Gröbner bases of ideals invariant under a commutative group: the non-modular case

Jean-Charles Faugère, Jules Svartz
INRIA, Paris-Rocquencourt Center, PolSys Project
UPMC, Univ Paris 06, LIP6
CNRS, UMR 7606, LIP6

ABSTRACT

We propose efficient algorithms to compute the Gröbner basis of an ideal \( I \subseteq \mathbb{k}[x_1, \ldots, x_n] \) globally invariant under the action of a commutative matrix group \( G \), in the non-modular case (where \( \text{char}(\mathbb{k}) \) doesn’t divide \( |G| \)). The idea is to simultaneously diagonalize the matrices in \( G \) and apply a linear change of variables on \( I \) corresponding to the base-change matrix of this diagonalization. We can now suppose that the matrices acting on \( I \) are diagonal. This action induces a grading on the ring \( \mathbb{R} \) compatible with the degree, indexed on \( G \), that we call \( G \)-degree. The next step is the observation that this grading is maintained during a Gröbner basis computation or even a change of ordering, which allows us to split the Macaulay’s matrices into \( [G] \) submatrices being roughly same size. In the same way, we are able to split the canonical basis computation or even a change of ordering, which allows us to parallelize the linear algebra steps, which has been successfully implanted. On instances coming from applications (NTRU cryptography, simulating action of the group, several approaches have been proposed to solve the system while taking the symmetries into account. In [2] Colin proposes to use invariants [20] to solve the system. This method is very efficient if the Hironaka Decomposition of the ring of invariants is simple, but for the Cyclic-n problem [12] for example, it seems better to use a second method based on SAGBI Gröbner Basis techniques [5]. However, it remains an open question to solve efficiently the system in the general case. In the biology problem [4] or in the physic problem [10], an approach has been proposed if the group \( G \) is supposed to be the symmetric group or copies of the symmetric group (elements of the form \( \{\sigma, \ldots, \sigma\} \in S_n^\sigma \). In our paper, we present efficient algorithms together with complexity analysis to solve polynomial systems which are globally invariant by any commutative group \( G \). The algorithms are based on three main ideas: first, since the group \( G \) is commutative, it is possible to diagonalize the group \( G \), assuming that the characteristic of the field \( \mathbb{k} \) and \( |G| \) are coprimes. Thus, up to some linear change of variables, we obtain an ideal \( I_{G} \) invariant under a diagonal group \( G_{\mathbb{k}} \) isomorphic to \( G \). The second idea is to introduce a grading on \( R = \mathbb{k}[x_1, \ldots, x_n] \) given by the group \( G_{\mathbb{k}} \). This grading exists for every finite group \( H \) and is indexed on \( X(H) \), the set of irreducible linear representations of the group \( H \). The decomposition \( R = \bigoplus_{X \in X(H)} R_X \) is known as the decomposition of \( R \) into isotypic components (see [18]). In our case, since \( G_{\mathbb{k}} \) is diagonal, the set \( X(G_{\mathbb{R}}) \) is isomorphic to \( G_{\mathbb{R}} \) and the isotypic components are generated by monomials. Therefore, we introduce the notion of \( G_{\mathbb{R}} \)-degree of a polynomial: assuming that \( G_{\mathbb{R}} \) is generated by diagonal matrices \( \text{Diag}(\hat{B}_1, \ldots, \hat{B}_s) \) of order \( q_i \) with \( q_1|q_2|\cdots|q_s = e \) and that \( \hat{B} \) is a primitive \( e \)-root of 1, we say that a polynomial \( f \in \mathbb{k}[x_1, \ldots, x_n] \) is \( G_{\mathbb{R}} \)-homogeneous of \( G_{\mathbb{R}} \)-degree \( (d_1, \ldots, d_i) \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_s} \) if \( f(\hat{B}_1 x_1, \ldots, \hat{B}_s x_n) = \hat{B}^{d_1} f(x_1, \ldots, x_n) \) for all \( i \). Notice that this action of diagonal groups on polynomials has been used in invariant theory or to speed up Gröbner basis computation in [18, 20, 19, 13]. However, to the best of our knowledge, the impact of such a grading on the complexity of Gröbner bases has not been studied.

Taking into account that the operation of taking the S-polynomial preserves this grading, the final idea is to observe that this can be used to speed up the Gröbner basis computation. More precisely, the Macaulay’s matrix can be decomposed in \( G_{\mathbb{R}} \) smaller independent matrices, being roughly same size. In particular, it allows

Categories and Subject Descriptors
I.1.2 [Computing Methodologies]: Symbolic and Algebraic Manipulation—Algorithms

1. INTRODUCTION

Solving multivariate polynomial systems is a fundamental problem in Computer Algebra, since algebraic systems can arise from many applications (cryptography, robotics, biology, physics, coding theory, etc...). One method to solve such systems is based on the Gröbner bases theory. Efficient algorithms to compute Gröbner bases have been proposed, for instance Buchberger’s algorithm [1], Faugère F5 or F4 [7, 8]. If the system has only a finite number of solutions the usual strategy is to compute a Gröbner basis for the DRL ordering, and then perform a change of ordering to obtain a Gröbner basis for the lexicographic ordering with the FGLM algorithm [6]. However, problems coming from applications are often highly structured: in several algebraic problems the set of solutions (the algebraic variety) is invariant under the action of a finite group. The underlying algebraic problem is to compute the variety \( V(I) \) associated to an ideal \( I \subseteq \mathbb{k}[x_1, \ldots, x_n] \) supposed to be globally stable under a finite matrix group \( G \subseteq \text{GL}_n(\mathbb{k}) \), which means that \( \forall f \in I \) \( \forall \alpha \in G \) \( f^\alpha \in I \). If all the equations are invariant under the action of the group, several approaches have been proposed to solve the system while taking the symmetries into account. In [2] Colin proposes to use invariants [20] to solve the system. This method is very efficient if the Hironaka Decomposition of the ring of invariants is simple, but for the Cyclic-n problem [12] for example, it seems better to use a second method based on SAGBI Gröbner Basis techniques [5]. However, it remains an open question to solve efficiently the system in the general case. In the biology problem [4] or in the physic problem [10], an approach has been proposed if the group \( G \) is supposed to be the symmetric group or copies of the symmetric group (elements of the form \( \{\sigma, \ldots, \sigma\} \in S_n^\sigma \). In our paper, we present efficient algorithms together with complexity analysis to solve polynomial systems which are globally invariant by any commutative group \( G \). The algorithms are based on three main ideas: first, since the group \( G \) is commutative, it is possible to diagonalize the group \( G \), assuming that the characteristic of the field \( \mathbb{k} \) and \( |G| \) are coprimes. Thus, up to some linear change of variables, we obtain an ideal \( I_{G} \) invariant under a diagonal group \( G_{\mathbb{R}} \) isomorphic to \( G \). The second idea is to introduce a grading on \( R = \mathbb{k}[x_1, \ldots, x_n] \) given by the group \( G_{\mathbb{R}} \). This grading exists for every finite group \( H \) and is indexed on \( X(H) \), the set of irreducible linear representations of the group \( H \). The decomposition \( R = \bigoplus_{X \in X(H)} R_X \) is known as the decomposition of \( R \) into isotypic components (see [18]). In our case, since \( G_{\mathbb{R}} \) is diagonal, the set \( X(G_{\mathbb{R}}) \) is isomorphic to \( G_{\mathbb{R}} \) and the isotypic components are generated by monomials. Therefore, we introduce the notion of \( G_{\mathbb{R}} \)-degree of a polynomial: assuming that \( G_{\mathbb{R}} \) is generated by diagonal matrices \( \text{Diag}(\hat{B}_1, \ldots, \hat{B}_s) \) of order \( q_i \) with \( q_1|q_2|\cdots|q_s = e \) and that \( \hat{B} \) is a primitive \( e \)-root of 1, we say that a polynomial \( f \in \mathbb{k}[x_1, \ldots, x_n] \) is \( G_{\mathbb{R}} \)-homogeneous of \( G_{\mathbb{R}} \)-degree \( (d_1, \ldots, d_i) \in \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_s} \) if \( f(\hat{B}_1 x_1, \ldots, \hat{B}_s x_n) = \hat{B}^{d_1} f(x_1, \ldots, x_n) \) for all \( i \). Notice that this action of diagonal groups on polynomials has been used in invariant theory or to speed up Gröbner basis computation in [18, 20, 19, 13]. However, to the best of our knowledge, the impact of such a grading on the complexity of Gröbner bases has not been studied.

Taking into account that the operation of taking the S-polynomial preserves this grading, the final idea is to observe that this can be used to speed up the Gröbner basis computation. More precisely, the Macaulay’s matrix can be decomposed in \( G_{\mathbb{R}} \) smaller independent matrices, being roughly same size. In particular, it allows

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Copyright 20XX ACM X-XXXX-XX-X/XX/XX ...$10.00.
us to split the matrices arising in classical Gröbner basis algorithms based on linear algebra like Macaulay/Lazard algorithm [16], \( F_1 [7] \) or \( F_5 [8] \). Therefore, the complexity (in time and in memory) of computing Gröbner bases of such invariant ideals can be decreased in both theory and practice. In the same way, in the case of a zero-dimensional ideal \( I_{2p} \), the canonical basis of the ring \( R/I_{2p} \) can also be decomposed in monomials having same \( G_2 \)-degree and thus we are able to split the multiplication matrices arising in FGLM.

In addition, this grading can be used to transform very easily a globally invariant problem into a problem for which all the equations are \( G_2 \)-homogeneous: we show that for each original equation \( f \) we can take the \( G_2 \)-homogeneous components of \( f \).

We have implemented in the computer algebra system Magma, “abelian” version of the \( F_5 \) and FGLM algorithms that run several times faster, compared to the same implementation of these classical algorithms. For example, applying FGLM on the Cyclic-10 problem (a system with 34940 solutions), instead of computing 10 multiplication matrices of size 34490, our algorithm compute 900 quasi-square matrices of sizes at most 348.

In order to compare similar implementations, we have implemented an “abelian” version of \( F_5 \) [7] in FGB (C language): computing a Gröbner basis of the Cyclic-10 problem is about 500 times faster with the new approach. Moreover, a grevlex Gröbner basis for the Cyclic-11 problem (184756 solutions) can be computed in less than 8 hours. We also demonstrate that our approach has a significant impact in other fields: NTRU is a well known cryptosystem and the underlying problem can easily be modeled by quadratic equations which are left globally invariant by the action of the cyclic group. We observe a factor of 250 in favor of the new approach for small size problems and more importantly we can solve previously untractable problems. Surprisingly, during these experiments, the linear algebra parts (that is building the matrices and the gaussian elimination parts) can sometimes be so accelerated that the management of the list of critical pairs becomes the most time-consuming part whereas it is usually negligible.

More generally, the algorithms given in this paper can also be used for other kind of structured polynomial systems such as quasi-homogeneous or multi-homogeneous polynomials. Hence we have now a systematic and uniform approach to solve those structured problems. Several further developments can be made on the subject: the Abelian-\( F_5 \) and Abelian-FGLM algorithms have to be implemented in C, and it seems possible to obtain a parallelized version of the Abelian-FGLM algorithm. We already have identified new classes of invariant problems which can be solved in polynomial time; for other class of problems the degree reached during the Gröbner basis computation is much lower than expected and it would be very useful to compute explicitly the Hilbert Series of ideals invariant under a diagonal group.

The organization of the paper is as follows: in section 2, we recall classical notations and explain the relations between the ideals \( I \) and \( I_{2p} \), and the matrix groups \( G \) and \( G_2 \). In section 3, we explain the grading induced by the diagonal matrix group \( G_2 \), and introduce the notion of \( G_2 \)-degree of monomials and polynomials. The vector space generated by all monomials having same \( G_2 \)-degree is no more than an isotypic component ([18]) but since the formulation is simpler in the case of a diagonal group, we introduce the notion of \( G_2 \)-degree of monomials and \( G_2 \)-homogeneous polynomials. The sections 4 and 5 provide variant of the \( F_5 \) and FGLM algorithms. The complexity questions are answered in section 6, and benchmarks are made in section 7.

2. LINEAR CHANGE OF VARIABLES

2.1 Frequently used notations

From now we assume that \( G \) is a finite commutative subgroup of \( \text{GL}_n(k) \), the set of square matrices with coefficient in a field \( k \) of characteristic 0 or \( p \) such that \( p \) and \( |G| \) are coprimes. \( G_2 \) will be used to denote a diagonal matrix group, conjugated to \( G \). \( R_k = k[x_1, \ldots, x_n] \) is the ring of polynomials with coefficients in \( k \). In the following, we will have to consider a finite simple extension of \( k \) that will be denoted \( K = k(\xi) \). The set of monomials of \( R_k \) will be denoted \( M_k \), simply \( M \) if there isn’t any ambiguity. We fix an admissible monomial ordering \( \preceq \) on the set of monomials (only admissible ordering are allowed, for a precise definition, we refer to [3] p. 53). For a given degree \( d \), \( M_k(R_k) \) (or only \( M_k \)) will be the set of all monomials in \( R_k \) of degree \( d \). For a polynomial in \( R_k \), \( \text{LC}(f) \) (resp \( \text{LM}(f) \), \( \text{LT}(f) \)) denotes the leading coefficient (resp leading monomial, leading term) in \( f \). We have the relation \( \text{LT}(f) = \text{LC}(f) \text{LM}(f) \).

2.2 Action of \( \text{GL}_n(k) \) on polynomials. Invariant rings.

This subsection describes the basic properties of the action of \( \text{GL}_n(k) \) on polynomials. We recall that \( G \) is a finite subgroup of \( \text{GL}_n(k) \). Let \( X \) be the column vector whose entries are \( x_1, \ldots, x_n \).

For a polynomial in \( R \) and \( A \in G \), let \( f^A \) be the polynomial obtained by substituting the components of \( A.X \) to \( x_1, \ldots, x_n \). Since \( (f^A)^B = f^{AB} \), we obtain an action of \( G \) on \( R \). Let \( R_k \) be the vector space of all homogeneous polynomials of degree \( d \).

\( \text{GL}_n(k) \) acts on \( R_k \). We observe that \( R_k \) preserves the homogeneous components.

**Definition 1** We denote by \( R_G \) the set of invariant polynomials, that means polynomials invariant under the action of \( G \) : \( f^A = f \) for every \( A \in G \).

Although we won’t work exclusively in the ring \( R_G \) of invariant polynomials, we will use several known properties on this set, especially in the complexity section.

**Example 1** The symmetric group \( \Sigma_n \) can be embedded in \( \text{GL}_n(k) \), and \( R_{\Sigma_n} \) is no more than the set of the so called symmetric polynomials. Let \( C_n \) be the subgroup of \( \Sigma_n \) generated by the n-cycle \( \sigma = (1, 2, \ldots, n) \). \( C_n \) is a cyclic group of order \( n \), embedded in \( \text{GL}_n(k) \) is generated by:

\[
\begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 1 \\
1 & 0 & 0 & \cdots & 0
\end{pmatrix}
\]

For example if \( n = 3 \) then \( x_1^2x_2 + x_2^2x_3 + x_3^2x_1 \) belongs to \( R_{\Sigma_3} \).

2.3 From commutative group to diagonal group

This subsection presents one of the main ideas of the paper, although it is very simple. We recall some well known facts about commutative matrix groups.

**Theorem 1** Any finite commutative group is isomorphic to some \( \mathbb{Z} / q_1 \mathbb{Z} \times \cdots \times \mathbb{Z} / q_k \mathbb{Z} \), with \( q_1, \ldots, q_k \). Moreover, the integers \( q_1, \ldots, q_k \) are unique.

**Definition-Proposition 1** Following the notations of the previous theorem, the integer \( e = q_i \) is called the exponent of the group and is the lowest common multiple of the orders of the elements of the group.

**Theorem 2** Let \( G \) be a finite commutative matrix group, and \( e \) be its exponent. Let \( \xi \) be a primitive e-th root of 1, in an extension of \( k \) and \( K = k(\xi) \). The subgroup \( G \) is diagonalizable over \( K \), meaning that there exists a matrix \( P \) in \( \text{GL}_n(K) \), such that the group \( G_2 = P^{-1}GP = \{ P^{-1}AP \mid A \in G \} \) is a diagonal group.

**Proof**. Every matrix \( A \in G \) is cancelled by the polynomial \( X^e - 1 \), which fully splits on \( K \) since \( \text{char}(k) \mid |G| \). So every matrix of \( G \) is diagonalizable, and it is well known that a set of diagonalizable matrices that commutes is codiagonalizable.

**Example 2** Let \( k \) be any field of characteristic 0 or coprime with \( n \). Then if we denote \( K = k(\xi) \) where \( \xi \) is a primitive n-root of 1.
in an extension of $k$, then the cyclic group $C_n$ defined in example 1 is diagonalizable with the base-change matrix $P = (\xi^{j-i})_{i,j \in \{1,...,n\}}$. The matrix associated to the cycle $(1,...n)$ becomes the diagonal matrix $D_n = \text{diag}(\xi, \xi^2, \ldots, \xi^{n-1})$.

**Definition 2** Let $I$ be an ideal in $R_k = k[x_1, \ldots, x_n]$. It is said to be stable under the action of $G$ ($G$-stable) if
\[ \forall f \in I \quad \forall a \in G \quad f^a \in I \]

**Proposition 1** Let $G$ be a $G$-stable ideal, and let $G_P$ and $P$ be the diagonal group and the base-change matrix obtained in theorem 2. Then $I_P = K\oplus(f^P, f \in I)$ is an ideal of $R_k$ stable under $G_P$. If $I = \{f_1, \ldots, f_m\}_R$, then $I_P = \{f_1^P, \ldots, f_m^P\}_R$.

**Example 3** To illustrate the definition, we use the well known Cyclic-group problem. The ideal $I$ of $R_k$ is generated by:
\[ h_1 = x_1 + \cdots + x_n \\
 h_2 = x_1 x_2 + x_2 x_3 + \cdots + x_n x_1 \\
 \vdots \\
 h_n = x_1 x_2 \cdots x_{n-1} - 1 \\
 h_n = x_1 x_2 \cdots x_n - 1 
\]
The ideal $I$ is obviously invariant under the cyclic group $C_n$, since each $h_i$ verifies $h_i^m = h_i$ and is also stable under the cyclic matrix $\xi h_i$ with $\xi$ a primitive $n$-root of 1, since $h_i^m = \xi^{m-1} h_i$. The group $G$ is generated by $\xi$ and $\xi h_i$ for $i = 1, \ldots, n$. With $P$ the matrix given in example 2, $G_P = P^{-1} G P$ is generated by $D_n$ and $\xi h_i$. Let $G$ be a diagonal group isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. We denote by $f_i$ the polynomials $h_i^m$, which generate $G_P$: for instance, $f_1 = x_1, f_2 = x_1 x_2 + x_2 x_3 + 3x_3^2, f_3 = x_1^3 + x_2^3 + 3x_1 x_2 x_3 + x_3^3 - 1$ when $n = 3$. It is easy to prove that, for the Cyclic-group problem, the polynomial $f_1$ is always $e_n$.

### 3. GRADING INDUCED BY A DIAGONAL MATRIX GROUP ON A POLYNOMIAL RING

In this section, we define the $G_P$-degree of a monomial where $G_P$ is a diagonal matrix group. This $G_P$-degree induces a grading of $R_k$ given by the isomorphism $G_P \simeq \mathbb{Z}/q\mathbb{Z}$.

#### 3.1 $G_P$-degree of monomials

Let $G_P$ be a diagonal group of $GL_n(K)$, with diagonal coefficients in $\mathbb{Z} = \{0, 1, 2, \ldots, \xi^{n-1}\}$, with $e$ the exponent of $G$ and $\xi$ a primitive $e$-root of 1, as defined in the previous section. Let $\phi$ be an isomorphism
\[ \phi : (G_P, D) \rightarrow (\mathbb{Z}/q\mathbb{Z})^n \]
and let $D_P$ be the preimage of $(0,0,0,\ldots,0)$, so $D_P$ generates a subgroup of $G_P$ of cardinal $|q^e|$.

**Example 4** With $G_P$ the group arising in previous example 3, we take $\phi$ such that $D_P = (0,0,0,\ldots,0)$.

**Proposition 2** For every monomial $m \in \mathcal{M}$ and for each $j$, there exists a unique $\mu_j \in \{0, \ldots, q_j - 1\}$ such that
\[ m^\mu = (\xi^0)^{\mu_1} \cdots (\xi^{q_j-1})^{\mu_j} m. \]

**Proof.** Let $m = \prod x_i^{e_i}$ and $D_P = \text{diag}(\beta_1, \ldots, \beta_n)$. Since $D_P$ has order $q$, the coefficients $\beta_i$ are $q$-roots of 1, so can be denoted $\xi^{j-i}$. Then
\[ m^\mu = (\beta_1)^{e_1} \cdots (\beta_n)^{e_n} = \prod (\beta_i)^{e_i} \text{mod } m = \xi^{\sum \mu_j} m. \]

Then, we can take $\mu_j = \sum e_i \alpha_i \text{mod } q_j$. Since $\xi$ has order $e$, $\xi^{\mu_j}$ has order $q_j$ and the unicity of $\mu_j$ is clear.

Instead of considering $\mu_j$ in $\{0, \ldots, q_j - 1\}$, we take $\mu_j$ in $\mathbb{Z}/q_j\mathbb{Z}$, which makes sense since $\xi^{q_j}$ has order $q_j$.

**Definition 3** The $k$-uple $\{\mu_1, \ldots, \mu_k\} \subseteq \mathbb{Z}/q\mathbb{Z}$ is said to be the $G_P$-degree of $m$ and is denoted $\text{deg}_{G_P}(m)$, although it depends on the choice of the matrices $D_j$ (more exactly, the choice of $\phi$). We denote by $G = \mathbb{Z}/q\mathbb{Z}$ the set of all $G_P$-degrees.

**Remark 1** It is yet unclear that every $\mu \in G$ is the $G_P$-degree of some monomial. It will be proved in the complexity section.

**Proposition 3** Since $\text{deg}_{G_P}(m) + \text{deg}_{G_P}(m') = \text{deg}_{G}(\text{mm'})$ for all $m, m' \in \mathcal{M}$, $R$ can be graded by $R = \bigoplus \text{Vect}(\mathcal{M})$, where $\mathcal{M}$ is the set of monomials of $G_P$-degree $\mu$.

**Proof.** Let $i \in \{1, \ldots, k\}$, $m, m' \in \mathcal{M}$ and $\mu, \mu'$ such that $m^\mu_i = \xi^{\mu_i} m$ and $m'^\mu_i = \xi^{\mu_i'} m'$. Then $(\text{mm'})^\mu_i = m^\mu_i m'^\mu_i = \xi^{\mu_i + \mu_i'} m$. It follows that the $G_P$-degree verifies $\text{deg}_{G_P}(m) + \text{deg}_{G_P}(m') = \text{deg}_{G}(\text{mm'})$ for all monomials $m, m' \in \mathcal{M}$. Hence $\text{deg}_{G_P}(1) = \{0, \ldots, 0\}$.

**Remark 2** If we denote by $\mathcal{M}_d$ the set of monomials of degree $d$ and $G_P$-degree $\mu$, $\mathcal{M}_d \subseteq \mathcal{M}_d' \subseteq \mathcal{M}_d' \subseteq \mathcal{M}_d' \subseteq \mathcal{M}_d' \subseteq \mathcal{M}_d' \subseteq \mathcal{M}_d' \subseteq \mathcal{M}_d'$ for all $d, d', g, g'$.

**Remark 2** If we denote by $\mathcal{M}_d \subseteq \mathcal{M}_d' \subseteq \mathcal{M}_d' \subseteq \mathcal{M}_d' \subseteq \mathcal{M}_d' \subseteq \mathcal{M}_d' \subseteq \mathcal{M}_d' \subseteq \mathcal{M}_d'$ for all $d, d', g, g'$.

**Example 5** Let $G_P$ be the matrix group generated by the diagonal matrix $D_P = \text{diag}(\xi^2, \xi^2, 1)$ where $\xi$ is a primitive 3-root of 1. Each $x_i$ has $G_P$-degree $i$ mod $n$, so $m = \prod x_i^{e_i}$ has $G_P$-degree $\sum \alpha_j$ mod $n$. Hence, $x_1 x_2 x_3$ (resp. $x_1 x_2 x_3$) has $G_P$-degree 0 (resp. 2).

**Example 6** (cont. of example 3) The $G_P$-degree of $x_i$ is $(i, 1)$.

#### 3.2 $G_P$-homogeneous polynomials

In this subsection, we define the notion of $G_P$-homogeneity. The cornerstone of the Abelian-FS algorithm (section 4) is that the S-polynomial of two $G_P$-homogeneous polynomials is $G_P$-homogeneous, which will be proved in theorem 3.

**Definition 4** A polynomial $f$ in $R_k$ is said to be $G_P$-homogeneous if all monomials of $f$ share the same $G_P$-degree $\{\mu_1, \ldots, \mu_k\} \subseteq G$. In this case, we set $\text{deg}_{G_P}(f) = \text{deg}_{G_P}(LM(f))$.

**Proposition 4** If $f$ is $G_P$-homogeneous and $m$ is a monomial, then $mf$ is $G_P$-homogeneous. Moreover, $\text{deg}_{G_P}(mf) = \text{deg}_{G_P}(m) + \text{deg}_{G_P}(f)$.

**Proof.** If $m$ is a monomial of $f$, then $\text{deg}_{G_P}(\text{mm}) = \text{deg}_{G_P}(\text{mm}) + \text{deg}_{G_P}(f) + \text{deg}_{G_P}(m)$, so all monomials of $mf$ share the same $G_P$-degree $\text{deg}_{G_P}(f) + \text{deg}_{G_P}(m) = \text{deg}_{G_P}(mf)$.

**Theorem 3** Let $f, g$ be two $G_P$-homogeneous polynomials of $R_k$. The S-polynomial of $(f, g)$, defined by
\[ S(f, g) = \frac{LM(f) \vee LM(g)}{LM(f) \vee LM(g)} \]
is $G_P$-homogeneous, and $\text{deg}_{G_P}(S(f, g)) = \text{deg}_{G_P}(LM(f) \vee LM(g))$. (LM(f) \vee LM(g)) denotes the lowest common multiple of $LM(f)$ and $LM(g)$.)
3.3 $G_\mathcal{P}$-homogeneous ideals

In this subsection, $G_\mathcal{P}$ is a diagonal group, and $I_\mathcal{P}$ is a $G_\mathcal{P}$-stable ideal generated by $f_1, \ldots, f_m$. A Gröbner basis computation preserves the $G_\mathcal{P}$-degree, but the polynomials $f_i$ are not necessarily $G_\mathcal{P}$-homogeneous. Our aim here is to prove that $G_\mathcal{P}$-homogeneous components of $f_i$ are in $I_\mathcal{P}$, and so to compute a Gröbner basis of $I_\mathcal{P}$, we take the $G_\mathcal{P}$-homogeneous components of generators of $I_\mathcal{P}$ as inputs. This operation is a negligible cost since at each degree $d$, the Abelian-FGLM algorithm (presented in the next section) separates the $\mathcal{A}_d$ into subsets $\mathcal{A}_d^\mathcal{P}$ of same $G_\mathcal{P}$-degree $g$.

**Theorem 4** An ideal is $G_\mathcal{P}$-stable if and only if it is $G_\mathcal{P}$-homogeneous.

It is obvious that a $G_\mathcal{P}$-homogeneous ideal is $G_\mathcal{P}$-stable. To prove the other implication, we will first prove a lemma.

**Lemma 1** Let $f \in I_\mathcal{P}$, and $D \in G_\mathcal{P}$, then the $gr(D)$-homogeneous components of $f$ are in $I_\mathcal{P}$.

**Proof.** Let $g$ be the order of $D$ in $G_\mathcal{P}$, and $\xi_D = \xi_D^g$. Then, all diagonal coefficients of $D$ are powers of $\xi_D$. $f$ can be written $\sum_{j=0}^{g-1} f_j$, with $f_j = \xi_D^j f_j$; in other words, the $f_j$ are the $gr(D)$-homogeneous components of $f$. Let $X_f = (f_0, f_1, \ldots, f_{g-1})$, $V = (\xi_D^j)_{0 \leq j, k \leq g-1}$, and $Y_f = VX_f$. Since $f_j = \xi_D^j f_j$, the column vector $Y_j$ is equal to $(f, f^p, \ldots, f^{p^{d-1}})$. Since $f \in I_\mathcal{P}$ and $I_\mathcal{P}$ is $G_\mathcal{P}$-stable, all components of $Y_f$ belong to $I_\mathcal{P}$. But $V$ is a VanDerMonde invertible matrix, so the components of $Y_f$ are obtained from $Y_f$ by linear combinations, and the $f_j$ belong to $I_\mathcal{P}$. 

**Proof.** We now prove the theorem by induction on $k$ where $G \simeq \mathbb{Z}/q_1 \mathbb{Z} \times \cdots \times \mathbb{Z}/q_k \mathbb{Z}$: the case $k = 1$ is the lemma. Now assume that $k \geq 2$ and let $D_1$ be the matrices generating $G_\mathcal{P}$ as defined in section 2. Let $f \in I_\mathcal{P}$. By the lemma, the $gr(D_1)$-homogeneous components of $f$ are in $I_\mathcal{P}$. Denote by $G_{\mathcal{P}_1}$ the subgroup of $G_\mathcal{P}$ generated by $D_1, D_2, \ldots, D_k$. Then $G_{\mathcal{P}_1} \simeq \mathbb{Z}/q_1 \mathbb{Z} \times \cdots \times \mathbb{Z}/q_k \mathbb{Z}$, and $I_\mathcal{P}$ is also $G_{\mathcal{P}_1}$-stable, and by induction the $G_{\mathcal{P}_1}$-homogeneous components of each $gr(D_1)$-homogeneous component of $f$ are in $I_\mathcal{P}$, but they are exactly the $G_{\mathcal{P}_1}$-homogeneous components of $f$.

**Example 8** Let $G_{\mathcal{P}}$ be the diagonal group of order 2 generated by the matrix diag$(-1, 1)$, acting on $\mathbb{R}^2$ by $x \mapsto x_1^1 x_2 - x_2 + 1 \in I_\mathcal{P}$, with $I_\mathcal{P}$ a $G_{\mathcal{P}}$-stable ideal. Then since $deg_{\mathcal{P}}(x_1) = 1$, $deg_{\mathcal{P}}(x_2^3) = 2$, $deg_{\mathcal{P}}(x_1^2 x_2) = 3$, and $deg_{\mathcal{P}}(x_1^2 x_2) = 1$, therefore $x_1 x_2 + x_1 x_2 - x_2 + 1 \in I_\mathcal{P}$.

**4. ABELIAN-FGLM ALGORITHM**

Now, we are able to describe the Abelian-FGLM algorithm, which is a variant of FGLM that takes advantage of the action of the abelian group $G_{\mathcal{P}}$. As usual, $I_\mathcal{P}$ is a $G_{\mathcal{P}}$-stable ideal, with $G_{\mathcal{P}}$ a diagonal group isomorphic to $G$, the set of $G_{\mathcal{P}}$-degrees. Let $f_1, \ldots, f_m$ be polynomials generating $I_\mathcal{P}$, supposed to be $G_{\mathcal{P}}$-homogeneous (according to theorem 4). All computation of the reduced Gröbner basis of $I_\mathcal{P}$ would implicitly use the grading $R = \xi_{\mathcal{P}} R_{\mathcal{P}}$, since it computes $S$-polynomials. There exist several versions of the $F_2$-algorithm (see [8, 5]), we present here a variant of the matrix version. The $F_2$-algorithm constructs matrices degree by degree. At a fixed degree $d$, it constructs $m$ matrices of the form $M_{d,j}$ for each $i$ between 1 and $m$, and performs row reduction on them to obtain $\tilde{M}_{d,j}$. In the homogeneous case, $m_1, \ldots, m_r$ are all monomials of degree $d$, whereas in the affine case, they are all monomials of degrees between 0 and $d$. For the sake of simplicity, we assume that all polynomials $f_i$ are homogeneous. The rows are indexed by couples of the form $m_i f_i$, the matrix $M_{d,j}$ is deduced from the matrix $M_{d,j-1}$ by adding all rows $m_i f_i$ with $m_i$ describing the set of monomials of degree $d$ minus the rows $f_i$, except monomials removed by the $F_2$-criterion (see [8, 5]). The key of the Abelian-FGLM algorithm is the following: the polynomials $f_i$ are $G_{\mathcal{P}}$-homogeneous, and also the polynomials $m_i f_i$. Therefore, the only non-zero coefficients of the row indexed by $m_i f_i$ are on columns indexed by monomials having same $G_{\mathcal{P}}$-degree. So, instead of building one Macaulay matrix $M_{d,j}$, we will construct $[G_\mathcal{P}]$ matrices $M_{d,j}^\mathcal{P}$ for all $g \in \mathcal{G}$. 

Notice that all the loops on $g \in \mathcal{G}$ are independent, so at each degree $d$, it is possible to parallelize on $|\mathcal{G}|$ different processors to speed up the computations. Assuming that the degrees of the primary invariants are relatively prime, we will see in the complexity section 6 that the number of monomials of $M_{d,j}$ having same $G_{\mathcal{P}}$-degree is almost the same for all $g$. In the affine case, we will prove without any assumption that the monomials of degree between 0 and $d$ are evenly distributed on $\mathcal{G}$. These considerations allow us to bound the complexity of the computation of a Gröbner basis on such ideals, and we will verify that in practice they make an improvement on the timings (see 7).

**5. ABELIAN-FGLM ALGORITHM**

In this section, we explain how to take advantage of the $G_{\mathcal{P}}$-grading to speed up the change of ordering, using a variant of the
classical FGLM algorithm [6]. We suppose that \( \dim(I_{g}) = 0 \), and that a Gröbner basis \( \mathcal{G}_{g} \) for an ordering \( \prec_{1} \) (for instance the DRL ordering) of the ideal \( I_{g} \) has already been computed, and we are interested in computing the Gröbner basis of \( I_{g} \) for an other ordering \( \prec_{2} \) (for example, the lexicographical ordering). First, we recall briefly the idea of the classical FGLM algorithm [6], and then we give the Abelian-FGLM algorithm. In this section, \( \text{Deg}(I_{g}) \) will denote the degree of \( I_{g} \), defined by the dimension of \( R_{K} / I_{g} \).

### 5.1 The FGLM algorithm

The idea of the FGLM algorithm is to pick up monomials \( m \) in \( R_{K} / I_{g} \) by increasing order for \( \prec_{2} \), and look for linear combinations in \( R / I_{g} \) between the Normal Forms \( \text{NF}(m, \mathcal{G}_{g}) \). Here is the pseudo-code of the algorithm applied to \( I_{g} \), although it works on every zero-dimensional ideal.

![FGLM algorithm](image)

The two steps (1) and (2) are made by linear algebra: we first compute the staircase \( \mathcal{E} = \{ m \in \mathcal{M} | m \text{ not reducible by } LM(\mathcal{G}_{g}) \} \)

The elements of \( \mathcal{E} \) form a basis of \( R_{K} / I_{g} \), which as dimension \( \text{Deg}(I_{g}) \), the degree of \( I_{g} \). Then, we compute the matrices of multiplication by the variables \( x_{i} \) in \( R_{K} / I_{g} \): we have to compute \( n \) matrices of size \( \text{Deg}(I_{g}) \times \text{Deg}(I_{g}) \)

Of the form \( m_{i} = x_{i} m \), with \( m_{i} \prec_{2} m \), so we already know the expression of \( \text{NF}(m_{i}, \mathcal{G}_{g}) \) in terms of \( \mathcal{G} \), which is a vector \( V' \). Then, \( \text{NF}(m, \mathcal{G}_{g}) \) is computed by the product \( V = M_{g} V' \).

The step (2) consists in deciding if \( m \) belongs to the new staircase in construction \( \mathcal{E} \) or if it is the leading monomial of a polynomial of the Gröbner basis for \( \prec_{2} \). To this end, we build a base-change matrix \( Q \) between \( \mathcal{E} \) and \( \mathcal{G} \): if \( s \) is the number of elements of the staircase \( \mathcal{E} = \{ u_{1} \prec_{2} \cdots \prec_{2} u_{s} \} \) at the current point of the algorithm, and \( V_{i} \) the vectors corresponding to \( \text{NF}(u_{i}, \mathcal{G}_{g}) \), then \( Q V_{i} \) is equal to the \( i \)-th vector of the canonical basis. Since the matrix \( Q \) is invertible, if all the components but the \( s \) first ones of \( Q V_{i} \) are zero, then we deduce a new element of the Gröbner basis \( \mathcal{G}_{g} \), otherwise \( m \) is a new element of \( \mathcal{E} \) and we have to update \( Q \) to map \( V \) on the \( i+1 \)-th element of the canonical basis.

### 5.2 The Abelian-FGLM algorithm

We can explain now the main difference between our version and the classical FGLM-algorithm, which follows from the proposition:

**Proposition 5** Let \( f \) be a \( G_{g} \)-homogeneous polynomial, and \( \mathcal{G}_{g} \) be the Gröbner basis of the ideal \( I_{g} \) for \( \prec_{1} \). Then \( NF(f, \mathcal{G}_{g}) \) is \( G_{g} \)-homogeneous, and has same \( G_{g} \)-degree as \( f \).

**Proof.** We have already seen that the property of being \( G_{g} \)-homogeneous is stable under \( x \)-polynomials operations, so \( NF(f, \mathcal{G}_{g}) \) is \( G_{g} \)-homogeneous. Moreover the only operations used in a Normal-Form computation are of the form \( f - f - \lambda m \) with \( \lambda \in G_{g} \), \( \lambda \in K \) and \( m \) a monomial such that \( LM(p) \) \( \lambda \) is equal to some monomial in \( f \), so \( \text{deg}_{G_{g}}(f) = \text{deg}_{G_{g}}(f) \).

If \( V \) is the column vector associated to \( NF(f, \mathcal{G}_{g}) \) in terms of \( G \), where \( f \) is \( G_{g} \)-homogeneous, we know that all components of \( V \) corresponding to monomials of \( G \) having a different \( G_{g} \)-degree are zero. Moreover, \( V M \) is the column vector associated to \( NF(f, \mathcal{G}_{g}) \), and since \( \text{deg}_{G_{g}}(v_{i}) = \text{deg}_{G_{g}}(v_{i}) + \text{deg}_{G_{g}}(u_{i}) \), all components of \( NF(x_{i} f, \mathcal{G}_{g}) \) of \( G_{g} \)-degree different from \( \text{deg}_{G_{g}}(v_{i}) + \text{deg}_{G_{g}}(u_{i}) \) are zero. So, we set \( g_{i} = \{ m \in G | \text{deg}_{G_{g}}(m) = g \} \) for each \( g \in G \), and we can construct \( n(G) \) matrices \( M_{g} \), the rows of which are indexed by \( \mathcal{E} \) and \( \text{deg}_{G_{g}}(u_{i}) \) and the columns by \( g_{i} \). Moreover, a linear dependence between a normal form \( NF(m, \mathcal{G}_{g}) \) and \( \{ NF(m', \mathcal{G}_{g}) | m' \in \mathcal{E} \} \) could happen only with monomials of \( G \) having same \( G_{g} \)-degree as \( m \). It is therefore possible to split the two staircases \( \mathcal{E} \) and \( \mathcal{G} \) into \( G \) parts. Moreover, we can construct \( |G| \) base-change matrices between these parts having same \( G_{g} \)-degree. The algorithm proceeds as the classical FGLM algorithm, but use smaller matrices: \( M_{g} \) to compute \( NF(x_{i} m, \mathcal{G}_{g}) \) and \( Q_{g} \) as base-change between \( g_{i} \) and \( \mathcal{G} \) having \( G_{g} \)-degree as \( g \).

### 6. COMPLEXITY QUESTIONS

In this section, we discuss the arithmetic complexity of the algorithms presented before. This complexity will be counted in terms of operations in \( K = k(\xi) \).

**Remark 3** A very interesting case is when \( k \) belongs to, so \( K = k \).

Assume that \( k \) is the finite group \( \mathbb{Z} \) with \( p \) prime. Then \( \xi \in k \Leftrightarrow \mathbb{N} - 1 \) splits on \( k \Leftrightarrow \mathbb{Z} / q \mathbb{Z} \Leftrightarrow \mathbb{Z} / (q-1) \mathbb{Z} \Leftrightarrow p \Rightarrow 1 \mathbb{Z} \)

By Dirichlet’s theorem, there are infinitely many such primes. Moreover, the distribution of such primes is \( 1/ \phi(e) \), where \( \phi \) is the Euler’s totient function. To compute the Gröbner basis of an ideal over \( Q \), it is more efficient to compute modulo some such primes and use modular methods to recover the original Gröbner basis.

We start by giving without proof a bound on the cost of the two first linear steps:

**Proposition 6** The cost of the diagonalization of the matrix group \( G \) is bounded by \( O((q_{1} + \cdots + q_{n})^{3}) \), and the cost of computing the \( p_{i}^{n} \) is bounded by \( O((q_{1} + \cdots + q_{n})^{3}) \) if there are \( m \) polynomials of degree less than \( d \) in \( n \) variables.

### 6.1 Dimensions of the subspaces \( R_{g} \)

#### 6.1.1 General facts about ring of invariants

The first object we are interested in is the ring of invariants \( R_{g} \), with \( G_{g} \) the diagonal matrix group. Notice that we consider the invariants in a theoretical point of view to obtain complexity bounds, so we don’t have to compute them. In this paragraph, we recall some well known facts about \( R_{g} \), without any assumption on \( G \), excepted that \( G \) is a finite matrix group of \( GL_{n}(K) \), char \( K \) doesn’t divide \( |G| \), and \( G \) is diagonalizable on \( K \). We follow the presentation of [20]. Although Sturmfels works on \( C \), the results can be easily extended since the characteristic polynomials of matrices in \( G \) fully split on \( K \).
Theorem 5 [20] The invariant ring $R^G_\delta$ is Cohen-Macaulay: there exist a set of $n$ homogeneous polynomials $\eta_1, \ldots, \eta_n$ and $t$ other invariant polynomials $\eta_{t+1}, \ldots, \eta_t$, such that $R^G_\delta = \bigoplus_{i=1}^t \eta_i \mathbb{Z}[\eta_{t+1}, \ldots, \eta_t]$.

The set of polynomials $\eta_i$ is called a set of primary invariants of $G$ and the set of $\eta_j$ a set of secondary invariants of $G$. A consequence of the previous theorem is the following proposition

Proposition 7 [20] The Hilbert (Molien) series of the ring $R^G_\delta$ is

$$H(R^G_\delta, z) = \sum_{d=0}^{\infty} \delta(R^G_\delta, d) z^d = \frac{\sum_{d=0}^{\infty} \deg(\eta_i) z^d}{\prod_{j=1}^t (1 - z^{\deg(\theta_j)})}$$

Proposition 8 [20] The set of secondary invariants depends on the chosen set of primary invariants, moreover the degrees of the primary invariants and the number of secondary invariants are related by the formula:

$$\sum_{d=0}^{\infty} \delta(R^G_\delta, d) z^d = \prod_{j=1}^t \deg(\theta_j) \big| G$$

Now, we want to give an estimation of the size of $R^G_\delta$ (set of invariant polynomials of degree $\delta$) compared to $R_\delta$. To give an estimation of the complexity of Abelian-FGLM algorithms, we are interested in two quantities.

Definition 6 We define the density of $R^G_\delta$ in $R_\delta$ and the density of $R^G$ in $R$ by

$$\delta(R^G_\delta, d) = \frac{\dim(R^G_\delta)}{\dim(R_\delta)}$$

$$\delta(R^G, d) = \lim_{D \to +\infty} \frac{\sum_{\delta=0}^{D} \dim(R^G_\delta)}{\sum_{\delta=0}^{D} \dim(R_\delta)}$$

The goal of this subsection is to prove the following theorem:

Theorem 6 The density $\delta(R^G_\delta, d)$ is well defined and is equal to $1/|G|$. If a set of primary invariants of $R^G_\delta$ can be chosen such that their degrees are relatively prime, the density $\delta(R^G_\delta)$ has the limit $\delta(R^G) = 1/|G|$ as $d$ tends to infinity.

Proof. Denote by $\alpha$ the degree of $\theta_1$, and by $\alpha$ the greatest common divisor of $\alpha_i$. We are interested in an asymptotic estimation of the coefficient in $z^{\alpha}$ in the Hilbert series of $R^G_\delta$. For now, denote by $f(z)$ the power series $1/(1 - z^{\alpha})$, and $[z^{\alpha}] f(z)$ the coefficient in $z^{\alpha}$ in the expansion of $f$. Clearly, $[z^{\alpha}] f(z) = 0$ if $\alpha$ doesn’t divide $\delta$. Then, if $\alpha|\delta$, $[z^{\alpha}] f(z) = [z^{\alpha}] \frac{1}{1 - z^{\alpha}} = \frac{1}{\prod_{i=1}^t (1 - z^{\alpha_i})}\gamma$,

where $\gamma$ is the coefficient of $z^{\alpha}$ in the partial fraction expansion, which can be obtained by

$$\gamma = \lim_{\delta \to +\infty} \frac{1}{\prod_{i=1}^t (1 + z + z^2 + \cdots + z^{\alpha_i - 1})} \text{ with } \alpha = \frac{\alpha}{1 - \frac{1}{\alpha}} \prod_{i=1}^t \alpha_i$$

Since $\lim_{n \to +\infty} \frac{1}{\prod_{i=1}^t (1 + z + z^2 + \cdots + z^{\alpha_i - 1})} = \text{constant}$,

we have obtained that:

$$[z^{\alpha}] f(z) = \left\{ \begin{array}{ll} \frac{1}{\prod_{i=1}^t \alpha_i} + o(d^{\alpha-1}) & \text{if } \alpha \nmid \delta \\ 0 & \text{if } \alpha \mid \delta \end{array} \right.$$
assuming they are homogeneous, so these ideals have same Hilbert series. Therefore, the index of regularity (homogeneous case) or the degree of regularity (affine case) are the same. For a good introduction to these notions, see [17]. From the Lazard algorithm [15] it is possible to derive a complexity bound of the computation of a Gröbner basis of zero dimensional homogeneous system.

**Theorem 8** [17] Let \( F = (f_1, \ldots, f_m) \in \mathbb{R}^m \) be a family of homogeneous polynomials generating a 0-dimensional ideal. The complexity of computing a Gröbner basis for the DRL ordering of the ideal \( (F) \) is bounded by \( O\left( (n + d_{deg}(F))^\omega \right) \).

The proof of the previous theorem is obtained by analyzing size and rank of the Macaulay’s matrix, and by the fact that a row echelon form of a matrix of size \((l,c)\) and rank \(r\) can be computed in times \(O(\ell c^r m^{-2})\) where \(\omega\) is the constant of linear algebra. In the case of an ideal \( F \) invariant under a diagonal group \( G' \), we have seen that such a matrix can be slitted into \([G']\) parts, and previous analysis of the size of the sets \( G' \) in theorem 7 proves that, under parallelization on the computations of row echelon form of the \([G']\) submatrices:

**Theorem 9** Let \( F = (f_1, \ldots, f_m) \in \mathbb{R}^m \) be a family of homogeneous polynomials generating a 0-dimensional ideal, invariant under a diagonal group \( G' \) such that a set of primary invariants of \( G' \) can be chosen with degrees relatively prime. The complexity of computing a Gröbner basis for the DRL ordering of the ideal \( (F) \) is bounded by \( O\left( (n + d_{deg}(F))^\omega \right) \).

**Remark 6** In the affine case, it seems that a bound similar to theorem 8 could be obtained (see [17], page 53), therefore we could obtain a similar improvement than in theorem 9.

**Abelian-FGLM algorithm.**

We are now interested in giving a complexity bound of the abelian-FGLM algorithm. Let \( I_G \) be a zero-dimensional ideal invariant under the diagonal group \( G \). We have to consider the two parts of the algorithm to give a complexity estimation: the construction of the multiplication’s matrices \( M_G \) and the loop in FGLM. We denote by \( d_{deg}(I_G) \) the degree of the ideal \( I_G \).

**Theorem 10** Under the hypothesis that the monomials of \( G \) are evenly distributed over the staircases \( G' \) (which is verified in practice), it is possible to obtain the reduced Gröbner basis \( G' \) from \( G' \) of \( I_G \) with \( O\left( (n + d_{deg}(I_G))^\omega \right) \) arithmetic operations in \( K \).

**Proof.** We follow the notations of [6].

- To compute the multiplication matrices, we have to compute the normal forms \(NF(m, G'z_i)\) for all \( m \in B(G'z_i) \cup M(G'z_i)\). For at most \( n d_{deg}(I_G) \) of these monomials, arithmetic computations are needed and since the staircases \( G'z_i \) have size about \( d_{deg}(I_G) / G'z_i \), each of these normal forms can be computed with \( O\left( (d_{deg}(I_G) / G'z_i)^2 \right) \) arithmetic operations in \( K \).

- In the same way, the loop in the FGLM algorithm presented in section 5 has to be done at most \( n d_{deg}(I_G) \) times. The cost of the linear operations was \( O\left( (n + d_{deg}(I_G))^2 \right) \) in the original FGLM algorithm [6] but it is reduced to \( O\left( (n + d_{deg}(I_G)^2 / G'z_i)^2 \right) \) here since the square matrices have a number of lines and columns divided by about \( |G'z_i| \). □

### 6.3 Polynomial complexity

Suppose that \( g_1, \ldots, g_m \) are affine polynomials of \( R \) of degree 2, which are individually invariant under the cyclic-\( n \) group. Usually, computing a Gröbner basis of \( I = (g_1, \ldots, g_m) \) is exponential, but we will see that we can obtain a Gröbner basis of \( I_G \) in polynomial time in \( n \) and \( m \). With \( P = (\xi_1^2), \) and \( f_i = g_i^P \), each \( f_i \) is invariant under \( D_\sigma = \text{diag}(\xi_1^2, \xi_2^2, \ldots, \xi_{n-1}^2, 1) \) and \( f_i \) as \( G_\sigma \)-degree 0.

**Lemma 2** The support of each \( f_i \) is contained in \( \{x_1, x_2^2\} \cup \{x_{n+i-1}, 1 \leq i \leq [(n - 1)/2]\} \).

**Proof.** Each \( x_i \) as \( G_\sigma \)-degree \( i \mod n \), so \( d_{deg}(x_i x_j) = i + j \mod n \) and the only monomials of degree 2 having \( G_\sigma \)-degree 0 are \( x_i x_{n+i-1} \). The only monomial of degree 1 and \( G_\sigma \)-degree 0 is \( x_n \), and 1 is also of \( G_\sigma \)-degree 0. □

**Theorem 11** A Gröbner Basis for every monomial ordering of a system of \( m \) equations invariant under \( D_\sigma = \text{diag}(\xi, \ldots, \xi^{n-1}, 1) \) can be computed in polynomial time in \( n + m \).

**Proof.** We just have to linearize the equations setting \( y_i = x_i x_{n+i-1} \) for each \( i \in \{0, \ldots, [(n - 1)/2]\} \), and perform a Gauss elimination on the equations. The result is a Gröbner Basis since the leading monomials of any pair of the obtained polynomials are coprime.

The matrix we have to reduce has \( m \) lines and \( [(n+5)/2] \) columns, and the complexity is polynomial in \( n + m \). □

**Remark 7** Similar results can be obtained for other groups and systems. This will be discussed in an extended version of this paper.

### 7. EXPERIMENTS

In this section, we report some experiments that show the improvements given by our approach on the computation of Gröbner basis of ideals invariant under a commutative group. We first present sizes of the sets \( M_G \) and \( d_{deg}(I_G) \) and then give timings obtained with an implementation of the algorithm Abelian-FGLM. A web page has been made for other softwares and benchmarks, see [9].

#### 7.1 Number of monomials of same \( G_\sigma \)-degree in \( \mathcal{M} \) or \( \mathcal{E} \)

In this subsection, we suppose that \( G \) is the cyclic group generated by the matrix \( M_G \) presented in example 1. Therefore \( G_\sigma \) is the group generated by the diagonal matrix with diagonal coefficients \((\xi, \xi^2, \ldots, \xi^{n-1}, 1)\). We want to compare the size of \( H_G \) with \(|\mathcal{M}_G|/n\) (recall that \( n \) is the order of \( G_\sigma \)). To this end we compute the relative standard deviation of the sets \(|\mathcal{M}_G|/n\) for several \( n \) and \( d \).

The following table presents some values of \( \sigma_{G_\sigma} \). We see that the monomials are very fast evenly distributed over \( G_\sigma \).

<table>
<thead>
<tr>
<th>d/n</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>10</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.33</td>
<td>0.00</td>
<td>0.20</td>
<td>0.00</td>
<td>0.094</td>
<td>0.00</td>
</tr>
<tr>
<td>1</td>
<td>0.00</td>
<td>0.14</td>
<td>0.00</td>
<td>0.09</td>
<td>0.00</td>
<td>0.01</td>
</tr>
<tr>
<td>2</td>
<td>0.20</td>
<td>0.00</td>
<td>0.10</td>
<td>0.09</td>
<td>0.02</td>
<td>0.01</td>
</tr>
<tr>
<td>3</td>
<td>0.00</td>
<td>0.09</td>
<td>0.00</td>
<td>0.02</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>4</td>
<td>0.00</td>
<td>0.09</td>
<td>0.00</td>
<td>0.02</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>5</td>
<td>0.00</td>
<td>0.09</td>
<td>0.00</td>
<td>0.02</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>6</td>
<td>0.00</td>
<td>0.09</td>
<td>0.00</td>
<td>0.02</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>7</td>
<td>0.00</td>
<td>0.09</td>
<td>0.00</td>
<td>0.02</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>8</td>
<td>0.00</td>
<td>0.09</td>
<td>0.00</td>
<td>0.02</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>9</td>
<td>0.00</td>
<td>0.09</td>
<td>0.00</td>
<td>0.02</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

**Table 1:** Repartition of the monomials under \( G_\sigma \)

way, the stairs \( G'z_i \) that appear in the abelian-FGLM algorithm have about same size. The table 2 presents some zero dimensional ideals together with the size of the group and the size of the stairs.

The final column is the relative standard deviation between \( n_{G_\sigma} \) and \(|\mathcal{M}_G|/n\).

From the experimental side, applying the \( F_4 \) algorithm on the cyclic 9 problem we obtain, in degree 15, a matrix of size \( 72558 \times 184756 \).
93917; applying the abelian-$F_2$ algorithm we obtain 9 independent matrices of roughly the same size: 8340 × 10703, 8180 × 10544, 8122 × 10484, 7804 × 10171, 7993 × 10358, 8042 × 10404, 7796 × 10162, 7967 × 10369 and 8314 × 10722.

### 7.2 Abelian-$F_2$ implementation

A first implementation of abelian of the $F_2$-algorithm [7] has been made. The algorithm constructs $(G_f)$ matrices at each degree, using the normal strategy of $F_2$. Notice that only the construction of the matrices and the operations of row-reduction on them have been parallelized, the handle of the list of critical pairs is still sequential. Surprisingly, the linear algebra can sometimes be accelerated that this handling can become the most time-consuming part whereas it is usually negligible. Therefore we report in the following tables two timings or ratios in each column: the timings are related to $F_4^{id}$ or $F_4^{id}/F_3^{id}$, which is the new abelian algorithm parallelized on $n$ cores. The first one is the total timing and the second one is only the parallelized part (that is to say, building the matrices and the linear algebra parts). The other columns contain the ratios between $F_4^{id}$ or $F_4^{id}/F_3^{id}$ and $F_2^{id}$ the standard $F_2$ applied on $f$ and $F_2^{id}$ the standard $F_2$ applied on $I_f$. In each case except table 7, the group $G$ acting on $f$ is the cyclic group $C_n$ generated by the matrix $M_0$ defined in example 1, and $G_f$ is the group generated by the diagonal matrix diag$(2, 4, 2, \ldots)$. Notice that we have to reach big-sized problems to have a significant impact. In table 3, we consider $n$ randomized equations of degree 3 stable under $C_n$, which give rise to equations of $G_{20}$-degree 0 in $I_f$. The table presents $n$ equations of degree 2, half of these equations in $I_f$ are of $G_{20}$-degree 0, and half of $G_{20}$-degree 1. In this case, the computation on $I_f$ becomes polynomial in $n$ and the handling of the critical pairs is the most time-consuming. All computations have been made on a computer with 4 Intel(R) Xeon(R) CPU E5-4620 0 @ 2.20GHz with 387 Go of RAM, on a field where $X^{26} - 1$ fully split (most of the time $\mathbb{F}_{5^{155}}$), according to remark 3.

### Speed-up

<table>
<thead>
<tr>
<th>$(n,d)$</th>
<th>$F_4^{id}$</th>
<th>$F_4^{id}/F_3^{id}$</th>
<th>$F_2^{id}$</th>
<th>$F_2^{id}/F_3^{id}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(8,5)</td>
<td>3.46s/2.48s</td>
<td>2.22/1.71</td>
<td>33.0/54.5</td>
<td></td>
</tr>
<tr>
<td>(9,3)</td>
<td>77.04s/64.21s</td>
<td>7.38/6.78</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(10,3)</td>
<td>762.60/72s</td>
<td>10.0/1.13</td>
<td>160.9/182</td>
<td></td>
</tr>
<tr>
<td>(11,3)</td>
<td>22162620/52s</td>
<td>13.0/1.40</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 3: $n$ cubic equations of $G_{20}$-degree 0

<table>
<thead>
<tr>
<th>$(n,d)$</th>
<th>$F_4^{id}$</th>
<th>$F_4^{id}/F_3^{id}$</th>
<th>$F_2^{id}$</th>
<th>$F_2^{id}/F_3^{id}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(25,2)</td>
<td>0.25s/0.00s</td>
<td>1.9/4.5</td>
<td>56.6/230</td>
<td></td>
</tr>
<tr>
<td>(30,2)</td>
<td>0.58s/0.11s</td>
<td>1.5/4.6</td>
<td>80.7/415</td>
<td></td>
</tr>
<tr>
<td>(35,2)</td>
<td>0.86s/0.11s</td>
<td>1.9/8.5</td>
<td>228.5/1735</td>
<td></td>
</tr>
<tr>
<td>(40,2)</td>
<td>1.55s/0.21s</td>
<td>2.4/8.5</td>
<td>508.0/2174</td>
<td></td>
</tr>
<tr>
<td>(45,2)</td>
<td>2.31s/0.34s</td>
<td>2.4/10.7</td>
<td>664.5/5043</td>
<td></td>
</tr>
<tr>
<td>(50,2)</td>
<td>3.96s/0.45s</td>
<td>2.6/13.3</td>
<td>753.8/5504</td>
<td></td>
</tr>
<tr>
<td>(55,2)</td>
<td>6.98s/0.66s</td>
<td>2.3/15.0</td>
<td>1207/12750</td>
<td></td>
</tr>
<tr>
<td>(60,2)</td>
<td>10.85s/0.96s</td>
<td>2.8/17.2</td>
<td>1294/14330</td>
<td></td>
</tr>
</tbody>
</table>

### Table 4: $n$ quadratic equations of $G_{30}$-degree 0 or 3

Table 5 presents timings on the Cyclic-$n$ problem, we see that Cyclic-11 could be solved in less than 8 hours although it is untractable with $F_2$. Table 7 is an example of ideals generating by ran-

### Speed-up

<table>
<thead>
<tr>
<th>$n$</th>
<th>$F_4^{id}/F_3^{id}$</th>
<th>$F_4^{id}$</th>
<th>$F_4^{id}/F_3^{id}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>0.305/0.40s</td>
<td>2.5/1.7</td>
<td>3.7/4.8</td>
</tr>
<tr>
<td>9</td>
<td>0.10t/s/71s</td>
<td>4.3/5.4</td>
<td>7.0/8.4</td>
</tr>
<tr>
<td>10</td>
<td>3.34t/290s</td>
<td>13.2/14.8</td>
<td>41.1/47.23</td>
</tr>
<tr>
<td>11</td>
<td>275.39/254/4s</td>
<td>67.5/89.4</td>
<td></td>
</tr>
</tbody>
</table>

### Table 5: NTRU equations

### Speed-up

<table>
<thead>
<tr>
<th>$n$</th>
<th>$F_4^{id}/F_3^{id}$</th>
<th>$F_4^{id}$</th>
<th>$F_4^{id}/F_3^{id}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>3.64s/2.52s</td>
<td>3.6/4.8</td>
<td>31.3/44.4</td>
</tr>
<tr>
<td>9</td>
<td>4.4</td>
<td>1.99/1.29</td>
<td>2.4/3.2</td>
</tr>
<tr>
<td>10</td>
<td>6.2</td>
<td>2.93/2.43</td>
<td>2.2/2.5</td>
</tr>
<tr>
<td>11</td>
<td>5.5</td>
<td>7.0/4.5</td>
<td>11.8/16.2</td>
</tr>
<tr>
<td>12</td>
<td>6.4</td>
<td>9.2/6.72s</td>
<td>17.7/19.8</td>
</tr>
<tr>
<td>13</td>
<td>8.2</td>
<td>10/10.106s</td>
<td>12.1/12.3</td>
</tr>
<tr>
<td>14</td>
<td>10</td>
<td>70/668s</td>
<td>11.1/11.4</td>
</tr>
</tbody>
</table>

### Table 7: $n = k_1 + k_2$ cubic equations invariant under $C_{k_1} \times C_{k_2}$

8. REFERENCES


