The complexity of root-finding in orders.

P. Spelier

Abstract

Given an order, a fundamental problem is deciding whether a univariate polynomial has a zero. It is a special case of deciding whether \( \text{Hom}(A, B) \) is non-empty for two orders \( A \) and \( B \). For fixed separable orders, deciding whether a polynomial has a zero is in \( \mathcal{P} \). If we instead fix a separable polynomial, the problem is \( \text{NP} \)-complete with probability \( 1 \). We provide several theorems about \( \text{NP} \)-completeness, culminating into a complete classification of the problem for quadratic and cubic polynomials. A main ingredient is a new type of algebraic \( \text{NP} \)-complete group-theoretic problems, as seen in \cite{Spe21}.

1 Introduction

An order is a commutative ring \( A \) whose underlying additive group is isomorphic to \( \mathbb{Z}^n \) for some integer \( n \in \mathbb{Z}_{\geq 0} \); this \( n \) is called the rank of that order, denoted by \( \text{rk} A \). After choosing an isomorphism to \( \mathbb{Z}^n \), an order is determined by how the standard basis vectors multiply; we specify an order by listing structure constants \((a_{ijk})_{1 \leq i,j,k \leq n} \in \mathbb{Z}^n \) which describe the multiplication by \( e_i \cdot e_j = \sum_{k=1}^n a_{ijk} e_k \) for the \( \mathbb{Z} \)-basis \( e_1, \ldots, e_n \). Given a polynomial \( f \in \mathbb{Z}[X] \), we denote the zero set of \( f \) in \( A \) by \( Z_A(f) \). This paper treats problems about deciding whether these zero sets are empty or not; specifically, we define the following problems.

Definition 1.1. Let \( f \in \mathbb{Z}[X] \) be a polynomial. Then the problem \( \Pi_f \) is defined as: given as input an order \( A \), determine whether \( Z_A(f) \), is non-empty.

Definition 1.2. Let \( A \) be an order. Then the problem \( \Pi_A \) is defined as: given as input a polynomial \( f \in \mathbb{Z}[X] \), determine whether \( Z_A(f) \) is non-empty.

We use the terminology of polynomial, non-deterministic polynomial, and \( \text{NP} \)-complete problems to classify these problems; we refer to these classes as \( \mathcal{P} \), \( \text{NP} \) and \( \text{NPC} \), respectively. A short treatment of the subject can be found in Appendix A of \cite{Spe21}.

We say a polynomial in \( \mathbb{Z}[X] \) is separable if it is separable over \( \mathbb{Q} \), or equivalently if it has no double roots in \( \overline{\mathbb{Q}} \). If \( f \) is non-separable resp. \( A \) is non-reduced, then we have little to no information about the problems \( \Pi_f \) resp. \( \Pi_A \).
For $f$ separable resp. A reduced, we have more control: the two following theorems show that $\Pi_f$ and $\Pi_A$ are then decidable. In fact, the theorem about $\Pi_A$ tells us exactly what happens for reduced $A$.

**Theorem 1.3.** Let $A$ be a reduced order. Then there is a polynomial time algorithm for $\Pi_A$.

**Theorem 1.4.** Let $f$ be a separable polynomial. Then $\Pi_f$ lies in $\text{NP}$.

This is proven in the beginning of Section 3. The behaviour of $\Pi_f$ varies considerably; for example $\Pi_{X^2+1}$ is in $\mathcal{P}$, while $\Pi_{X^2+X+1}$ is NP-complete (see Theorem 1.7). In general, we have the following conjecture.

**Conjecture 1.5.** Let $f \in \mathbb{Z}[X]$ be separable. Then $\Pi_f$ lies in $\mathcal{P}$ or in $\text{NP}\text{-}\text{C}$.

Ideally, we would like a constructive proof of this statement: an algorithm that tells us for every separable polynomial $f$, whether $\Pi_f$ admits a polynomial time algorithm or is NP-complete. In Section 3 some polynomial time problems are treated, and there are several NP-completeness theorems which work in specific cases. These NP-completeness theorems all have in common that they use a prime dividing the discriminant $\Delta(f)$. We will use the following terminology.

**Definition 1.6.** Let $R$ be any commutative ring, let $f \in R[X]$ be a polynomial, let $a \in R$ and let $k \in \mathbb{Z}_{\geq 0}$. We say that $a$ is a $k$-fold zero (double, triple, \ldots) of $f$ in $R$ if in $R[X]$ we have $(X - a)^k \mid f$. We say that $a$ is a zero of $f$ of multiplicity $k$ in $R$ if $a$ is a $k$-fold zero but not a $(k + 1)$-fold zero.

For the quadratic and cubic case we have proven the conjecture, culminating in the following two theorems (see Lemma 3.5 for the non-monic case).

**Theorem 1.7.** For $f \in \mathbb{Z}[X]$ quadratic monic, we have $\Pi_f \in \mathcal{P}$ if $\Delta(f) = -4$ or $\Delta(f)$ is a square, and $\Pi_f \in \text{NP}\text{-}\text{C}$ otherwise.

This statement is proven in Section 3.1.

**Theorem 1.8.** For $f \in \mathbb{Z}[X]$ cubic monic, we have $\Pi_f \in \mathcal{P}$ if $f$ is reducible, and $\Pi_f \in \text{NP}\text{-}\text{C}$ otherwise.

In Section 3 enough general theorems and ad hoc lemmas are proven to classify all but a small set of cubic polynomials: specifically, Proposition 3.34 tells us that for cubic monic irreducible $f$ with discriminant not of the form $\pm 3^k$ we have $\Pi_f \in \text{NP}\text{-}\text{C}$. In Section 4 we treat the problem of finding all cubic monic polynomials with discriminant of the form $\pm 3^k$; in Theorem 4.1 we eventually find a minimal set $S$ of polynomials such that for every cubic irreducible polynomial $f$ that does not satisfy the conditions of Proposition 3.34 there exists $g \in S$ with $\Pi_f = \Pi_g$. Here equality of problems means that their respective sets of instances coincide, as well as their sets of yes-instances.
Finally, we treat the remaining polynomials from $S$ in Section 5 using ad hoc arguments, thereby completing the proof of Theorem 1.8. An important tool in the NP-completeness proofs is a new family of algebraic problems, classified in [Spe21]. These problems and some theorems will be mentioned in Section 2.

We also take a short look at the case where $f$ is non-separable: in Section 6, we prove the following theorem.

**Theorem 1.9.** If Hilbert’s Tenth Problem over $\mathbb{Q}(i)$ is undecidable, then the problem $\Pi_{(x^2 + 1)^2}$ is undecidable.

This paper is based on the author’s thesis [Spe18].

### 2 Group-theoretic NP-complete problems

We recall the following definitions, remarks and theorems from [Spe21].

**Definition 2.1.** Let $R$ be a commutative ring that is finitely generated as a $\mathbb{Z}$-module, let $G$ be a finite $R$-module and $S$ a subset of $G$. Then define the problem $P_{G,S}^R$ as follows. With input $t \in \mathbb{Z}_{\geq 0}, x_* \in G^t$, the $t$-th Cartesian power of $G$, and $H$ a submodule of $G^t$ given by a list of generators, decide whether $(x_* + H) \cap S^t$ is non-empty. Write $P^R_{G,S}$ for $P_{G,S}^R$.

**Definition 2.2.** Let $R$ be a commutative ring that is finitely generated as a $\mathbb{Z}$-module, let $G$ be a finite $R$-module and $S$ a subset of $G$. Then define the problem $\Pi_{G,S}^R$ as the subproblem of $P_{G,S}^R$ where $x_* = 0$. I.e., with input $t \in \mathbb{Z}_{\geq 0}$ and $H$ a submodule of $G^t$ given by a list of generators, decide whether $H \cap S^t$ is non-empty. Write $\Pi_{G,S}$ for $\Pi^R_{G,S}$.

**Remark 2.3.** If $R$ is not finitely generated as a $\mathbb{Z}$-module, we can replace it by its image in $\text{End}(G)$.

**Remark 2.4.** Note that $R, G, S$ are not part of the input of the problem. In particular, computations inside $G$ can be done in $O(1)$.

Note these problems are certainly in $\mathcal{NP}$, as one can easily give an $R$-linear combination of the generators of the submodule (and add $x_*$ if necessary), and check that it lies in $S^t$. For $R = \mathbb{Z}$, an $R$-module is just an abelian group; there are two theorems that completely classify the problems $P_{G,S}$ and $\Pi_{G,S}$, in the sense that for each problem we either have a polynomial time algorithm or a proof of NP-completeness.

**Definition 2.5.** With $G$ an abelian group and $S \subset G$, we call $S$ a coset if there is some $x \in G$ such that $S - x$ is a subgroup of $G$. 
Theorem 2.6. If $S$ is empty or a coset, then we have $P_{G,S} \in \mathcal{P}$. In all other cases, $P_{G,S}$ is NP-complete.

Theorem 2.7. If $S$ is empty or $\theta(S) := \bigcap_{a \in \mathbb{Z} | aS \subset S} aS$ is a coset, then we have $\Pi_{G,S} \in \mathcal{P}$. In all other cases, $\Pi_{G,S}$ is NP-complete.

Remark 2.8. Note that if $0 \in S$, then $\theta(S) = \{0\}$; additionally, if $G$ is a group with order a prime power and $S$ does not contain $0$, then $\theta(S) = S$, by Lemma 2.15 of [Spe21].

3 General results on NP-completeness of $\Pi_f$

In this section we prove some general results on when $\Pi_f$ is NP-complete. First we will give an algorithm that shows that for reduced orders $A$ we have $\Pi_A \in \mathcal{P}$, which after a slight modification also proves that $\Pi_f \in \mathcal{NP}$ for separable $f \in \mathbb{Z}[X]$ (i.e., those with no double roots in $\mathbb{Q}$). The real work is in the proofs of NP-completeness; we will give a short explanation about the problem in general, including an explanation of when $\Pi_f, \Pi_g$ are equal, some polynomial algorithms and a lemma that allows us to restrict to monic polynomials.

Algorithm 3.1. We take as input $A$ an order, $f \in \mathbb{Z}[X]$ a non-constant polynomial such that either $f$ is separable or $A$ is reduced. The algorithm returns whether $f$ has a zero in $A$.

1. If $f$ is separable, replace $A$ by $A_{\text{sep}}$, the subring consisting of elements of $A$ that are the zero of some separable polynomial in $\mathbb{Z}[X]$, using Algorithm 4.2 of [LS17].

2. Apply Algorithm 7.2 of [LS18] to $E := A \otimes \mathbb{Z} \mathbb{Q}$ to find irreducible polynomials $g_1, \ldots, g_s \in \mathbb{Q}[X]$ with $E \cong \prod_{i=1}^s K_i$ where $K_i = \mathbb{Q}[X]/(g_i)$, together with an isomorphism $\varphi : \prod_{i=1}^s K_i \rightarrow E$.

3. Use the LLL algorithm [Len84] to find $Z_{K_i}(f)$ for every $K_i$.

4. For every $(\alpha_i)_{i=1}^s \in \prod_{i=1}^s Z_{K_i}(f)$, use the isomorphism $\prod_{i=1}^s K_i \rightarrow E$ to compute $\varphi((\alpha_i)_{i=1}^s)$ with respect to the $\mathbb{Z}$-basis $e_1, \ldots, e_{rk A}$ of $A$, and test whether all coefficients are integral. If all coefficients are integral, then $f$ has a zero in $A$; the answer is yes.

5. If no zeroes of $f$ in $A$ were found in the previous step, the answer is no.

Proposition 3.2. The time complexity is

$$O\left( p \left( \text{rk } A \text{ deg } f \log \left( 1 + \sum_{1 \leq i,j,k \leq n} |a_{ijk}| \right) \right) (\text{deg } f)^{|\text{Spec}(A \otimes \mathbb{Q})|} \right)$$

where $p(m) = O(m^\ell)$ for some fixed integer $\ell$. 

4
Proof. The adding of 1 inside the logarithm is done to correctly handle the case \( \text{rk } A = 1 \). The standard operations as multiplication, addition, all take polynomial time in \((1 + \text{rk } A)(1 + \deg f) \log \left( 1 + \sum_{1 \leq i,j,k \leq n} |a_{ijk}| \right)\). Note that the \( s \) we have found in the second step equals \(|\text{Spec}(A \otimes \mathbb{Z} \mathbb{Q})|\), and that in every field of characteristic zero \( f \) has at most \( \deg f \) zeroes, so we check at most \((\deg f)|\text{Spec}(A \otimes \mathbb{Z} \mathbb{Q})|\) candidates. Then for each candidate it takes \( O((\text{rk } A)^2)\) computations to apply \( \varphi \), and time \( O(\text{rk } A) \) to compute whether that zero of \( f \) in \( E \) indeed lies in \( A \).

Remark 3.3. A special case is where \( A \) is a domain, where Algorithm 3.1 always runs in polynomial time.

Proof of Theorem 1.4. We use the definition of \( \mathsf{NP} \) as given in Definition A.5 of \[\text{Spe21}\]. To prove that for \( f \) separable, \( \Pi_f \) lies in \( \mathsf{NP} \), it sufficed to give for each yes-instance \( A \) a certificate \( c(A) \in A \) such that there is an algorithm that given \( A, c \in A \) outputs “yes” if \( c = c(A) \) and “no” if \( A \) is a no-instance, in polynomial time in the size of the input. Note that by encoding \( A \) in \( \mathbb{Z}_{>0} \), this is indeed equivalent to the aforementioned definition. Our algorithm is very short.

1. Calculate whether \( f(c) = 0 \).

If we take \( c(A) \in Z_A(f) \), then Algorithm 3.1 also shows that the size of \( c(A) \) is polynomial in the size of the input, hence our algorithm works in polynomial time. Hence the problem \( \Pi_f \) lies in \( \mathsf{NP} \). □

Remark 3.4. This does not necessarily work for non-separable polynomials, as then we cannot guarantee that if \( Z_A(f) \) is non-empty, it contains a small element.

Lemma 3.5. Let \( f \in \mathbb{Z}[X] \) be non-zero, and let \( f_{\text{mon}} \) be its largest degree monic divisor in \( \mathbb{Z}[X] \). Then \( \Pi_f = \Pi_{f_{\text{mon}}} \).

Proof. It suffices to show for any order \( A \) that \( Z_A(f) \neq \emptyset \) holds if and only if \( Z_A(f_{\text{mon}}) \neq \emptyset \) holds. Obviously, if \( f_{\text{mon}} \) has a zero in \( A \), then so does \( f \). If \( f \) has a zero \( \alpha \) in \( A \), then, as \( A \) is an order, \( \alpha \) is the zero of some monic polynomial \( g \). If we then use again that \( A \) is torsion free, we see that \( \alpha \) is a zero of the monic polynomial \( \gcd(g, f) \). Any monic polynomial that divides \( f \) also divides \( f_{\text{mon}} \), so \( f_{\text{mon}} \) has a zero in \( A \). This in fact proves the stronger statement \( Z_A(f) = Z_A(f_{\text{mon}}) \). □

Definition 3.6. Let \( f, g \in \mathbb{Z}[X] \) be two polynomials. Then we say that \( f \) and \( g \) are equivalent, notation \( f \sim g \), if and only if there exist ring homomorphisms \( \varphi : \mathbb{Z}[X]/(f) \rightarrow \mathbb{Z}[X]/(g), \psi : \mathbb{Z}[X]/(g) \rightarrow \mathbb{Z}[X]/(f) \).
Example 3.7. For any \( f \in \mathbb{Z}[X] \), we have \( f \sim f(\pm X + k) \) with \( k \in \mathbb{Z} \).

Example 3.8. For \( n \in \mathbb{Z}_{\geq 1} \), write \( n = 2^s s \) with \( s \) odd. Then \( X^n + 1 \sim X^{2^r} + 1 \).

Per the functional bijection between \( Z_A(f) \) and \( \text{Hom}(\mathbb{Z}[X]/(f), A) \), the following lemma follows trivially.

**Lemma 3.9.** Let \( f, g \in \mathbb{Z}[X] \) be two monic polynomials. Then \( \Pi_f = \Pi_g \) holds if and only if \( f \) and \( g \) are equivalent.

Now we will treat the few polynomial cases known so far. We start with a rather trivial lemma. Recall that a problem is called trivial if all instances are yes-instances or all instances are no-instances; note that trivial problems always lie in \( \mathcal{P} \).

**Lemma 3.10.** Let \( f \in \mathbb{Z}[X] \) be a polynomial with \( \mathbb{Z}\Phi(f) \neq \emptyset \). Then \( \Pi_f \) is trivial.

**Proof.** By the condition \( \mathbb{Z}\Phi(f) \neq \emptyset \), there is a homomorphism \( \mathbb{Z}[X]/(f) \to \mathbb{Z} \), hence \( \text{Hom}(\mathbb{Z}[X]/(f), A) \) is non-empty for any order \( A \). \( \Box \)

There is one family of polynomials for which a non-trivial polynomial time algorithm is known, as proven in the following theorem.

**Theorem 3.11.** Let \( n \in \mathbb{Z}_{\geq 1} \). Then for \( f = X^n + 1 \) we have \( \Pi_f \in \mathcal{P} \).

**Proof.** A zero of \( f \) is necessarily a root of unity. By Theorem 1.2 of [LS17], we can find a set of generators \( S \) for \( \mu(A) \), the group of roots of unity. Then asking whether \( f \) has a root in \( A \) is asking whether in \( \mu(A) \) the element \( -1 \) is an \( n \)-th power, i.e., if \( -1 \) is in the subgroup generated by \( \{ s^n \mid s \in S \} \). Theorem 1.3 of the mentioned article allows us to compute this in polynomial time, hence this gives a polynomial time algorithm for \( \Pi_f \). \( \Box \)

**Remark 3.12.** Note that we have found a polynomial time algorithm for \( \Pi_{\Phi_n} \) with \( \Phi_n \) the \( n \)-th cyclotomic polynomial, where \( n \) is a power of two. Strangely enough, Theorem 3.15 will tell us that for \( X^2 + X + 1 \), the third cyclotomic polynomial, the problem is NP-complete as \( (X+1)^2 + (X+1) + 1 \equiv X^2 \mod 3 \).

Now we will prove two general theorems that can be used to classify problems \( \Pi_f \) as NP-complete. First we will state a general lemma that we will use multiple times to prove NP-completeness; although it cannot be applied in every proof in Section 3.1 and Section 3.2, the general idea will be used in all proofs.

**Lemma 3.13.** Let \( f \in \mathbb{Z}[X] \) be a polynomial, \( A \) an order, \( \psi : A \to B \) a surjective ring homomorphism with \( B \) finite, \( R \) a subring of \( B \), and \( G \) an \( R \)-module inside \( B \). Assume that \( G \cap R = 0 \) and the multiplication on \( B \) restricted to \( G \times G \) is the zero map. Let \( a \in R \) such that \( \psi(Z_A(f)) = a + S \) with \( S \subset G \). Then \( \Pi_{\psi}^{G,S} \leq \Pi_f \).
Proof. Let \((t, H)\) be an instance of \(\Pi^R_{G,S}\). Note that \(R\) has a unique \(R\)-linear ring homomorphism into \(B^t\), the diagonal map. We write this as an inclusion; in that way, we have \(R[H] \subset B^t\). By the condition that multiplication on \(G\) is the zero map and \(G \cap R = 0\) we have that \(R[H]\), the subring of \(B^t\) generated by \(R\) and \(H\), is (under the condition \(t > 0\)) as an \(R\)-module isomorphic to \(R \oplus H\). Now we see that \(R[H] \cap (a + S^t)\) is in bijection with \(H \cap S^t\), by the map \(x \mapsto x - a\). Let \(A_H \subset A^t\) be the inverse image of \(R[H]\) with respect to the map \(A^t \to B^t\); as \(R[H]\) is a ring, so is \(A_H\). We see that we end up with a surjective map \(Z_{A_H}(f) \to H \cap S^t\). A surjective map has the property that the domain is empty if and only if the codomain is empty, hence \(H \cap S^t \neq \emptyset\) if and only if \(Z_{A_H}(f) \neq \emptyset\). So we produce \(A_H\) as an instance of \(\Pi_f\), completing the reduction. \(\Box\)

Remark 3.14. Note that if \(R = \mathbb{Z} \cdot 1 \subset B\), then an \(R\)-module is just an abelian group \(G\) that satisfies \(|R|G = 0\), with no further structure. Hence then \(\Pi^R_{G,S}\) equals \(\Pi_{G,S}\).

Theorem 3.15. Let \(f\) be a monic irreducible polynomial over \(\mathbb{Z}\) of degree \(n > 1\), and \(p \nmid n\) a prime such that \(f \equiv X^n \mod p\). Then \(\Pi_f\) is NP-complete.

Proof. We will use Lemma 3.13.

Let \(\alpha_1, \ldots, \alpha_n\) be the zeroes of \(f\) in \(\overline{\mathbb{Q}}\), and let \(A\) be the order \(\mathbb{Z}[\alpha_1, \ldots, \alpha_n]\). Let \(I\) be the \(A\)-ideal generated by \(\alpha_1, \ldots, \alpha_n\).

Now let \(B := A/(pA + I^2)\), which is non-zero as \(f \equiv X^n \mod p\), let \(R = \mathbb{F}_p \subset B\), let \(\overline{\alpha}_i\) be the image of \(\alpha_i\) in \(B\), let \(G = \langle \overline{\alpha}_1, \ldots, \overline{\alpha}_n \rangle\), and \(S = \{\overline{\alpha}_1, \ldots, \overline{\alpha}_n\}\).

We will prove that \(\Pi^p_{G,S} = \Pi_{G,S}\) is NP-complete.

As \(G\) is a group with order a power of \(p\), by Theorem 2.7 and Remark 2.8 it suffices to check that \(0 \notin S\) and that \(S\) is not a coset.

By the condition on \(f \mod p\), we see that \(J := I + pA\) is nilpotent in \(A/pA\). As \(A = \mathbb{Z}[I]\) we have \(A/pA = \mathbb{F}_p[J]\). Since \(n > 1\), we have \(\text{rk} A \geq 2\) hence \(|A/pA| \geq p^2\), which implies that \(J \neq \{0\}\). As \(J\) is nilpotent, that implies that \(J^2 \subset J\). So at least one of \(\overline{\alpha}_1, \ldots, \overline{\alpha}_n\) is non-zero, and by the transitivity of the Galois action, all of them are non-zero.

We have to prove that \(S\) is not a coset. Since a coset has \(p\)-power cardinality, it suffices to prove that \(|S| > 1\) and \(|S| \mid n\). Assume \(|S| = 1\). Then in \(B\), we have \(\overline{\alpha}_1 = \cdots = \overline{\alpha}_n\), as \(\alpha_1 + \cdots + \alpha_n \in p\mathbb{Z}\) we have \(n\overline{\alpha}_1 = 0\). We know \(n\) is a unit in \(\mathbb{F}_p\), hence \(\overline{\alpha}_1 = 0\), contradiction. The fact \(|S| \mid n\) follows immediately from the action of the Galois group. As said, we find that \(S\) is not a coset.

Now note that \(G \cdot G = 0\) and \(G \cap \mathbb{F}_p = 0\), so with \(a = 0\) all of the conditions of Lemma 3.13 are satisfied. Together with the NP-completeness of \(\Pi_{G,S}\), this implies that \(\Pi_f\) is NP-complete. \(\Box\)

Proposition 3.16. Let \(f\) be a monic irreducible polynomial over \(\mathbb{Z}\) of degree \(n > 1\) and \(p \mid \Delta(f)\) an odd prime. Let \(A\) be an order with \(\alpha_1, \alpha_2\) two distinct zeroes of \(f\) in \(A\). Further, let \(a \in \mathbb{F}_p\), let \(\mathbb{F}_q = \mathbb{F}_p(a)\) and let \(\psi : \mathbb{Z}[\alpha_1, \alpha_2] \to \mathbb{F}_q[X]/(X^2) = \mathbb{F}_q[\varepsilon]\) be a ring homomorphism such that \(\psi(\alpha_1) = a + \varepsilon\) and
\[\psi(\alpha_2) = a - \varepsilon.\] Finally assume, that we have that \(Z_A(f) = \{\alpha_1, \alpha_2\}\) or we have both that \(Z_{Z[A_1]}(f) = \{\alpha_1\}\) and that all zeroes in \(Z_A(f) \setminus \{\alpha_1, \alpha_2\}\) get sent under \((F_q[c] \to F_q) \circ \psi\) to something different from \(a\). Then \(\Pi_f\) is NP-complete.

**Proof.** We first consider the case that \(Z_A(f) = \{\alpha_1, \alpha_2\}\); we will directly use Lemma 3.13. Let \(B = F_q[c]\), let \(R = F_q\). Now let \(G = cF_q, S = \{\pm \varepsilon\}\). As \(G \cdot G = 0\) and \(G \cap R = 0\), all of the conditions of Lemma 3.13 hold, hence \(\Pi_{G,S}^R \leq \Pi_f\). By Lemma 2.10 of [Spe21] we see that \(\Pi_{G,S}^R\) is NP-complete as \(p > 2\), hence so is \(\Pi_f\).

We now consider the second case; we have to slightly change the proof as we cannot use Lemma 3.13 directly. We still reduce from the problem \(\Pi_{F_q,\{\pm 1\}}^R\), which is NP-complete by Lemma 2.10 of [Spe21]. Let \((t, H)\) be an instance of \(\Pi_{F_q,\{\pm 1\}}^R\). Let \(B = F_q[c]\), let \(R = F_q\), and let \(R_H = R[\varepsilon F_q \times \varepsilon H] \subset B^{t+1}\). Let \(\varphi : \mathbb{Z}[\alpha_1] \times A^t \to B^{t+1}\) be \(\psi\) on every coordinate, and let \(A_H = \varphi^{-1}(R_H)\). We want to find which elements in \(R_H\) are the image under \(\varphi\) of a zero of \(f\). Such an element is of the form \(x + \varepsilon \cdot (y, h)\) with \(x \in R \subset B^t, y \in F_q\) and \(h \in H\). Since \(Z_{\mathbb{Z}[\alpha_1]}(f) = \{\alpha_1\}\), on the first coordinate we must get \(a + \varepsilon, \) meaning \(x = a\) and \(y = 1\). On the last \(t\) coordinates, we then have \(a + \varepsilon h\). By assumption any zero \(\alpha \in Z_A(f) \setminus \{\alpha_1, \alpha_2\}\) is sent under \(\psi\) to \(b + c\varepsilon\) with \(b \neq a\). Hence the fact that \(a + \varepsilon (y, h)\) is the image under \(\varphi\) of some zero of \(f\) in \(A_H\), is equivalent to it lying in the image under \(\varphi\) of some element in \(\{\alpha_1\} \times \{\alpha_1, \alpha_2\}^t\). So we see that \(Z_{A_H}(f)\) is non-empty if and only if \(H \cap S^t\) is non-empty. \(\square\)

For the proof of the second general theorem we first state a definition, following Section 1.6 of [Gio13].

**Definition 3.17.** Let \(R\) be a commutative ring, and fix \(f \in R[X]\) monic of degree \(n\). Then we define \(A_0 = R, f_0 = f\) and recursively for \(0 \leq i < n\) we define \(A_{i+1} = A_i[X_{i+1}]/(f_i(X_{i+1})), \alpha_{i+1} = \overline{X_{i+1}} \in A_{i+1}\) and \(f_{i+1}(X) = \frac{f_i(X)}{X - \alpha_{i+1}}\) as element of \(A_{i+1}[X]\).

We will only use this definition in the case \(R = \mathbb{Z}\). Note that if the Galois group of \(f\) over \(\mathbb{Q}\) is \(S_n\), then \(A_i\) is isomorphic to \(\mathbb{Z}[\beta_1, \ldots, \beta_i]\) where \(\beta_1, \ldots, \beta_n\) are the zeroes of \(f\) in \(\mathbb{Q}\). For any other Galois group, this is never the case for \(i = n\), as the rank of \(A_n\) is \(n!\) while the rank of \(\mathbb{Z}[\beta_1, \ldots, \beta_n]\) is \(|\text{Gal}(f)| < n!\). Furthermore, note that in \(A_i[X]\) we have \(\prod_{j=1}^i (X - \alpha_j) \mid f\), and by Theorem 1.6.7 of [Gio13], the ring \(A_i\) is universal with this property, i.e., in the case \(R = \mathbb{Z}\) we have that \(A_i\) represents the functor from commutative rings to sets \(S \mapsto \{(s_1, \ldots, s_i) \in S^i \mid \prod_{j=1}^i (X - s_j)\text{ divides } f\} \}

**Theorem 3.18.** Let \(f\) be a monic irreducible polynomial over \(\mathbb{Z}\) of degree \(n \geq 2\) with either the Galois group acting triply transitively on \(\mathbb{Z}/(\mathbb{Z}^*)\) or \(n = 2\). Let \(p\) be an odd prime factor of \(\Delta(f)\). If \(n = 3\), assume that \(f\) has a zero of multiplicity 2 modulo \(p\). Then \(\Pi_f\) is NP-complete.
Proof. This proof works by showing that the conditions of Proposition 3.16 hold, where we choose \( a \in \overline{\mathbb{F}}_p \) to be a zero of \( f \) of multiplicity at least 2 (or exactly 2 if \( n = 3 \)). Write \( \mathbb{F}_q \) for \( \mathbb{F}_p(a) \).

First, we construct the map \( \psi \) as needed. Our \( A \) will be \( A_2 \). Let \( \alpha_1, \alpha_2 \) be the roots \( x_1, x_2 \) of \( f \) in \( A_2 \). As \( \text{Gal}(f) \) acts triply transitively on \( \mathbb{Z}_q(f) \) or \( n = 2 \), we have that \( A_2 \) is isomorphic to \( \mathbb{Z}[\alpha, \beta] \) where \( \alpha, \beta \) are any two zeroes of \( f \) in \( \mathbb{Q} \). We use the universal property of \( A_2 \) to construct \( \psi: A_2 \to \mathbb{F}_q[x] \) with \( \psi(\alpha_1) = a + \varepsilon, \psi(\alpha_2) = a - \varepsilon \); the universal property implies that this map exists, since \((X - (a + \varepsilon))(X - (a - \varepsilon)) = (X - a)^2\), which divides \( f \) modulo \( p \) exactly because \( a \) is a double zero of \( f \).

Now, let \( n \neq 3 \). Then the conditions tell us that \( A_2 \) only contains \( \alpha_1, \alpha_2 \) and no other roots of \( f \), which means the conditions for Proposition 3.16 hold. If \( n = 3 \), then as \( f_1 \) is irreducible over \( \mathbb{Z}[\alpha_1] \) we have that \( \mathbb{Z}[\alpha_1](f) = \{\alpha_1\} \), and as \( a \) is a root of multiplicity 2, we can also apply Proposition 3.16. \( \square \)

As a consequence, we have the following theorem on the average behaviour of \( \Pi_f \).

**Theorem 3.19.** Fix \( n \geq 2 \) an integer differing from 3, and let \( f \) be a random monic degree \( n \) polynomial in \( \mathbb{Z}[X] \). Then with probability 1, we have that \( \Pi_f \) is NP-complete.

Proof. Note that with probability 1, the polynomial \( f \) will be irreducible with Galois group \( S_n \). By Minkowski’s theorem, the discriminant will never be a unit. It immediately follows that for \( n \neq 3 \) the only polynomials with Galois group \( S_n \) for which we have not proven NP-completeness yet, are those with discriminant \( \pm 2^k \). Since the discriminant is not of the form \( \pm 2^k \) with probability 1, we see that if the degree \( n \geq 2 \) is fixed, then the problem \( \Pi_f \) is almost surely NP-complete. \( \square \)

**Remark 3.20.** For \( n = 3 \), this result will also hold by Theorem 1.8.

### 3.1 Quadratic polynomials

In this section we will prove Theorem 1.7 by fully treating the quadratic case. Let \( f \in \mathbb{Z}[X] \) be a quadratic monic polynomial. If \( f \) is reducible, then by Lemma 3.10 the problem \( \Pi_f \) is in \( \mathcal{P} \). If \( f \) is irreducible and there is an odd prime dividing \( \Delta(f) \), then we can use Theorem 3.16 or Theorem 3.18 to find that \( \Pi_f \) is NP-complete. The only case that remains is \( f \) irreducible, \( \Delta(f) = \pm 2^k \) with \( k \in \mathbb{Z}_{\geq 0} \). Since an irreducible polynomial of degree \( \geq 2 \) has a prime factor in its discriminant by Minkowski’s theorem, we have \( k \geq 1 \). Hence \( f \) has a double root modulo 2, so the coefficient of \( X \) is even. By translating, we may assume \( f = X^2 - a \), with discriminant \( 4a \).

Hence the only polynomials that remain are of the form \( X^2 - a \) with \( |a| \) a power of 2 and \( a \) not a square. For \( X^2 + 1 \), we have given a polynomial time algorithm in Theorem 3.11. In all other cases, we have \( 2 \mid a \) and we can use the following theorem.
Theorem 3.21. Let \( f = X^2 - a \) with \( 2 \mid a \) and \( a \) not a square. Then \( \Pi_f \) is NP-complete.

Proof. We will reduce from \( \Pi_{\mathbb{Z}/8\mathbb{Z} \{\pm 1\}} \), which is NP-complete by Theorem 2.7.

Let \( A = \mathbb{Z}[\sqrt{a}] \) and \( B = \mathbb{Z}/8\mathbb{Z}[\sqrt{a}], R = \mathbb{Z}/8\mathbb{Z} \subset B \); let \( S \subset B \) be \( \{\pm \sqrt{a}\} \) and \( G = (\mathbb{Z}/8\mathbb{Z}) \cdot \sqrt{a} \subset B \). Now let \((t, H)\) be an instance of \( \Pi_{\mathbb{Z}/8\mathbb{Z} \{\pm 1\}} \), let \( C \) be the \( B \)-algebra \( \{(x_1, \ldots, x_t) \in B^t \mid x_1 \equiv \cdots \equiv x_t \mod 2B\} \). As \( \sqrt{a} \equiv -\sqrt{a} \mod 2B \), we have \( S^t \subset C \). Letting \( H' = H\sqrt{a} \cap C \), we see that \((t, H)\) is a yes-instance if and only if \( H' \cap S^t \) is non-empty. Note that \( H' = ((\sqrt{a}+2B^t) \cap H') \cup (2B^t \cap H') \); if \( H' \subset 2B^t \), this is trivially a no-instance. Otherwise, we see \( H' = (1+2B^t) \cap H' \) hence \( H' \cdot H' \cdot H' \) is generated by elements of the form \( \prod_{i=1}^3 (\sqrt{a} + \sqrt{a}x_i) \) with \( x_1, x_2, x_3 \in 2B^t \) and \( \sqrt{a} + \sqrt{a}x_1, \sqrt{a} + \sqrt{a}x_2, \sqrt{a} + \sqrt{a}x_3 \in H' \). Because \( 4a = 0 \) in \( B \), this product equals \( a\sqrt{a}(1 + x_1 + x_2 + x_3) \). Now using that \( ax_3 = -ax_3 \), we see this equals \( a\sqrt{a}(1 + x_1 + x_2 + x_3) \). This implies that \( H' \cdot H' \cdot H' \) is a subset of \( H' \), which means that \( \mathbb{Z}/8\mathbb{Z}[H'] \) is as an additive group \( \mathbb{Z}/8\mathbb{Z} + H' + H' \cdot H' \), with \( \mathbb{Z}/8\mathbb{Z}[H'] \cap S^t = H' \cap S^t \). Then we define \( A_H \) to be the inverse image of \( \mathbb{Z}/8\mathbb{Z}[H'] \) under the natural map \( A' \to B' \), and we see that \( A_H \) contains a zero of \( f \) exactly if \( H' \cap S^t \neq \emptyset \), completing the reduction.

This concludes the proof of Theorem 3.21.

3.2 Cubic polynomials

In this part we will prove NP-completeness for many monic cubic polynomials. Note that a reducible monic cubic polynomial \( f \) has a zero in \( \mathbb{Z} \), and hence \( \Pi_f \) is trivial according to Lemma 3.10. Therefore we will consider only irreducible monic polynomials. To concisely state our many lemmas, we first state a definition, using the terminology of Definition 3.17.

Definition 3.22. Let \( f \in \mathbb{Z}[X] \) be monic irreducible cubic. We define the \( \mathbb{Z} \)-rank of \( f \), written \( \text{rk}_\mathbb{Z}(f) \), to be the rank of the smallest \( A_1 \) which contains three zeroes of \( f \).

Note that we have \( \text{rk}_\mathbb{Z}(f) = 6 \) if \( f_1 \) is irreducible over \( A_1 \), and \( \text{rk}_\mathbb{Z}(f) = 3 \) otherwise.

If the \( \mathbb{Z} \)-rank of some cubic monic irreducible polynomial \( f \) is 6 and \( \text{Gal}(f) = A_3 \), then one can check that \( A_2 \otimes_\mathbb{Z} \mathbb{Q} \) contains 9 zeroes of \( f \); the following important lemma controls the number of zeroes in \( A_2 \).

Lemma 3.23. Let \( f \) be monic irreducible cubic, with \( \mathbb{Z} \)-rank 6. Then \( f \) has exactly three zeroes in \( A_2 \).

Proof. If \( \text{Gal}(f) = S_3 \), then the statement is trivial, as then \( A_2 \) is isomorphic to \( \mathbb{Z}/\mathbb{Z}[f] \). From now on, assume \( \text{Gal}(f) = A_3 \), with \( \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \langle \sigma \rangle \). Note \( f \) has at least three zeroes \( \alpha_1, \alpha_2, \alpha_3 \) in \( A_2 \), obtained by the construction of \( A_2 \). Let \( \alpha, \beta = \sigma(\gamma), \gamma = \sigma(\beta) \) be the zeroes of \( f \) in \( \mathbb{Q} \), where we pick our algebraic
closure of $\mathbb{Q}$ such that $\alpha = \alpha_1$. Note that $A_2 \otimes \mathbb{Z} \mathbb{Q}$ is naturally isomorphic as an $A_1$-algebra to $\mathbb{Q}(\alpha) \times \mathbb{Q}(\alpha)$, with $\alpha_2 \otimes 1$ being sent to $(\beta, \gamma)$. Under this isomorphism, $A_1 = \mathbb{Z}[\alpha]$ is sent to $\mathbb{Z}[\alpha] \subset \mathbb{Q}(\alpha) \times \mathbb{Q}(\alpha)$ by the diagonal. All in all we have the injections in the following diagram

$$
A_2 = \mathbb{Z}[\alpha, \alpha_2] \hookrightarrow \mathbb{Q}(\alpha) \times \mathbb{Q}(\alpha)
$$

$$
A_1 = \mathbb{Z}[\alpha] \hookrightarrow \mathbb{Q}(\alpha)
$$

Now we define an equivalence relation on the nine zeroes of $f$ in $\mathbb{Q}(\alpha) \times \mathbb{Q}(\alpha)$ by $x \sim y$ if the fields they generate inside $\mathbb{Q}(\alpha) \times \mathbb{Q}(\alpha)$ are the same. The nine zeroes fall into three equivalence classes: the corresponding fields are $\alpha$ and $\psi \in \mathbb{Q} \setminus \mathbb{Z}$ as they are by hypothesis not in $\mathbb{Q}(\alpha) \times \mathbb{Q}(\alpha)$. Specifically, we see that $\alpha_2 \not\sim \alpha$, and hence $\alpha_3 \not\sim \alpha, \alpha_2$ by the symmetry. We claim that of each equivalence class, only one zero lies in $\mathbb{Z}[\alpha, \alpha_2]$. By the symmetry, we only need to prove it for the equivalence class containing $\alpha$, consisting of $(\alpha, \alpha), (\beta, \beta), (\gamma, \gamma)$. Note that $\mathbb{Z}[\alpha, \alpha_2]$ has basis $1, \alpha$ as $\mathbb{Z}[\alpha]$-module and $\mathbb{Q}(\alpha) \times \mathbb{Q}(\alpha)$ has basis $1, \alpha_2$ as $\mathbb{Q}(\alpha)$-module. So $\mathbb{Z}[\alpha, \alpha_2] \cap \mathbb{Q}(\alpha) = \mathbb{Z}[\alpha]$, and hence $\beta, \gamma$ are not in $\mathbb{Z}[\alpha, \alpha_2]$ as they are by hypothesis not in $\mathbb{Z}[\alpha]$. This proves that each equivalence class contains only one zero in $\mathbb{Z}[\alpha, \alpha_2]$, so $\mathbb{Z}[\alpha, \alpha_2] = A_2$ has exactly three zeroes of $f$. 

\[\square\]

**Lemma 3.24.** Let $f \in \mathbb{Z}[X]$ be monic irreducible cubic of $\mathbb{Z}$-rank $6$. If there is a prime $p$ with $p \neq 2$ such that $f$ has a zero of multiplicity $2$ modulo $p$, then $\Pi_f$ is NP-complete.

**Proof.** If $\text{Gal}(f) = S_3$, then this is a special case of Theorem 3.18. For $\text{Gal}(f) = A_3$, we can prove the NP-completeness directly from Proposition 3.10 and Lemma 3.23. We will check the conditions of Proposition 3.10. Write $f \equiv (X - a)^2(X - b) \mod p$ with $a \neq b \mod p$. As in the proof of Theorem 3.18, we take $A = A_2$ and use that $f$ has exactly three zeroes $\alpha_1, \alpha_2, \alpha_3$ in $A$. Then we construct by the universal property of $A$ a ring homomorphism $\psi : A \to \mathbb{F}_3[\varepsilon]$ with $\psi(\alpha_1) = a + \varepsilon$ and $\psi(\alpha_2) = a - \varepsilon$. By $\alpha_1 + \alpha_2 + \alpha_3 = 2a + b$ we have $\psi(\alpha_3) = b$. Also, note that $\mathbb{Z}[\alpha_1](f) = \{\alpha_1\}$ since $f$ has $\mathbb{Z}$-rank $6$. 

\[\square\]

**Lemma 3.25.** Let $f \in \mathbb{Z}[X]$ be monic irreducible cubic. If there is a prime $p$ with $p \neq 3$ and $f \equiv (X - a)^3 \mod p$ for some $a \in \mathbb{F}_p$, then $\Pi_f$ is NP-complete.

**Proof.** Special case of Theorem 3.18. 

\[\square\]

**Lemma 3.26.** Let $f \in \mathbb{Z}[X]$ be monic irreducible cubic of $\mathbb{Z}$-rank $3$. Then there is no prime $p$ such that $f$ has a zero of multiplicity $2$ modulo $p$.

**Proof.** Let $\alpha$ be one of the zeroes of $f$ in $\overline{\mathbb{Q}}$. Note that since $\mathbb{Z}[\alpha]$ already contains the other two zeroes of $f$, the Galois group of $f$ acts on $\mathbb{Z}[\alpha]$. Let $p$ be a rational
prime. We will show that \( \text{Gal}(f) \) acts transitively on the primes above \( p \); if it did not, there would be \( p \mid p, q \mid p \) with \( p, q \) in different \( \text{Gal}(f) \)-orbits. Then using the Chinese remainder theorem, there is an element \( x \) such that \( x \in p \), but not in any \( \sigma(q) \) for \( \sigma \in \text{Gal}(f) \). Then \( N_{K/Q}(x) = \prod_{\sigma \in \text{Gal}(f)} \sigma(x) \) is contained in \( p \) but not in \( q \); but \( N_{K/Q}(x) \in \mathbb{Z} \) and both \( p, q \) have intersection \( (p) \) with \( \mathbb{Z} \), so that is impossible.

Hence, all primes over \( p \) must be isomorphic. In particular \( f \) mod \( p \) factors as a product of polynomials, all of the same degree. We conclude the proof by observing that 2 does not divide 3. \( \square \)

Remark 3.27. This lemma becomes false if one replaces the rank condition by the condition \( \text{Gal}(f) = A_3 \). For example take \( X^3 + 6X^2 - X - 5 \) with discriminant 65\(^2\); modulo 5 this factors as \( X(X + 3)^2 \).

**Proposition 3.28.** Let \( f \in \mathbb{Z}[X] \) be monic irreducible cubic. If \( \Delta(f) \neq \pm 2^k 3^\ell \) with \( k, \ell \in \mathbb{Z}_{\geq 0} \), then \( \Pi_f \) is NP-complete. Further, if \( f \equiv (X - a)^3 \mod 2 \) or \( f \equiv (X - a)(X - b)^2 \mod 3 \) with \( b \not\equiv a \mod 3 \), then \( \Pi_f \) is NP-complete as well.

**Proof.** If \( \Delta(f) \) contains a prime factor \( p > 3 \), then \( f \) has a zero of multiplicity 3 or 2 modulo \( p \). In the first case, \( \Pi_f \) is NP-complete by Lemma 3.25. In the second case, by contraposition of Lemma 3.26 we have \( \text{rk}_2(f) = 6 \) and hence by Lemma 3.24 the problem \( \Pi_f \) is NP-complete.

Furthermore, if \( f \equiv (X - a)^3 \mod 2 \) or \( f \equiv (X - a)(X - b)^2 \mod 3 \) with \( b \not\equiv a \) then we can again use respectively Lemma 3.25 or Lemma 3.26 followed by Lemma 3.24. \( \square \)

**Lemma 3.29.** Let \( f \in \mathbb{Z}[X] \) be monic irreducible cubic such that \( f \) has a zero of multiplicity 2 modulo \( 3 \) and one of multiplicity 3 modulo 3. Then \( \Pi_f \) is NP-complete.

**Proof.** Note that by Lemma 3.26 the \( \mathbb{Z} \)-rank of \( f \) is 6. Let \( A \) be the \( A_2 \) corresponding to \( f \), and let \( \alpha_1, \alpha_2, \alpha_3 \) be the three zeroes of \( f \) in \( A_2 \) given by Lemma 3.26. As in the proof of Theorem 3.13, using that \( f \) has a zero \( a \) of order 2 modulo 2, we find that for any \( t \in \mathbb{Z}_{\geq 0} \) there is a homomorphism \( \varphi : A_1 \times A_1 \to \mathbb{F}_2 \) obtained from applying on each coordinate the morphism \( \psi : A_2 \to \mathbb{F}_2 \) where one sends both \( \alpha_1 \) and \( \alpha_2 \) to \( a \). Then one can check that under \( \psi \) the zero \( \alpha_3 \) is sent to \( a + 1 \). We let \( A' \subset A_1 \times A_1 \) be the inverse image of \( \mathbb{F}_2 \subset \mathbb{F}_2^{\times +1} \); the zeroes of \( f \) in \( A' \) are exactly \( \{(\alpha_1) \times (\alpha_1, \alpha_2)^t \} \). Let \( A' \) be a zero of \( f \) of multiplicity 3 modulo 3 and let \( \psi' \) be the ring homomorphism \( A_2 \to \mathbb{F}_2[t] \) given by \( \psi'(\alpha_1) = a + \epsilon, \psi'(\alpha_2) = a - \epsilon \). We reduce from \( \Pi_{\mathbb{F}_2, \{\pm 1\}} \); letting \((t, H)\) be an instance of \( \Pi_{\mathbb{F}_2, \{\pm 1\}} \) and \( R_H = \mathbb{F}_2[\epsilon \mathbb{F}_2 \times \epsilon H] \) we see that the inverse image of \( R_H \) with respect to \( A' \to \mathbb{F}_2[t] \) contains a zero of \( f \) if and only if \( H \cap \{\pm 1\} \) is non-empty, completing the reduction. As \( \Pi_{\mathbb{F}_2, \{\pm 1\}} \) is NP-complete, this completes the proof. \( \square \)

**Lemma 3.30.** There are no irreducible cubic polynomials with discriminant \( \pm 2^k \) with \( k \in \mathbb{Z}_{\geq 0} \).
Proof. Let \( f \) be such a polynomial — we will derive a contradiction. Let \( \mathbb{Z}[\alpha] = \mathbb{Z}[X]/(f) \) with \( \alpha = \overline{X} \), let \( K = \mathbb{Q}(\alpha) \) and let \( \Delta \) be the discriminant of \( K \) (and note that \( \Delta \) is also a power of 2, up to sign). We now have the following inclusion of fields:

\[
\begin{array}{c}
\mathbb{Q}(\sqrt{\Delta}) \\
\mathbb{K}(\sqrt{\Delta}) \\
K \\
\mathbb{Q}
\end{array}
\]

Using that the Minkowski bound is at least 1 (see for example Corollary 5.10 of [Ste17]), we find \( \Delta \) is in absolute value at least 13. However, the discriminant of \( \mathbb{Q}(\sqrt{\Delta}) \) is one of \( 1, -4, \pm 8 \) (it is 1 exactly if \( \text{Gal}(f) = A_3 \)). From this we will derive a contradiction, using the discriminant of \( \mathbb{K}(\sqrt{\Delta}) \) in between. We do this by looking at the splitting behavior of \( (2) \).

Since \( 2 \mid \Delta \), the prime \( (2) \) ramifies over \( \mathbb{K}/\mathbb{Q} \). We see that in \( \mathcal{O}_K \) either \( (2) = p^3 \) or \( (2) = p^2q \) with \( p \neq q \). In the first case, since then \( p \) ramifies tamely, we have \( 2^2|\Delta \), so \( \Delta = \pm 4 \), contradiction with the upper bound \( |\Delta| \geq 13 \) we found earlier. The other case is a bit more complex. Note that in this case \( f \) has Galois group \( S_3 \) as \( \mathbb{K}/\mathbb{Q} \) is clearly not Galois; in a Galois extension, all ramification indices of a prime over 2 are equal. That \( \mathbb{K}/\mathbb{Q} \) is not Galois implies that the discriminant of \( \mathbb{Q}(\sqrt{\Delta}) \) is not 1, so it is divisible by 2. Hence \( (2) \) factors as \( r^2 \) in \( \mathbb{Q}(\sqrt{\Delta}) \). Since \( K(\sqrt{\Delta})/\mathbb{Q} \) is a Galois extension, we see that in \( K(\sqrt{\Delta}) \) we have \( (2) = (tuv)^2 \) with \( tuv = r \) and \( tu = p \) and \( v^2 = q \). We see that \( K(\sqrt{\Delta})/\mathbb{Q}(\sqrt{\Delta}) \) is unramified, and hence \( \Delta_K(\sqrt{\Delta}) = \Delta^3_{\mathbb{Q}(\sqrt{\Delta})} \). Note we also have \( \Delta_{K(\sqrt{\Delta})} \geq \Delta^2 \). Now we make another small case distinction: if \( \Delta_{\mathbb{Q}(\sqrt{\Delta})} = -4 \), we find \( |\Delta| \leq 8 \), contradiction. If \( \Delta_{\mathbb{Q}(\sqrt{\Delta})} = \pm 8 \), we find \( |\Delta| \leq 22 \), but \( \Delta \) is a power of two with an odd number of factors 2 and it is in absolute value at least 13, and we again arrive at contradiction.

We conclude that there is no cubic number field with discriminant \( \pm 2^k \), so also no irreducible cubic polynomial with such a discriminant.

We again summarise the results in a proposition.

**Proposition 3.31.** Let \( f \in \mathbb{Z}[X] \) be monic irreducible cubic. If \( \Delta(f) \) has a prime factor other than 3 or \( f \) does not have a triple zero modulo 3, then \( \Pi_f \) is NP-complete.

Proof. If \( \Delta(f) \) has a prime factor bigger than 3, the problem is already NP-complete by Proposition 3.28; from now on, assume that it does not have such a prime factor. If \( \Delta(f) \) is divisible by 2, then by contraposition of Lemma 3.30 it is also divisible by 3, and unless \( f \) has a zero of multiplicity 2 modulo 2 and a zero of multiplicity 3 modulo 3, the problem is NP-complete by Proposition 3.28; if we are in that case, we can use Lemma 3.29 to prove NP-completeness.

This proves the first part of the statement.
If \(|\Delta(f)|\) is a power of 3, then it is divisible by 3 by the Minkowski bound \(\lfloor \Delta(f) \rfloor \geq 13\). If it does not have a triple zero modulo 3, it must have a zero of multiplicity 2, which means that the problem is NP-complete by Proposition 3.28.

We finish this section with two lemmas that tell us what happens if the polynomial has a triple zero modulo a power of 3, for the \(\mathbb{Z}\)-rank 6 and 3 cases separately.

**Lemma 3.32.** Let \(f \in \mathbb{Z}[X]\) be monic irreducible cubic with \(\mathbb{Z}\)-rank 6 with a triple root modulo 9. Then \(\Pi_f\) is NP-complete.

**Proof.** Assume by translation that \(f \equiv X^3 \mod 9\). Let \(B = (\mathbb{Z}/9\mathbb{Z})[\omega, \varepsilon]\), where \(1 + \omega + \omega^2 = 0\) and \(\varepsilon^2 = 0\). Let \(R = \mathbb{Z}/9\mathbb{Z}\) and let \(a = 0\). Letting \(\alpha_1, \alpha_2, \alpha_3\) be the three zeroes of \(f\) in \(A_2\) (guaranteed by Lemma 3.23), we use the universal property of \(A_2\) to give a map \(A_2 \to R\) sending \(\alpha_1\) to \(\varepsilon\) and \(\alpha_2\) to \(\omega\varepsilon\) and \(\alpha_3\) to \(\omega^2\varepsilon\). Taking \(R = \mathbb{Z}/9\mathbb{Z} \subset R\) and \(G = \mathbb{Z}/9\mathbb{Z}[\omega, \varepsilon]\), we can now reduce from the problem \(\Pi_{\mathbb{Z}/9\mathbb{Z}[\omega, \varepsilon]}\) this problem is NP-complete by Theorem 2.7.

**Lemma 3.33.** Let \(f \in \mathbb{Z}[X]\) be monic irreducible cubic with \(\mathbb{Z}\)-rank 3. Then \(f\) does not have a triple root modulo 27.

**Proof.** We will argue by contradiction. Let \(f\) be as in the conditions, and assume by translating that \(f\) has 0 as a triple root modulo 27. Let \(\alpha, \beta, \gamma\) be the zeroes of \(f\) in \(\mathbb{Q}\). We define \(R := \mathbb{Z}[\alpha]/(27) \cong (\mathbb{Z}/27\mathbb{Z})[\eta]\) where \(\eta^3 = 0\). As \(f\) splits as \((X - \alpha)(X - \beta)(X - \gamma)\) in \(\mathbb{Z}[\alpha]\), we find that \(X^3\) totally splits over \(R\) with one of the factors being \(X - \eta\). It can be seen that if \(X^3\) factors over \(R\) as \((X - \eta)(X - a)(X - b)\) then \((X - a)(X - b) = X^2 + \eta X + \eta^2\). Since \(X^2 + \eta X + \eta^2\) splits over \(R\), the discriminant \(-3\eta^2\) is a square of \(R\). Let \(x \in R\) be such that \(-3\eta^2 = x^2\) (in fact, we can take \(x = a - b\)). Let \(m = (3, \eta)\) be the maximal ideal in \(R\). We see \(-3\eta^2 \in m^3 \setminus m^4\), hence \(x \in m \setminus m^2\). But if \(3u + v\eta\) is an element of \(m \setminus m^2\), then \(u\) or \(v\) is a unit, and in both cases the square is in \(m^2 \setminus m^3\) as \(9, 3\eta, \eta^2\) form a basis of the \(\mathbb{F}_3\) vector space \(m^2/m^3\). This means that \(-3\eta^2\) is not a square, contradiction, so no such \(f\) exists.

These lemmas all together give us the following proposition.

**Proposition 3.34.** Let \(f\) be monic irreducible cubic. Then \(\Pi_f\) is NP-complete if at least one of the following conditions holds:

- \(\Delta(f)\) has a prime factor other than 3;
- \(f\) does not have a triple zero modulo 3;
- \(\text{rk}_\mathbb{Z}(f) = 6\) and \(f\) has a triple zero modulo 9;
- \(f\) has a triple zero modulo 27.
Proof. This proposition consists of four statements; the first two are given by Proposition 3.31, the third by Lemma 3.32, and the fourth by the contraposition of Lemma 3.33 followed by Lemma 3.32. □

4 Cubic polynomials with discriminant \( \pm 3^\ell \)

In the previous section we have proven that for any cubic monic irreducible polynomial \( f \in \mathbb{Z}[X] \) whose discriminant has a prime factor that is not 3, the problem \( \Pi_f \) is NP-complete. This motivates the following theorem; the exact conditions of the theorem complement Proposition 3.34, in the sense that if \( f \) cubic monic irreducible does not satisfy these conditions, then it holds that \( \Pi_f \in \text{NP} \) by Proposition 3.34. We refer to Definitions 3.22 and 3.6 for the definitions of \( \mathbb{Z} \)-rank and equivalence of polynomials respectively.

Theorem 4.1. Let \( f \in \mathbb{Z}[X] \) be monic irreducible cubic, with discriminant of the form \( \pm 3^k \) with \( k \in \mathbb{Z}_{\geq 0} \). Assume that \( f \) has a zero of multiplicity 3 modulo 3, and not a triple zero modulo 27. Also, assume that if the \( \mathbb{Z} \)-rank is 6, then \( f \) does not have a triple zero modulo 9. Then \( f \) is equivalent to one of the polynomials in Table 4.2.

For the proof of Theorem 4.1, we first state a definition and a trivial lemma about integral points on a family of elliptic curves. Throughout the rest of the section, we take \( S = \{3\} \), and denote the \( S \)-integers \( \mathbb{Z}_S \) as \( \mathbb{Z}_S \).

Definition 4.2. Let \( a \in \mathbb{Z} \setminus \{0\} \). Then \( C_a \) is the elliptic curve given by the equation \( y^2 = x^3 + a \).

Lemma 4.3. Let \( a,k \in \mathbb{Z} \). Then there is a bijection \( C_a(\mathbb{Q}) \to C_{ak^6}(\mathbb{Q}) \) given by \( (x,y) \mapsto (k^2 x, k^3 y) \); if \( k \) is a power of 3, this induces a bijection \( C_a(\mathbb{Z}_S) \to C_{ak^6}(\mathbb{Z}_S) \).

Proof. Both statements follow immediately from the calculation
\[
(k^3 y)^2 - (k^2 x)^3 - k^6 a = k^6 (y^2 - x^3 - a).
\]

Proof of Theorem 4.1. Let \( f \) be a cubic irreducible polynomial with discriminant \( \pm 3^\ell \) with \( \ell \geq 1 \), satisfying the conditions of the theorem. Since \( f \) has a triple zero modulo 3, the coefficient corresponding to \( X^2 \) is divisible by 3. Hence we can put \( f \) into the form \( X^3 + pX + q \) with \( p,q \in \mathbb{Z} \) by translation.

Now \( \Delta(f) \) has the simple formula \( -4p^3 - 27q^2 \). Setting \( -4p^3 - 27q^2 = \pm 3^\ell \), we find a family of elliptic-curve-like diophantine equations. Multiplying such an equation by \( 2^3 3^3 \), and substituting \( x = -2^3 3p, y = 2^2 3^3 q \), we find the equation
\[
C_{\mp 2^3 3^4} : y^2 = x^3 \mp 2^4 3^{3\ell}
\]
with \( \ell' = \ell + 3 \). To find all possible polynomials up to equivalence, it
suffices to find all integral points \((x, y)\) on one of these curves. Lemma 4.3 will
us do even more: we can parametrise all points on \( \bigcup_{s \geq 0, \pm 1} C_{s \pm 3s'}(\mathbb{Z}_S) \) by
\( \bigcup_{6 > \ell \geq 0, \pm 1} C_{s \pm \ell'}(\mathbb{Z}_S ) \times \mathbb{Z}_{\geq 0} \). Now theorem 4.3 of [Silo9] tells us there are
only finitely many \( S \)-integral points on the curves \( C_{s \pm \ell'} \) with \( 0 \leq \ell < 6 \). The
author used Sage [Sag18] to explicitly find these points. The list of parametrised
polynomials up to the transformation \( f(X) \mapsto -f(-X) \) can be seen in Table 4.1. The reducible polynomials are those with Galois group of cardinality 1 or 2. Next to the irreducible polynomials are the values of
\( \ell \). The irreducible polynomials are the values of \( t \) that the polynomial has integral coefficients. Now we observe that all polynomials have a triple root modulo 9 and
als have a triple root modulo 27 for \( t \) that the polynomial has integral coefficients. Now we observe that all polynomials have a triple root modulo 9 and
\( Z \)-rank 6. This almost give the final Table 4.2, it only remains to observe that \( X^3 - 3X + 1 \sim X^3 - 21X + 37 \), as for \( f \in \{ X^3 - 3X + 1, X^3 - 21X + 37 \} \) we have that \( \mathbb{Z}[X]/(f) \) is the ring of integers
of \( \mathbb{Q}(\zeta_9 + \zeta_9^{-1}) \) where \( \zeta_9 \) is a primitive ninth root of unity; \( \zeta_9 + \zeta_9^{-1} \) is a zero of
\( X^3 - 3X + 1 \), and \( 3(\zeta_9 + \zeta_9^{-1})^2 + \zeta_9 + \zeta_9^{-1} - 6 \) is a zero of \( X^3 - 21X + 37 \).
Furthermore, note that the three polynomials in Table 4.2 are pairwise non-
equivalent, as all of the discriminants are different.

| Polynomial | Cardinality of Galois group | All \( t \in \mathbb{Z}_{\geq 0} \) for which the polynomial is integral |
|------------|----------------------------|---------------------------------|
| \( X^3 - 1/2 \cdot 3^{2t} X + 1/27 \cdot 3^{3t} \) | 3 | \( \geq 1 \) |
| \( X^3 - 73/108 \cdot 3^{2t} X + 595/2916 \cdot 3^{3t} \) | 1 | - |
| \( X^3 - 7/9 \cdot 3^{2t} X + 37/27 \cdot 3^{3t} \) | 3 | \( \geq 1 \) |
| \( X^3 - 3^{2t} X + 1/3 \cdot 3^{3t} \) | 3 | \( \geq 1 \) |
| \( X^3 - 193/12 \cdot 3^{2t} X + 2081/108 \cdot 3^{3t} \) | 2 | - |
| \( X^3 + 1/27 \cdot 3^{3t} \) | 2 | \( \geq 1 \) |
| \( X^3 - 1/12 \cdot 3^{2t} X + 7/108 \cdot 3^{3t} \) | 6 | - |
| \( X^3 + 1/9 \cdot 3^{3t} \) | 6 | \( \geq 1 \) |
| \( X^3 + 2/3 \cdot 3^{2t} X + 7/27 \cdot 3^{3t} \) | 2 | \( \geq 1 \) |
| \( X^3 + 1/3 \cdot 3^{3t} \) | 6 | \( \geq 1 \) |
| \( X^3 - 3 \cdot 3^{2t} X + 5/12 \cdot 3^{3t} \) | 6 | - |
| \( X^3 - 6 \cdot 3^{2t} X + 17/24 \cdot 3^{3t} \) | 6 | \( \geq 1 \) |

Table 4.1: A list containing all monic cubic polynomials in \( \mathbb{Z}[X] \), up to the
substitution \( f(X) \mapsto -f(-X) \), that have a triple zero modulo 3 and discriminant
of the form \( \pm 3^k \), together with the Galois group.
5 NP-completeness for difficult cubic polynomials

In this section we prove NP-completeness for the problems $\Pi_f$ with $f$ in Table 4.2 at the end concluding the proof of Theorem 4.8.

Lemma 5.1. Let $f = X^3 − 3$. Then $\Pi_f$ is NP-complete.

Proof. Let $\alpha, \beta, \gamma$ be the three zeroes of $f$ in $\overline{Q}$. Let $B$ be the finite ring $\mathbb{Z}/9\mathbb{Z}[\pi] := \mathbb{Z}/9\mathbb{Z}[X]/(X^3 + 3)$. Note $B$ has a $\mathbb{Z}/3\mathbb{Z}$-grading $B = B_0 \oplus B_1 \oplus B_2$ with $B_i = \pi^i \mathbb{Z}/9\mathbb{Z} \oplus \pi^{i+3} \mathbb{Z}/9\mathbb{Z}$. We denote $\zeta := −\frac{1}{4} + \frac{1}{4}\pi^3$; observe that $\zeta^2 + \zeta + 1 = 0$. In this ring, $X^3 − 3$ has a factorisation as $(X + \pi^2)(X + \zeta^2)(x + \zeta^2)$. As $\text{Gal}(f) = S_3$, the order $A := \mathbb{Z}[\alpha, \beta, \gamma]$ is naturally isomorphic to to $A_2$. Then by the universal property of $A_2$, we have a morphism $\psi : A \to B$ given by $\psi(\alpha) = −\pi^2, \psi(\beta) = −\zeta^2, \psi(\gamma) = −\zeta^2\pi^2$. Letting $S = \{\psi(\alpha), \psi(\beta), \psi(\gamma)\}$, we note $S \subset B_2$. We define $G = B_2$. Note that $S$ is not a coset in $G$ and does not contain zero. By Theorem 2.7 and Lemma 2.8 this means $\Pi_G, S$ is NP-complete.

We will give a reduction $\Pi_{G,S} \leq \Pi_f$. Let $(t, H)$ be an instance of $\Pi_{G,S}$. Let $C$ be the subring of $B^t$ given by $C = \{(x_1, \ldots, x_t) \in B^t | x_1 \equiv \cdots \equiv x_t \mod \zeta − 1\}$. Note $S^t \subset C$, as $\psi(\alpha) \equiv \psi(\beta) \equiv \psi(\gamma) \mod \zeta − 1$. Let $H'$ be $H$ intersected with $C$. We may assume $H'$ is not contained in $(\zeta − 1)B^t$; if it is, clearly $H' \cap S^t = \emptyset$. Note that in $B_2/(\zeta − 1)B_2$ we have $\pi^2(\zeta − 1) = 3\pi^2 + 5\pi^5 = 0$ and $\pi^5(\zeta − 1) = −3\pi^2 + 3\pi^5 = 0$. We deduce that $B_2/(\zeta − 1)B_2 = \{0, \pi^2, 2\pi^2\}$. Writing $H' = \langle H' \cap (\pi^2 + (\zeta − 1)\pi^2 B_0') \rangle \cup \langle H' \cap (\pi^2 + (\zeta − 1)\pi^2 B_0') \rangle$, we see $H' = \langle H' \cap (\pi^2 + (\zeta − 1)\pi^2 B_0') \rangle$. That means that $H' \cdot H' \cdot H' \cdot H'$ is generated by elements of the form $\prod_{i=1}^4(\pi^2 + (\zeta − 1)\pi^2 x_i)$ with $x_i \in B_0, \pi^2 + (\zeta − 1)\pi^2 x_i \in H'$ for $i = 1, \ldots, 4$. Using that $\pi^2 = −3$ and that the exponent of $B$ equals 9, we see that the product equals $−3\pi^2 \left(1 + \sum_{i=1}^4 x_i(\zeta − 1)\right)$, which equals $−3\sum_{i=1}^4(\pi^2 + (\zeta − 1)\pi^2 x_i) \in H'$. Hence $H' \cdot H' \cdot H' \cdot H' \cap H'$, meaning that $\mathbb{Z}/9\mathbb{Z}[H']$ is equal to $\mathbb{Z}/9\mathbb{Z} + H' + H' \cdot H' + H' \cdot H' \cdot H' \cdot H'$, meaning that $\mathbb{Z}/9\mathbb{Z}[H']$ is equal to $\mathbb{Z}/9\mathbb{Z} + H' \cap S^t$ hence equals $H'$ itself. Now we can define $A_H$ to be the inverse image under $A^t \to B^t$ of $\mathbb{Z}/9\mathbb{Z}[H']$, and we see $Z_f(A_H)$ is non-empty exactly if $H \cap S^t$ is non-empty. This completes the reduction. □

| Polynomial      | Discriminant | Factorisation of discriminant |
|-----------------|--------------|------------------------------|
| $X^3 − 3$      | −243         | $−3^5$                       |
| $X^3 − 3X + 1$ | 81           | $3^4$                        |
| $X^3 − 9X + 9$ | 729          | $3^6$                        |
Lemma 5.2. Let $f = (X - 1)^3 - 3(X - 1) + 1 = X^3 - 3X^2 + 3$. Then $\Pi_f$ is NP-complete.

Proof. Let $R$ be the ring $\mathbb{F}_3[x] = \mathbb{F}_3[x]/(x^2)$, and let $G$ be a free $R$-module of rank 1, with generator $m$. Let $S = \{0, m, -m - \varepsilon m\} \subseteq G$. Note that $P^R_{G,S}$ is NP-complete, as by Lemma 2.6 of [Spe21] with $\varphi : x \mapsto m - x$ we have $P^R_{G,\{0,m\}} \leq P^R_{G,S}$, and by Lemma 2.10 we know $P^R_{G,\{0,m\}}$ is NP-complete. Now we define a new problem $P$: the input is $t \in \mathbb{Z}_{>0}$, a sub-$R$-module $H$ of $G^t$ and $x_\ast \in G^t$ with $(m, \ldots, m) - \varepsilon x_\ast \in H$; the output is whether $(x_\ast + H) \cap S^t$ is non-empty. Obviously, $P \leq P^R_{G,S}$. We will also prove $P^R_{G,S} \leq P$. Let $(t, H, x_\ast)$ be an instance of $P^R_{G,S}$. For ease of notation, from now on we write $\varphi$ for a vector consisting of all $x'_s$. Let $t' = t + 1$, $H' = H \times \{0\} + R \cdot (m - \varepsilon (x_\ast, 0))$ and $x'_\ast = (x_\ast, 0)$. Then $(t', H', x'_\ast)$ is an instance of $P$. If $(t, H, x_\ast)$ is a yes-instance of $P^R_{G,S}$ with $h \in H$ such that $h + x_\ast \in S^t$, then $(h, 0) \in H'$ and $(h, 0) + (x_\ast, 0) \in S^{t'}$, so $(t', H', x'_\ast)$ is a yes-instance of $P$. Conversely, if $(t', H', x'_\ast)$ is a yes-instance of $P$, then there is an $h' \in H'$ with $h' + (x_\ast, 0) \in S^{t'}$. By looking at the last coordinate, we see that $h'$ can be written as $(h, 0) + v(m - \varepsilon (x_\ast, 0))$ with $h \in H, v \in R$. Note that $\sigma : G \to G, x \mapsto (1 + \varepsilon)(x - m)$ gives a bijection on $S$ which cycles $S$. If we also denote $\sigma$ for the map $G^{t'} \to G^t$ that applies $\sigma$ coordinatewise, we see that $\sigma(x'_\ast + H') = x'_\ast + (1 + \varepsilon)(m - \varepsilon x'_\ast)$ which implies that $\sigma(x'_\ast + H')$ lies in $x'_\ast + H'$. Then clearly $\sigma$ also acts on $(x'_\ast + H') \cap S^{t'}$. Therefore without loss of generality $(h, 0) + v(m - \varepsilon (x_\ast, 0)) + (x_\ast, 0)$ is zero on the last coordinate, meaning $v = 0$. Then $(h, 0) + (x_\ast, 0) \in S^{t'}$ hence $h + x_\ast \in S^t$, so we find $(t, H, x_\ast)$ is a yes-instance of $P^R_{G,S}$. We have now proven that $P \approx P^R_{G,S}$, so we have $P \in \text{NP}$.

We will now reduce from $P$ to $\Pi_f$. Let $\alpha$ be a zero of $f$ in $\mathbb{Q}$, and note that with $A := \mathbb{Z}[\alpha]$ we have $Z_A(f) = \{\alpha, \alpha^2 - 2\alpha, \alpha - \alpha^2 + 3\}$. Let $p$ be the prime ideal in $A$ over 3 generated by $\alpha$; then (3) factorises as $p^3$. Define $B = A/p^4$. Note that as $-3 = \alpha^2(\alpha - 3)$ we have $-3 = \alpha^3$ in $B$. Finally, note that $Z_A(f)$ can be written as $\alpha + \{0, \alpha^2 - 3\alpha, -\alpha^2 + 3\}$ where $\{0, \alpha^2 - 3\alpha, -\alpha^2 + 3\}$ is a subset of $p^2$, and modulo $p^4$ it is equal to $\{0, \alpha^2, -\alpha^2 - \alpha^3\}$. This means the image of $Z_A(f)$ in $B$ is $\alpha + \{0, \alpha^2, -\alpha^2 - \alpha^3\}$.

We take $m$, the generator of $G$, to be $\alpha^2 \in B$, with $\varepsilon \in R$ acting on $G$ as multiplication by $\alpha$. Let $(t, H, x_\ast)$ be an instance of $P$. Now define $R_H \subset B^t$ as $\mathbb{Z}/9\mathbb{Z} + \mathbb{Z}/3\mathbb{Z}(\alpha + x_\ast) + H$. Note that this is in fact a ring; the only non-trivial requirement is that $(\alpha + x_\ast)^2 \in R_H$, but $(\alpha + x_\ast)^2 = \alpha^2 + 2\alpha x_\ast = m - \varepsilon x_\ast$, which is an element of $H$ by definition of the problem $P$. Also, note that $x_\ast \in R_H$ is $-\alpha^3$, and $\alpha^3 = \varepsilon(m - \varepsilon x_\ast) \in H$. This tells us that $R_H \cap G^t = H$. Now we see that $(\alpha + S^t) \cap R_H = (\alpha + x_\ast) + (-x_\ast + S^t) \cap R_H$ is in bijection with the set of $\mathbb{Z}^t$-subsets of $H$. As $\alpha + S$ is the image of $Z_A(f)$ in $B$, we see $Z_f(A_H)$ is non-empty exactly if $(x_\ast + H) \cap S^t$ is non-empty. This completes the reduction.

Lemma 5.3. Let $f = X^3 - 9X + 9$. Then $\Pi_f$ is NP-complete.

Proof. Let $\alpha$ be a zero of $f$ in $\mathbb{Q}$, and note that with $A = \mathbb{Z}[\alpha]$ we have $Z_A(f) =$
{α, α + α² - 6, -2α - α² + 6}. Let \( B = A/(9, 3α²) \), \( R = \mathbb{Z}/9\mathbb{Z} \subset B \). We see \( B \) is a ring of cardinality 3⁹, generated as an additive group by 1, \( α, α² \) of order 9, 9, 3 respectively. To prove NP-completeness, let \( G = (α² + 3) \subset B \). This is a group of cardinality 3. Let \( S = \{±(α² + 3)\} \subset G \). Note that \( S \) is not a coset and does not contain 0, so \( Π_{G,S} \) is NP-complete. We will reduce from this problem to \( Π_f \). Let \( (t, H) \) be an instance of \( Π_{G,S} \). Write \( T \) for the image of \( Z_A(f) \) in \( B \).

Let \( t' = 2t + 1 \). Let \( t' = \{ (x, -x, 0) \mid x \in H \} \subset B'^t \). Let \( x_1 = (α - (α² + 3), α) \), and let \( R_H = R[H', x_1] \). Note that as an additive group, this is generated by \( \mathbb{Z}/9\mathbb{Z}, H', x_1, x_1², H' x_1 \). We see \( x_1 \) and \( x_1² \) have order 9 and 3 respectively.

Claim: \( R_H \cap T'^t \) is non-empty if and only if \( H \cap S^t \) is non-empty. We prove this by examining an element \( x \in R_H \cap T'^t \). Let \( σ : B → B, x → x² + x + 3 \) and \( τ : B → B, x → -2x - (x² + 3) \) be two maps, and note that by virtue of the Galois group still acting on \( T \), we have that \( σ, τ \) induce transitive permutations on \( T \), and \( σ|_T = τ|_T \). Denoting by \( σ \) and \( τ \) the two maps \( B' → B' \) that coordinatewise perform \( σ \) respectively \( τ \) it is clear that \( σ(R_H), τ(R_H) \) are subsets of \( R_H \), as \( R_H \) is a ring. This tells us that \( σ(x), τ(x) \) also lie in \( R_H \cap T'^t \). Letting \( π : B' → B \) denote the projection onto the last coordinate, we see that this means that \( R_H \cap T'^t \) is non-empty if and only if \( R_H \cap T'^t \cap π^{-1}(α) = x_1 \) is non-empty.

As \( π(1) = 0 \), we have that \( π(R_H) = π(\mathbb{Z}/9\mathbb{Z} + \mathbb{Z}/9\mathbb{Z} x_1 + \mathbb{Z}/3\mathbb{Z} x_1²) \). As \( π(1) = 1, π(x_1) = α, π(x_1²) = α² \) we see that \( R_H \cap π^{-1}(α) = x_1 + H' + H' x_1 \). Finally, it will prove that \( (x_1 + H' + H' x_1) \cap T'^t \) is non-empty if and only if \( H \cap S^t \) is non-empty. Note that \( x_1 + H' + H' x_1 \) contains an element of \( T'^t \) if and only if there are \( h_1, h_2 \in H' \) with \( x_1 + h_1 + h_2 x_1 \in T'^t \). Writing \( h_1 = (x, -x, 0) \) and \( h_2 = (y, -y, 0) \) with \( x, y \in H \), this is equivalent to \( (x, -x) + (y, -y)(α - (α² + 3)) \in \{±(α² + 3), -3α²\}² \). As \( (α³ + 3)\mathbb{G} = 0 \), we can write \( (x, -x) + (y, -y)(α - (α² + 3)) = (x, -x) + α(y, -y) \) with \( α\mathbb{G} = (3α) \). Then we see that \( (y, -y) \) is an element of \( (0, -((α² + 3))²)² \), implying \( y = 0 \). So we find \( R_H \cap T'^t \neq ∅ ⇔ ∃ x \in H : (x, -x) \in \{±(α² + 3)\}² \). This is clearly equivalent to \( H \cap S^t \neq ∅ \), proving the claim.

That means that we have constructed a subring \( R_H \subset B'^t \) such that \( R_H \cap T'^t \neq ∅ ⇔ H \cap S^t \neq ∅ \) holds. Letting \( A_H \) be the inverse image of \( R_H \) under the natural map \( A'^t → B'^t \), we have completed the reduction.

**Proof of Theorem 4.13** Let \( f \in \mathbb{Z}[X] \) be cubic, monic. By Lemma 3.10 we have \( Π_f \in Π_f \) if \( f \) is irreducible. Assume that \( f \) is irreducible. If it satisfies the conditions of Proposition 3.34 then \( Π_f \) is NP-complete by that proposition. Otherwise, it satisfies the conditions of Theorem 4.11 and hence is equivalent to one of the three polynomials in Table 4.2. For those three polynomials NP-completeness has been proven in this section. This completes the proof.

**6 An undecidability result**

In this section we prove the undecidability of \( Π_{\mathbb{Q}(i)} \), contingent on the undecidability of Hilbert’s Tenth Problem over \( \mathbb{Q}(i) \). We first give a short definition
Definition 6.1. We define \( \text{HTP}(R, S) \) with \( R \) a ring and \( S \subset R \) to be: given an \( n \in \mathbb{Z}_{\geq 1} \) and a set of polynomials \( P \) in \( R[X_1, \ldots, X_n] \), determine whether the polynomials in \( P \) have a common zero in \( S^n \). We write \( \text{HTP}(R) \) for \( \text{HTP}(R, R) \).

We start by rewriting \( \text{HTP}(\mathbb{Q}(i)) \) with the following definition and theorem.

Definition 6.2. We define \( v : \mathbb{Q}(i) \to \frac{1}{2}\mathbb{Z} \cup \{\infty\} \) as the extension of the 2-adic valuation on \( \mathbb{Q} \) with \( v(2) = 1 \). Write \( A \) for the ring of \((1+i)\)-adic Gaussian integers.

Theorem 6.3. The problem \( \text{HTP}(\mathbb{Q}(i)) \) is equivalent with \( \text{HTP}(\mathbb{Q}(i), A^*) \).

Proof. We prove the reduction \( \text{HTP}(\mathbb{Q}(i), A^*) \leq \text{HTP}(\mathbb{Q}(i)) \) by separably proving \( \text{HTP}(\mathbb{Q}(i), A^*) \leq \text{HTP}(\mathbb{Q}(i), A) \) and \( \text{HTP}(\mathbb{Q}(i), A) \leq \text{HTP}(\mathbb{Q}(i)) \). For the first one, we can model a unit of \( A \) by adding for every variable \( X_j \) occurring the polynomial \( X_jY_j = 1 \). For the second reduction, we use Lemma’s 6, 9 and 10 of [Rob59]. Let \( p = (1+i) \), and let \( q_1, q_2 \) be two different primes in the inverse ideal class of \( p \) with \( q_1, q_2 \) all distinct (this is possible by Lemma 6 of the article), and let \( a_1, a_2 \) be such that \( (a_j) = p q_j \) for \( j = 1, 2 \). Let \( b_1, b_2 \) be as given by the proof of Lemma 9. Then by Lemma 10, the equation \( 1 - a_1 b_j c_j^2 = x^2 - a_j y^2 - b_j z^2 \) has a solution in \( x, y, z \) if and only if \( c_j \) is a \( p \)-adic and a \( q_j \)-adic integer. Since \( q_1, q_2 \) are distinct, the equations \( c = c_1 + c_2, 1 - a_1 b_1 c_1^2 = x_1^2 - a_1 y_1^2 - b_1 z_1^2, 1 - a_2 b_2 c_2^2 = x_2^2 - a_2 y_2^2 - b_2 z_2^2 \) model that \( c \) is a \((1+i)\)-adic integer. This completes the inequality \( \text{HTP}(\mathbb{Q}(i), A^*) \leq \text{HTP}(\mathbb{Q}(i)) \).

For the inequality \( \text{HTP}(\mathbb{Q}(i)) \leq \text{HTP}(\mathbb{Q}(i), A^*) \), note that the expression \( \frac{x+y}{x^2+y^2} \) takes on every value in \( \mathbb{Q}(i) \) for \( x, y, z \in A^* \); this is clear from \( A^* + A^* = A \) and the fact that \(-7\) is 2-adically a square, implying that \( z^2 + 7 \) can have arbitrarily small valuations. That means that we can replace each variable \( X_i \) by \( \frac{x_i+y_i}{x_i^2+y_i^2} \), clearing out denominators, to find an equivalent system of equations for the problem \( \text{HTP}(\mathbb{Q}(i), A^*) \). \( \square \)

We first slightly alter the definition of HTP to a slightly less usual but more useful form.

Definition 6.4. We define \( \text{HTP}'(R, S) \) with \( R \) a ring and \( S \subset R \) to be: given an \( n \in \mathbb{Z}_{\geq 1} \) and a set of polynomials \( P \) in \( R[X_1, \ldots, X_n] \) of degree at most 2, determine whether the polynomials in \( P \) have a common zero in \( S^n \). We write \( \text{HTP}'(R) \) for \( \text{HTP}'(R, R) \).

Theorem 6.5. Take any ring \( R \) and \( S \subset R \). The problems \( \text{HTP}(R, S) \) and \( \text{HTP}'(R, S) \) are equivalent.

Proof. The reduction \( \text{HTP}'(R, S) \leq \text{HTP}(R, S) \) is trivial from the definition.

We will now show \( \text{HTP}(R, S) \leq \text{HTP}'(R, S) \). Let \( (n, P) \) be an input for \( \text{HTP}(R, S) \). We briefly sketch the reduction, producing \( (m, Q) \) such that the polynomials in \( Q \) have a common zero exactly if \( P \) has a zero.
1. Let \( m := n, Q := P \).

2. While \( Q \) contains a polynomial \( q \) containing a monomial \( c \prod_{i=1}^{k} x_{n_i}, c \neq 0 \) where \( n_i \in \{1, \ldots, m\} \) for \( i = 1, \ldots, k \) of degree \( k \) strictly bigger than 2, make \( m := m + 1, Q := Q \cup \{X_m - X_{n_1}X_{n_2}\} \) and in \( q \) replace the monomial \( c \prod_{i=1}^{k} x_{n_i} \) with \( cX_m \prod_{i=1}^{k} x_{n_i} \), lowering the degree of that monomial.

Note that the zero set of \( Q \) is conserved in each step, and that step 2 always terminates. This proves the theorem.

**Proof of Theorem 1.9** By Theorems 6.3 and 6.5 we reduce from the problem \( \text{HTP}'(Q(i), A^*) \). Let \( n \in \mathbb{Z}_{\geq 1} \) and \( P = \{p_1, \ldots, p_m\} \) a subset of \( Q(i)[X_1, \ldots, X_n] \) consisting of polynomials of degree at most 2 be given. By removing denominators, assume \( P \subset \mathbb{Z}[X_1, \ldots, X_n] \). We will construct input order \( B \) for \( \Pi_{(X^2+1)^2} \) that is a yes-instance if and only if the polynomials in \( P \) have a common zero in \( (A^*)^n \).

Embed \( \mathbb{Z}[i, X_1, \ldots, X_n] \) in \( \mathbb{Z}[i, X_0, \ldots, X_n] \). We now multiply every monomial in one of the polynomials of \( S \) by a power of \( X_0 \) such that the polynomial is homogeneous of degree 2; call the resulting homogeneous polynomials \( q_1, \ldots, q_m \). For \( 1 \leq k \leq m \) let \( C_k \) be twice the matrix corresponding to the quadratic form \( q_k \). Note \( C_k \in \text{Mat}(n+1, \mathbb{Z}[i]) \). Letting \( X = (X_0, \ldots, X_n) \), we then have \( X^\top C_k X = 2q_k(X_0, \ldots, X_n) \) and \( q_k(1, X_1, \ldots, X_n) = p_k(X_1, \ldots, X_n) \).

Let \( 1, v_0, v_1, \ldots, v_n, u_1, \ldots, u_m \) be formal variables and define \( \mathbb{Z}[i] \)-modules \( V = \bigoplus_{k=0}^{n} v_k \mathbb{Z}[i] \) and \( W = \bigoplus_{k=1}^{m} w_k \mathbb{Z}[i] \). We then choose \( B' \) additively equal to \( 1 \cdot \mathbb{Z}[i] \oplus V \oplus W \). We define a multiplication on \( B' \) by making it an \( \mathbb{Z}[i] \)-module in the obvious way, defining multiplication by 1 to be the identity, multiplication on \( V \times W, W \times V \) to be the zero map, and letting \( \varphi_k : V \times V \to w_k \mathbb{Z}[i] \) be the bilinear symmetric map defined by \( C_k \). We see that \( B' \) is automatically commutative, and the multiplication is associative. Finally, identify \( B' \) as the \( \mathbb{Z} \)-module to \( \mathbb{Z} \oplus \mathbb{Z}[i] \oplus \mathbb{Z}[i]^{\oplus 2(n+1)} \oplus \mathbb{Z}[i]^{\oplus 2m} \) and let \( B \) be the submodule \( \mathbb{Z} \oplus \left( \mathbb{Z}[i] \oplus \mathbb{Z}[i]^{\oplus 2(n+1)} \oplus \mathbb{Z}[i]^{\oplus 2m} \right) \). Note \( B \) is actually a subring and hence an order.

It remains to prove that \( Z_B((X^2 + 1)^2) \) is non-empty if and only if \( Z_{(A^*)^n}(P) \) is non-empty. Note that the subring \( \mathbb{Z}[i] \) is the separable subring of \( B' \), and \((V + W) \cap B' \) is the nilpotent part. Let \( x = a + \sum_{k=0}^{n} b_k v_k + \sum_{k=1}^{m} c_k w_k \) with \( a, b_k, c_k \in \mathbb{Z}[i] \) be an element of \( B \). Then if \( (x^2 + 1)^2 = 0 \), without loss of generality we have \( a = i \). We see \( x^2 + 1 \) then becomes \( \sum_{k=0}^{n} 2ib_k v_k + w \) for some \( w \in W \). Letting \( b = (b_0, \ldots, b_n) \), we see that \( (x^2 + 1)^2 = -4 \sum_{k=1}^{m} b^\top C_k b w_k \), and hence \( B \) contains a zero of \( (X^2 + 1)^2 \) if and only if there is a \( b \in \mathbb{Z}[i]^{n+1} \) with \( q_k(b_0, \ldots, b_n) = 0 \) for every \( 1 \leq k \leq m \), with \( b \) being \( 1 + i \) modulo \( (2) \) on every coordinate. As every \( b_i \) is specifically non-zero, that is equivalent to having an \( x \in Q(i)^n \) with \( p_j(x_1, \ldots, x_n) = 0 \) for every \( 1 \leq j \leq m \), with \( v(x_j) = 0 \) for \( 1 \leq j \leq n \). To recap: \( Z_B((X^2 + 1)^2) \) is non-empty if and only if the polynomials in \( P \) have a common zero in \( (A^*)^n \). This completes the proof of Theorem 1.9.
References

[Gio13] A. Gioia. On the Galois closure of commutative algebras. PhD thesis, Leiden University, 2013.

[Len84] A. K. Lenstra. Factoring multivariate integral polynomials. Theoret. Comput. Sci., 34(1-2):207–213, 1984.

[LS17] H. W. Lenstra, Jr. and A. Silverberg. Roots of unity in orders. Found. Comput. Math., 17(3):851–877, 2017.

[LS18] H. W. Lenstra, Jr. and A. Silverberg. Algorithms for commutative algebras over the rational numbers. Found. Comput. Math., 18(1):159–180, 2018.

[Rob59] Julia Robinson. The undecidability of algebraic rings and fields. Proc. Am. Math. Soc., 10(6):950–957, 1959.

[Sag18] Sage Developers. SageMath, the Sage Mathematics Software System (Version 8.2), 2018. http://www.sagemath.org.

[Sil09] J. H. Silverman. The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Springer, Dordrecht, second edition, 2009.

[Spe18] P. Spelier. The complexity of root-finding in orders. Bachelor thesis, 2018.

[Spe21] P. Spelier. The complexity of intersecting subproducts with subgroups in cartesian powers. arXiv:??, 2021.

[Ste17] P. Stevenhagen. Number rings, 2017.