt[3]{b} = d \in \mathbb{K} \). This implies that \( d(\alpha + \beta) \) is a root of \( R(x) = x^3 - 3bx + ab \), for the right choice of \( \alpha \) and \( \beta \). We have that

\[
\text{disc}(R(x)) = 108b^3 - 27a^2b^2 = -27b^2\Delta
\]

and then

\[
\sqrt{\text{disc}(R(x))} = 3b \cdot i\sqrt{3} \cdot \sqrt{\Delta} = -9bn \in \mathbb{K}.
\] (3.2)

From this and the fact that \( R(x) \) is irreducible for Lemma 2.4, we obtain that \( \text{Gal}(\mathbb{M}/\mathbb{K}) \cong C_3 \), where \( \mathbb{M} \) is the splitting field of \( R(x) \), and \( \mathbb{M} = \mathbb{K}(\alpha + \beta) \) is a normal extension of \( \mathbb{K} \) of degree 3.

Since \( \sqrt[3]{b} \in \mathbb{K} \) we know that \( [F:\mathbb{K}] = 6 \) and if the Galois group is not \( C_6 \) then it should be \( S_3 \), but \( S_3 \) does not have a normal subgroup of order two.

Conversely, if \( \sqrt[3]{b} \notin \mathbb{K} \) then \( \mathbb{K}(\sqrt[3]{b}) \) and \( \mathbb{K}(\sqrt[3]{b} \zeta_3) \) are two distinct cubic extensions of \( \mathbb{K} \), but the group \( C_6 \) has only one subgroup of order two.
We now prove a similar result for the case when the Galois group is $S_3$.

**Proposition 3.7.** Under the same conditions in Proposition 3.6 we have that $\text{Gal}\left(\mathbb{F}/\mathbb{K}\right) \cong S_3$ if and only if $R(x) = x^3 - 3bx + ab$ is reducible over $\mathbb{K}$.

**Proof.** As before, let us begin with the if implication. Say $\alpha \beta (\alpha + \beta) = c \in \mathbb{K}$; then one has

$$ba - \alpha^5 \sqrt{b} - a\alpha^2 \sqrt{b} - c^3 \sqrt{b^2} = 0$$

and, like in the proof of Proposition 3.3, this is a non-trivial $\mathbb{K}$-linear combination between elements of the basis

$$\mathcal{D} = \{\alpha^i \sqrt{b^j} \mid i = 0, ..., 5; j = 0, 1, 2\}$$

of $\mathbb{K}(\sqrt[3]{b}, \alpha)$. Hence, the Galois group cannot have order 18. Clearly, we also have that $\text{Gal}\left(\mathbb{F}/\mathbb{K}\right)$ is not isomorphic to $C_6$ for Proposition 3.6 and we conclude using Lemma 2.4.

Conversely, suppose that $\text{Gal}\left(\mathbb{F}/\mathbb{K}\right) \cong S_3$. Then we know that $\sqrt{b} \notin \mathbb{K}$ for Proposition 3.6 and $\mathbb{F} = \mathbb{K}(\sqrt[3]{b}, \zeta_3)$. If we assume that $R(x)$ is irreducible then we can prove that its splitting field is a normal extension of $\mathbb{K}$ of degree 3, using Equation (3.2). This is a contradiction because $S_3$ doesn’t have normal subgroups of order two.

We conclude with the following corollary.

**Corollary 3.8.** Under the same conditions in Proposition 3.6 we have that $\text{Gal}\left(\mathbb{F}/\mathbb{K}\right) \cong C_3 \times S_3$ if and only if $\sqrt[3]{b} \notin \mathbb{K}$ and $R(x)$ is irreducible over $\mathbb{K}$.

**Proof.** It follows immediately from Lemma 2.4, Propositions 3.6 and 3.7.

Furthermore, we produce some families of polynomials whose Galois groups can be determined from the results in this subsection.

**Corollary 3.9.** Suppose that $\mathbb{K} = \mathbb{Q}$. Then we have that

1. if $f(x) = x^6 + 3(3n + 1)^2$ then $\text{Gal}\left(\mathbb{F}/\mathbb{Q}\right) \cong S_3$;
2. if $f(x) = x^6 + (5n + 1)^3x^3 + (5n + 1)^6$ then $\text{Gal}\left(\mathbb{F}/\mathbb{Q}\right) \cong C_6$;
3. if $f(x) = x^6 + px^3 + p^2$ where $p \equiv 1 \mod 5$ is prime then $\text{Gal}\left(\mathbb{F}/\mathbb{Q}\right) \cong C_3 \times S_3$.

**Proof.** In Case 1 the polynomial $R(x)$ is clearly reducible and 3 is not a square in $\mathbb{Q}$. In Case 2 $b$ is a cube and in Case 3 we see that $R(x) = x^3 - 3p^2x + p^3$. This polynomial is irreducible because the only possible rational solutions are $\{1, p, p^2, p^3\}$, but it is easy to check that none of these actually makes $R(x)$ vanish.

### 3.2 Proof of Theorem 1.1: cubic roots of unity in $\mathbb{K}$

In this subsection we suppose that $\mathbb{K}$ is a field with characteristic different from two, but such that all the three cubic roots of unity belong to $\mathbb{K}$. This means that either $\text{char}(\mathbb{K}) = 3$ or $\zeta_3 \in \mathbb{K}$.

Note that if $f(x) = x^6 + ax^3 + b$ is irreducible over $\mathbb{K}$ then $\Delta \neq -3n^2$ for every $n \in \mathbb{K}$.

**Proposition 3.10.** Suppose that $\zeta_3 \in \mathbb{K}$ and $f(x) = x^6 + ax^3 + b$ is irreducible over $\mathbb{K}$, a field such that $\text{char}(\mathbb{K}) \neq 2$. Denote with $\mathbb{F}$ the splitting field of $f(x)$ as before. Then we have that
• \( \text{Gal} \left( \overline{F}/K \right) \cong S_3 \) if and only if \( \sqrt[3]{b} \in K \) and \( R(x) = x^3 - 3bx + ab \) is irreducible over \( K \);

• \( \text{Gal} \left( \overline{F}/K \right) \cong C_6 \) if and only if \( \sqrt[3]{b} \notin K \) and \( R(x) \) is reducible over \( K \).

**Proof.** Let us prove the if implications first. Since \( \sqrt[3]{b}, \zeta_3 \in K \) one has \( [F : K] = 6 \) and \( F = K(\sqrt[3]{\alpha \beta}, \zeta_3) \) because \( \sqrt[3]{b} (\alpha + \beta) \) is a root of \( R(x) \) which is irreducible. Moreover, the field \( F \) is the splitting field of \( R(x) \) because \( \text{char}(K) \neq 3 \) and \( \sqrt{\text{disc}(R(x))} = m\sqrt{\Delta} \) for some non-zero \( m \in K \). Then it follows from a standard result in Galois theory, see [3], that \( \text{Gal} \left( \overline{F}/K \right) \) is isomorphic to \( S_3 \). Note that here we use that \( \text{char}(K) \neq 2 \).

Now suppose that \( \sqrt[3]{b} \notin K \) and \( R(x) \) is reducible. The fact that \( [F : K] \neq 18 \) follows in the same way as in the proof of Propositions 3.10 and 3.11. Then we have that \( F = K(\sqrt[3]{\alpha \beta}, \sqrt[3]{\beta}) \), but \( K(\sqrt[3]{\beta}) \) is a normal extension of \( K \) because it is the splitting field of \( x^3 - b \). This implies that \( \text{Gal} \left( \overline{F}/K \right) \cong C_6 \).

Conversely, suppose that \( \text{Gal} \left( \overline{F}/K \right) \) is isomorphic to \( C_6 \). We immediately obtain that \( \sqrt[3]{b} \notin K \) for what we said before and Lemma 2.4. If \( R(x) \) is irreducible then, since \( \text{disc}(R(x)) \) is not a square in \( K \) and \( \text{char}(K) \neq 2 \), the Galois group should be \( S_3 \), but this is a contradiction.

Finally, we say that \( \text{Gal} \left( \overline{F}/K \right) \cong S_3 \). Then \( R(x) \) is irreducible over \( K \), again for what we said before and Lemma 2.4 and \( K(\sqrt[3]{b}) \) is a normal extension of degree three of \( K \) if we suppose that \( \sqrt[3]{b} \) is not in \( K \). This completes the proof because \( S_3 \) does not have a normal subgroup of order two.

From the previous proposition we also obtain the following result.

**Corollary 3.11.** With the hypothesis of Proposition 3.10 we have that \( \text{Gal} \left( \overline{F}/K \right) \cong C_3 \times S_3 \) if and only if \( \sqrt[3]{b} \notin K \) and \( R(x) \) is irreducible over \( K \).

**Proof.** It follows immediately from Lemma 2.4 and Proposition 3.10.

The following corollary shows another family of polynomials with Galois group isomorphic to \( C_6 \).

**Corollary 3.12.** If \( f(x) = x^6 - p \) where \( p \) is a prime integer then \( \text{Gal} \left( \overline{F}/\mathbb{Q}(\zeta_3) \right) \cong C_6 \).

**Proof.** We note that \( f(x) \) is always irreducible over \( \mathbb{Q}(\zeta_3) \). In fact, it is irreducible over \( \mathbb{Q} \) for the Eisenstein criterion and one has \( [\mathbb{Q}(\zeta_3, \sqrt[3]{p}) : \mathbb{Q}] = 12 \). Moreover, one has \( \sqrt[3]{p} \notin \mathbb{Q}(\zeta_3) \) since \( [\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2 \), while \( R(x) = x^3 + 3px \) is clearly reducible.

There is only one case which is left to study: when \( K \) is a field with characteristic equal to three. We do this in the following proposition.

**Proposition 3.13.** Suppose that \( K \) is a field such that \( \text{char}(K) = 3 \) and \( f(x) = x^6 + ax^3 + b \) is irreducible over \( K \).

Then we have that \( [F : K] = 6, 18 \) depending on whether \( K(\sqrt[3]{a}, \sqrt[3]{b}) \) is degree 3 or 9 over \( K \), but \( f(x) \) and \( F \) are not separable and then we cannot define the Galois group.

**Proof.** Since \( \text{char}(K) = 3 \) we have that \( R(x) = x^3 + ab \) and \( \alpha + \beta = -\sqrt[3]{a} \). We observe that \( f(x) \) factors as

\[
 f(x) = \left( x^2 + \sqrt[3]{a} x + \sqrt[3]{b} \right)^3 \quad (3.3)
\]

in the algebraic closure of \( K \). Therefore, the field \( F \) coincides with the splitting field of \( x^2 + \sqrt[3]{a} x + \sqrt[3]{b} \) over \( K(\sqrt[3]{a}, \sqrt[3]{b}) \).

We have that \( K(\sqrt[3]{a}) \) and \( K(\sqrt[3]{b}) \) are two extensions of \( K \) of degree one or three. Furthermore, if \( \sqrt[3]{a}, \sqrt[3]{b} \in K \) then the factor \( x^2 + \sqrt[3]{a} x + \sqrt[3]{b} \) of \( f(x) \) in Equation (3.3) belongs to \( K[x] \), but \( f(x) \) is
irreducible over \( K \). In other words, one has \([K(\sqrt[3]{a}, \sqrt[3]{b}) : K] = 3, 9\); in fact, if the degree was 6 then \( \sqrt[3]{b} \) should be the root of a degree 2 polynomial in \( K(\sqrt[3]{a}) \), and

\[
[K : K] = [K : K(\sqrt[3]{a}, \sqrt[3]{b})] \cdot [K(\sqrt[3]{a}, \sqrt[3]{b}) : K] = 6, 18.
\]

Since \( f(x) \) is irreducible we have that it is the minimal polynomial of \( \alpha \) over \( K \). The roots of \( f(x) \) are \( \alpha \) and \( \beta \), each one with multiplicity three, which means \( \alpha \) is not separable over \( K \). In particular, this implies that \( F \) is not a separable extension of \( K \) and then there is no Galois group in this case. \( \square \)

Note that irreducible polynomials of this kind really exist: examples are given by \( x^6 - u \) and \( x^6 + uvx^3 + u \in F_3(u, v)[x] \), where \( u \) and \( v \) are transcendental over \( F_3 \). The proposition we proved before clearly implies that their splitting field \( F \) is not a separable extension. Moreover, we can also observe that the group of automorphisms of \( F \) only has two elements, despite \([F : F_3(u, v)] \) being higher.

### 3.3 Irreducible polynomials over finite fields

In this subsection \( K \) is a finite field; in other words, we consider \( K = F_{p^k} \) where \( p \) is an odd prime and \( k \geq 1 \) is an integer. We say that \( p \neq 2 \) because we want \( \text{char}(K) \) different from two.

It is known from Galois theory \([3]\) that the algebraic extensions of a finite field are uniquely determined from the degree and are always separable. Moreover, it follows immediately from this fact that Galois groups of finite extensions of \( F_{p^k} \) are cyclic.

If we take an irreducible polynomial \( f(x) = x^6 + ax^3 + b \in F_{p^k}[x] \) then it has to be \( \text{Gal}(F/F_{p^k}) \) \( \cong C_6 \), where \( F \) is the splitting field of \( f(x) \). Since the results obtained in the previous subsections hold for finite fields too, provided that the characteristic is not two, we can prove a criterion that allows us to say when a polynomial \( f(x) \) as before is irreducible.

**Proof of Theorem 1.52** Let us consider Case 1. If \( f(x) \) is irreducible then the Galois group of the splitting field \( F \) is isomorphic to \( C_6 \). The claim follows from Proposition 3.6 because \( \zeta_3 \) is not in the field for our assumption on \( p^k \).

Suppose that \( R(x) \) is irreducible. Then the splitting field of \( R(x) \) over \( F_{p^k} \) has degree three. This means that, since \( \text{char}(K) \neq 2 \), the discriminant of \( R(x) \) is a square in \( F_{p^k} \); in other words, we have that \( -3\Delta \) is a square.

Now, we use the hypothesis that \( p^k \equiv 1 \) mod 3 and \( p \) is not three, which tells us that \( \zeta_3 \notin F_{p^k} \) and then \( -3 \) and \( \Delta \) are both not squares in \( F_{p^k} \). This implies that \( F \) contains an extension of \( F_{p^k} \) of degree two and one of degree three; hence, one has \([F : F_{p^k}] = 6\).

We conclude that \( f(x) \) is irreducible because the only factorizations of \( f(x) \) in the algebraic closure of \( F_{p^k} \) are: products of two degree three polynomials or products of three degree two polynomials. In these cases one has \([F : F_{p^k}] = 3, 2\). We cannot have \( \alpha \in F_{p^k} \) because otherwise \( 2\alpha^3 + b = \sqrt{\Delta} \) also belongs to \( F_{p^k} \); this is impossible for what we said before.

We now prove Case 2. If \( f(x) \) is irreducible then the claim follows in the same way as in Case 1 from Proposition 3.10 because \( p^k \equiv 1 \) mod 3 implies \( \zeta_3 \in F_{p^k} \). Suppose that \( \sqrt[3]{b}, \sqrt{\Delta} \notin F_{p^k} \); then we have that \([F : F_{p^k}] = 6\) and we conclude as in Case 1.

Finally, if \( p = 3 \) then we have that the map \( x \to x^3 \) is the Frobenius automorphism of \( F_{3^k} \). This means that any element in the field is a cube and \( f(x) = \left(x^2 + \sqrt[3]{a} x + \sqrt[3]{b}\right)^3 \) is reducible over \( F_{p^k} \). \( \square \)

We note that \( p^2 \) is always equal to \( 1 \) mod 3 when \( p \neq 3 \) and then Case 1 can only happen if \( k \) is odd.
4 Subfields

In this section we use Galois correspondence to give a complete list of all the intermediate extensions of \( K \) inside the splitting field \( \mathbb{F} \) of \( f(x) = x^6 + ax^3 + b \). We consider all the possible cases that we studied before in the paper. Moreover, we assume \( \text{char}(K) \neq 2, 3 \).

4.1 \( \zeta_3 \notin K \) and \( \Delta \neq -3n^2 \)

\( \sqrt{\Delta} \notin K \) and \( R(x) \) reducible over \( K \)  
We explicitly described the Galois group in Subsection 3.1. We have that \( \text{Gal} \left( \mathbb{F}/K \right) \cong D_6 \) and there are 14 proper subfields, as shown in Figure 3.

- Degree 2:
  \[ K(\sqrt{\Delta}), K(\zeta_3), K(\sqrt{-3\Delta}) \]
  normal
  we recall that \( K(\zeta_3) = K(i\sqrt{3}) \);

- Degree 3:
  \[ K(\sqrt[3]{b}), K(\sqrt[3]{b} \zeta_3), K(\sqrt[3]{b} \zeta_3^2) \]
  since when we say \( \sqrt{\Delta} \notin K \) we mean exactly that \( x^3 - b \) is irreducible;

- Degree 4:
  \[ K(\sqrt{\Delta}, \zeta_3) \]
  normal

- Degree 6:
  \[ K(\zeta_3, \sqrt{b}) \]
  normal
  this is the splitting field of \( x^3 - b \) over \( K \),
  \[ K(\alpha), K(\alpha \zeta_3), K(\alpha \zeta_3^2) \]
  \[ K(\alpha \zeta_3 + \beta \zeta_3^2), K(\alpha + \beta \zeta_3), K(\alpha + \beta \zeta_3^2) \]
  each of these extensions is fixed by exactly one symmetry of \( D_6 \), see Figure 2.

\( \sqrt{b} \in K \) and \( R(x) \) irreducible over \( K \)  
The Galois group is isomorphic to \( D_6 \) like in the previous case.

\[
\begin{array}{c|c|c}
| 1 & 1 & 1 \\
2 & 7 & 1 \\
3 & 1 & 1 \\
4 & 3 & 0 \\
6 & 3 & 3 \\
12 & 1 & 1 \\
\end{array}
\]

Figure 3: This table shows the number of subgroups of \( D_6 \) (central column) of a given order (left column). The right column indicates the number of normal subgroups.
Then we again have 14 subfields, see Figure 3:

- **Degree 2:**
  \[ K(\sqrt{\Delta}), K(\zeta_3), K(\sqrt{-3\Delta}) \]
  normal
  
  In this case \( K(\sqrt{-3\Delta}) \) is the quadratic extension that corresponds to \( C_6 \triangleleft D_6 \);

- **Degree 3:**
  \[ K(\alpha + \beta), K(\alpha\zeta_3 + \beta\zeta_3^2), K(\alpha\zeta_3^2 + \beta\zeta_3) \]
  since \( R(x) \) is irreducible and its discriminant is not a square in \( K \), the cubic subfields are generated by its roots;

- **Degree 4:**
  \[ K(\sqrt{\Delta}, \zeta_3) \]
  normal;

- **Degree 6:**
  \[ K(\sqrt{-3\Delta}, \alpha + \beta) \]
  normal
  
  This is the splitting field of \( R(x) \) over \( K \),
  \[ K(\alpha), K(\alpha\zeta_3), K(\alpha\zeta_3^2) \]
  these extensions have degree six because they are generated by roots of \( f(x) \), which is irreducible, and are distinct because \( \zeta_3 \notin K \). Furthermore, they all contain \( \sqrt{\Delta} \) and then they are the three symmetries of the \( S_3 \) subgroup of \( D_6 \) represented by \( K(\sqrt{\Delta}) \),
  \[ K(\zeta_3, \alpha + \beta), K(\zeta_3, \alpha\zeta_3 + \beta\zeta_3^2), K(\zeta_3, \alpha\zeta_3^2 + \beta\zeta_3) \]
  corresponding to the three symmetries of the \( S_3 \) subgroup of \( D_6 \) represented by \( K(\zeta_3) \); such subgroup also corresponds to \( \text{Gal}(K(\zeta_3)/K) \), which is the splitting field of \( R(x) \) over \( K(\zeta_3) \).

\( \sqrt{b} \notin K \) and \( R(x) \) irreducible over \( K \). The Galois group is isomorphic to \( S_3 \times S_3 \). There are 58 subfields as shown in Figure 4.
Figure 4: Table of the subgroups of $S_3 \times S_3$. The diagram on the right shows the two normal extensions of $K$ of degree six which generate $F$.

A basis for the splitting field $F$ is

$$E = \left\{ \alpha^i \cdot \zeta_3^j \cdot \sqrt[3]{b}^k \mid i = 0, \ldots, 5; j = 1, 2; k = 0, 1, 2 \right\}$$

and then $\text{Gal}(F/K)$ is completely determined by:

- $F(\alpha) = \alpha \zeta_3^i$ \quad $i = 0, 1, 2$;
- $F(\alpha) = \beta \zeta_3^i$ \quad $i = 3, 4, 5$;
- $F(\zeta_3) = \zeta_3^j$ \quad $j = 1, 2$;
- $F(\sqrt[3]{b}) = \sqrt[3]{b} \zeta_3^k$ \quad $k = 0, 1, 2$.

It is possible to distinguish each pair of the following subfields, say $K_1$ and $K_2$ for example, by showing that one of these automorphisms fixes $K_1$, but not $K_2$.

- **Degree 2:**
  $$K(\zeta_3), K(\sqrt{3\Delta}), K(\sqrt{\Delta})$$  
  normal
  there are three subgroups of order 18 in $S_3 \times S_3$: two are isomorphic to $C_3 \times S_3$, while the third one to $C_3 \times S_3$. The latter subgroup corresponds to $K(\sqrt{\Delta})$;

- **Degree 3:**
  $$K(\sqrt[3]{b}), K(\sqrt[3]{b} \zeta_3), K(\sqrt[3]{b} \zeta_3^2),$$
  $$K(\sqrt[3]{b}(\alpha + \beta)), K(\sqrt[3]{b}(\alpha \zeta_3 + \beta \zeta_3^2)), K(\sqrt[3]{b}(\alpha \zeta_3^2 + \beta \zeta_3))$$;

- **Degree 4:**
  $$K(\sqrt{\Delta}, \zeta_3)$$  
  normal.
\begin{itemize}
  \item Degree 6:
  \[ \mathbb{K}(\zeta_3, \sqrt[3]{\Delta}), \mathbb{K}\left(\sqrt{-3\Delta}, \sqrt[3]{\alpha + \beta}\right) \] normal
  see Figure 4
  \[ \mathbb{K}\left(\zeta_3, \sqrt[3]{\alpha + \beta}\right), \mathbb{K}\left(\zeta_3, \sqrt[3]{\alpha \zeta_3 + \beta \zeta_3^2}\right), \mathbb{K}\left(\zeta_3, \sqrt[3]{\alpha \zeta_3^2 + \beta \zeta_3}\right) \]
  these three extensions are generated by \( \mathbb{K}(\zeta_3) \) and the three cubic subfields of \( \mathbb{K}\left(\sqrt{-3\Delta}, \sqrt[3]{\alpha + \beta}\right) \),
  \[ \mathbb{K}(\sqrt{-3\Delta}, \sqrt[3]{\Delta}), \mathbb{K}(\sqrt{-3\Delta}, \sqrt[3]{\alpha \zeta_3}), \mathbb{K}(\sqrt{-3\Delta}, \sqrt[3]{\beta \zeta_3^2}) \]
  these other three are instead generated by \( \mathbb{K}(\sqrt{-3\Delta}) \) and the three cubic subfields of \( \mathbb{K}(\zeta_3, \sqrt[3]{\Delta}) \),
  \[ \mathbb{K}\left(\sqrt{-\Delta}, \sqrt[3]{\Delta}\right), \mathbb{K}\left(\sqrt{\Delta}, \sqrt[3]{\alpha \zeta_3 + \beta \zeta_3^2}\right), \mathbb{K}\left(\sqrt{\Delta}, \sqrt[3]{\alpha \zeta_3^2 + \beta \zeta_3}\right) \]
  they are generated by \( \mathbb{K}(\sqrt{\Delta}) \) and the three cubic subfields of \( \mathbb{K}(\zeta_3, \sqrt[3]{\Delta}) \),
  \[ \mathbb{K}\left(\sqrt{\Delta}, \sqrt[3]{\alpha + \beta}\right), \mathbb{K}\left(\sqrt{\Delta}, \sqrt[3]{\alpha \zeta_3 + \beta \zeta_3^2}\right), \mathbb{K}\left(\sqrt{\Delta}, \sqrt[3]{\alpha \zeta_3^2 + \beta \zeta_3}\right) \]
  as before these extensions are generated by \( \mathbb{K}(\sqrt{\Delta}) \) and the three cubic subfields of \( \mathbb{K}\left(\sqrt{-3\Delta}, \sqrt[3]{\alpha + \beta}\right) \),
  \[ \mathbb{K}(\alpha), \mathbb{K}(\alpha \zeta_3), \mathbb{K}(\alpha \zeta_3^2), \mathbb{K}(\beta), \mathbb{K}(\beta \zeta_3), \mathbb{K}(\beta \zeta_3^2) \]
  these subfields have the property of not containing any cubic extension of \( \mathbb{K} \), because they correspond to the six subgroups of \( S_3 \times S_3 \) of order six which are only contained by the \( C_3 \times S_3 \) subgroup;
  
  \item Degree 9:
  \[ \mathbb{K}(\alpha + \beta), \mathbb{K}(\alpha \zeta_3 + \beta \zeta_3^2), \mathbb{K}(\alpha \zeta_3^2 + \beta \zeta_3), \mathbb{K}((\alpha + \beta)\zeta_3^2), \mathbb{K}(\alpha + \beta \zeta_3), \mathbb{K}(\alpha \zeta_3 + \beta), \mathbb{K}((\alpha + \beta)\zeta_3), \mathbb{K}(\alpha \zeta_3^2 + \beta), \mathbb{K}(\alpha + \beta \zeta_3^2) \]
  each of the 9 subgroups of \( S_3 \times S_3 \) of order four is only contained in two subgroups of order 12, which are maximal. Hence, the extensions of degree 9 are generated by the elements obtained by taking the quotient of the generators of every cubic subfield of \( \mathbb{F} \);
  
  \item Degree 12:
  \[ \mathbb{K}\left(\sqrt{-\Delta}, \zeta_3, \sqrt[3]{\Delta}\right), \mathbb{K}\left(\sqrt{-\Delta}, \zeta_3, \sqrt[3]{\alpha + \beta}\right) \] normal
  these are the splitting fields of \((x^3 - b)(x^2 - \Delta)\) and \( R(x)(x^2 - \Delta) \),
  \[ \mathbb{K}(\zeta_3, \alpha), \mathbb{K}(\zeta_3, \beta) \]
  these extensions are clearly of degree 12 and they are distinct because \( \beta = \sqrt[3]{\zeta_3 - 1} \sqrt[3]{\alpha} \notin \mathbb{K}(\zeta_3, \alpha) \); moreover, they are not normal because they do not contain all the roots of \( f(x) \);
  
  \item Degree 18:
  \[ \mathbb{K}(\alpha, \beta), \mathbb{K}(\alpha, \beta \zeta_3), \mathbb{K}(\alpha, \beta \zeta_3^2), \mathbb{K}(\alpha \zeta_3, \beta), \mathbb{K}(\alpha \zeta_3, \beta \zeta_3), \mathbb{K}(\alpha \zeta_3^2, \beta), \mathbb{K}(\alpha \zeta_3^2, \beta \zeta_3), \mathbb{K}(\zeta_3, \alpha + \beta), \mathbb{K}(\zeta_3, \alpha + \beta \zeta_3), \mathbb{K}(\zeta_3, \alpha + \beta \zeta_3^2), \]
  \[ \mathbb{K}(\zeta_3, (\zeta_3 - 1)(\alpha - \beta)), \mathbb{K}(\zeta_3((\zeta_3 - 1)(\alpha - \beta))) \]
  the easiest way to show that these extensions are all different is to check that each one is fixed exactly by one element of order two of \( S_3 \times S_3 \).
\end{itemize}
4.2 \( \zeta_3 \notin \mathbb{K} \) and \( \Delta = -3n^2 \)

\( \sqrt[3]{b} \notin \mathbb{K} \) and \( R(x) \) reducible over \( \mathbb{K} \) The Galois group is isomorphic to \( S_3 \) and we immediately see that the proper subfields are the following four extensions of \( \mathbb{K} \).

- **Degree 2:** \( \mathbb{K}(i\sqrt{3}) \) normal;

- **Degree 3:** \( \mathbb{K}(\sqrt[3]{b}), \mathbb{K}(\sqrt[3]{b} \zeta_3), \mathbb{K}(\sqrt[3]{b} \zeta_3^2) \);

\( \sqrt[3]{b} \in \mathbb{K} \) and \( R(x) \) irreducible over \( \mathbb{K} \) We have that \( \text{Gal}(\mathbb{F}/\mathbb{K}) \cong C_6 \) and then there are only two subfields of \( \mathbb{F} \).

- **Degree 2:** \( \mathbb{K}(i\sqrt{3}) \) normal;

- **Degree 3:** \( \mathbb{K}(\alpha + \beta) \) normal;

\( \sqrt[3]{b} \notin \mathbb{K} \) and \( R(x) \) irreducible over \( \mathbb{K} \) In this case the Galois group is isomorphic to \( C_3 \times S_3 \) and there are 12 subfields, see Figure 5.

- **Degree 2:** \( \mathbb{K}(i\sqrt{3}) \) normal;

- **Degree 3:** \( \mathbb{K}\left(\sqrt[3]{b}(\alpha + \beta)\right) \) normal

this is the splitting field of \( R(x) \), whose discriminant is now a square in \( \mathbb{K} \),

\( \mathbb{K}(\sqrt[3]{b}), \mathbb{K}(\sqrt[3]{b} \zeta_3), \mathbb{K}(\sqrt[3]{b} \zeta_3^2) \);

- **Degree 6:** \( \mathbb{K}(\zeta_3, \sqrt[3]{b}), \mathbb{K}\left(\zeta_3, \sqrt[3]{b}(\alpha + \beta)\right) \) normal

these extensions are the splitting fields of \( x^3 - b \) and \( R(x)(x^2 + x + 1) \) respectively,

\( \mathbb{K}(\alpha), \mathbb{K}(\beta) \)
Figure 5: Table of the subgroups of $C_3 \times S_3$. The diagram on the right shows the decomposition of $F$ into two normal extension of $K$, one of degree three and the other of degree six.

- **Degree 9:**
  
  $K(\alpha + \beta), K((\alpha + \beta)\zeta_3), K((\alpha + \beta)\zeta_3^2)$

  because each of three subgroup of $C_3 \times S_3$ of order two is the intersection of one non-normal order 6 subgroup with the normal order 6 subgroup.

4.3 $\zeta_3 \in K$

$\sqrt{b} \notin K$ and $R(x)$ reducible over $K$ The Galois is isomorphic to $C_6$ and we have two subfields.

- **Degree 2:**
  
  $K(\sqrt{\Delta})$ normal;

- **Degree 3:**
  
  $K(\sqrt[3]{b})$ normal.

$\sqrt{b} \in K$ and $R(x)$ irreducible over $K$ The Galois is isomorphic to $S_3$ and we have four subfields.

- **Degree 2:**
  
  $K(\sqrt{\Delta})$ normal;

- **Degree 3:**
  
  $K(\alpha + \beta), K(\alpha\zeta_3 + \beta\zeta_3^2), K(\alpha\zeta_3^2 + \beta\zeta_3)$

  generated by the three roots of $R(x)$.

$\sqrt{b} \notin K$ and $R(x)$ irreducible over $K$ We have that $\text{Gal}\left(\frac{F}{K}\right) \cong C_3 \times S_3$ and we have 12 subfields, see Figures $\mathbb{F}$ and $\mathbb{K}$.
Figure 6: The diagram shows the decomposition of $\mathbb{F}$ into two normal extension of $K$, one of degree three and the other of degree six.

- **Degree 2:**
  \[ K(\sqrt[3]{b}) \text{ normal} ; \]

- **Degree 3:**
  \[ K(\sqrt[3]{b}) \text{ normal} \]
  this is the splitting field of \( x^3 - b \),
  \[ K \left( \sqrt[3]{b}(\alpha + \beta) \right), K \left( \sqrt[3]{b} (\alpha \zeta_3^2 + \beta \zeta_3^2) \right), K \left( \sqrt[3]{b} (\alpha \zeta_3^2 + \beta \zeta_3) \right) \]
  the three roots of \( R(x) \);

- **Degree 6:**
  \[ K \left( \sqrt[3]{b} (\alpha + \beta) \right), K \left( \sqrt[3]{b} \right) \text{ normal} \]
  these extensions are the splitting fields of \( R(x) \) and \((x^3 - b)(x^2 - \Delta)\) respectively,
  \[ K(\alpha), K(\beta) ; \]

- **Degree 9:**
  \[ K (\alpha + \beta), K (\alpha \zeta_3 + \beta \zeta_3^2), K (\alpha \zeta_3^2 + \beta \zeta_3) \]
  again each of three subgroup of \( C_3 \times S_3 \) of order two is the intersection of one non-normal order 6 subgroup with the normal order 6 subgroup.

**References**

[1] G. Butler and J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra, 11 (1983), no. 8, pp. 863–911.

[2] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[3] D. Cox, *Galois theory*, John Wiley & Sons Inc., Hoboken, NJ, 2012, pp. xxviii+570.

[4] A. S. Elsenhans, *Improved methods for the construction of relative invariants for permutation groups*, J. Symbolic Comput., 79 (2017), no. 2, pp. 211–231. 
[5] C. Fieker and J. Klüners, *Computation of Galois groups of rational polynomials*, J. Comput. Math., 17 (2014), no. 1, pp. 141–158.

[6] J. Harrington and L. Jones, *The irreducibility of power compositional sextic polynomials and their Galois groups*, Math. Scand., 120 (2017), no. 2, pp. 181–194.

[7] A. Hulpke, *Techniques for the computation of Galois groups*, Algorithmic algebra and number theory, Springer, Berlin, 1999, pp. 65–77.

[8] L. Soicher and J. McKay, *Computing Galois groups over the rationals*, J. Number Theory, 20 (1985), no. 3, pp. 273–281.

[9] R. Stauduhar, *The determination of Galois groups*, Math. Comp., 27 (1973), pp. 981–996.

[10] N. Sutherland, *Computing Galois groups of polynomials (especially over function fields of prime characteristic)*, J. Symbolic Comput., 71 (2015), pp. 73–97.