Théorie des invariants

Tristan Vaccon

octobre 2012

Table des matières

Lien avec les leçons d'algèbre de l'agrégation

101 : groupe opérant sur un ensemble
(105 : groupe des permutations d'une ensemble fini)
107 : représentations
114 : séries formelles
115 : fractions rationnelles
117 : Polynômes à n indéterminées
118 : notion de dimension
120 : dimension, rang
123 : déterminant
145 : combinatoire (possible)
(150 : racines d'un polynôme)
243 : série entière, comme exemple

1 Programme d'Erlangen

L'objectif du *Programme d'Erlangen*, lancé en 1872 par Félix Klein, est de fonder la géométrie sur les notions d'actions de groupe et d'invariants.

Géométrie	Espace	Groupe	Invariants Globaux	Fonctions invariantes
Affine	Espace affine R^n	$GA(R^n) \simeq R^n \rtimes GL_n(R)$ Groupe des isomorphismes affines de R^n	Sous-espaces affines	
Euclidienne	Espace euclidien $(R^n, (\ ,\ ))$	$Isom(R^n) \simeq R^n \rtimes O_n(R)$ Groupe des isomorphismes affines de R^n	Sous-espaces affines, sphères	distances, produits scalaires
Sphérique	Sphère euclidiene S^n	$O_{n+1}(R)$	Grands cercles	
Projective	Espace projectif PR_n	PG_nR, groupe projectif	Sous-espaces projectifs	birapport

Exemple. Une des visions de la relativité restreinte donne quelque chose comme :
- L'espace-temps est un espace affine réel de dimension 4.
- Son espace vectoriel tangent est muni d'une forme quadratique de signature $(1,3)$ (c'est-à-dire, quitte à choisir une base, elle s'écrit $t^2 - x^2 - y^2 - z^2$, métrique de Minkowski).
- Les transformations vectorielles qui préservent cette forme quadratique forment le groupe de Lorentz $O_{1,3}$.
- Les transformations affines qui la préservent forment le groupe de Poincaré $\mathbb{R}^4 \rtimes O_{1,3}$.
- Les lois de la physique sont des invariants pour ce groupe ?

Exemple. On considère $M_n(A)$ pour A anneau intègre, et on considère l'action de $GL_n(A)$ sur $M_n(A)$ par similitude : $P\dot{M} = P^{-1}MP$.

Alors on connait les orbites (théorie des invariants de similitude) et, au moins dans le cas d'un corps (peut-être dans le cas général), on connait toutes les fonctions polynomiales en les coefficients des matrices qui sont invariantes : ce sont les polynômes engendrés par les coefficients du polynôme polynôme caractéristique des matrices de $M_n(k)$.

2 La théorie classique des invariants

Définition 2.1. Let k be a field. For $g \in GL_n(k)$ and $P \in k[X_1, \ldots, X_n]$, we note $g \cdot P = P(g^{-1}(X_1, \ldots, X_n)^t)$.

This provides a group action of $GL_n(k)$ over $k[X_1, \ldots, X_n]$.

Définition 2.2. Let $G \subset GL_n(k)$ be a finite matrix group, then $f \in k[X_1, \ldots, X_n]$ is invariant under G if for all $A \in G$, $f(X) = f(A.X)$.

The set of all invariant polynomials is denoted $k[X_1, \ldots, X_n]^G$, and is naturally a subring of $k[X_1, \ldots, X_n]$ containing the constant polynomials, and is called the ring of invariants of $k[X_1, \ldots, X_n]$ under the action of G.

Proposition 2.3. *Let $G \subset GL_n(k)$ be a finite matrix group, then $f \in k[X_1, \ldots, X_n]$ is invariant under G if and only if all of its homogeneous components are.*

Remarque. If $g \in GL_n(k)$, then by proposition 2.3, the action of g over $k[X_1, \ldots, X_n]_d$ (for some $d \in \mathbb{N}^*$) correspond to that of $Sym^d(g)^{-1} \in GL_n(k[X_1, \ldots, X_n]_d) = GL_n(Sym^d(k[X_1, \ldots, X_n]_1))$.

3 Polynômes symétriques

Let R be a domain and k be a field. The most famous example is given by the symmetric polynomials of $k[X_1, \ldots, X_n]$. Indeed :

Définition 3.1. A polynomial is called symmetric if for any permutation matrix A, $f(A.X) = f(X)$.

Définition 3.2. In $R[x_1, \ldots, x_n]$, the elementary symmetric functions $\sigma_1, \ldots, \sigma_n$ are defined by :

$$\sigma_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} x_{i_1} \ldots x_{i_k}.$$

A lot is known about symmetric polynomials :

Théorème 3.3. *Every symmetric polynomial in $R[x_1, \ldots, x_n]$ can be written uniquely as a polynomial in the elementary symmetric functions $\sigma_1, \ldots, \sigma_n$.*

Proposition 3.4. *We consider the ring $k[x_1, \ldots, x_n, y_1, \ldots, y_n]$ with a monomial ordering such that any monomial involving one of the x_i is greater than all the polynomial of $k[y_1, \ldots, y_n]$ (for instance, the lexicographical ordering). Let G be Gröbner basis of $I = \langle \sigma_1 - y_1, \ldots, \sigma_n - y_n \rangle \subset k[x_1, \ldots, x_n, y_1, \ldots, y_n]$. Let $f \in k[x_1, \ldots, x_n]$, let g be the remainder of the division of f by G, then f is symmetric if and only if $g \in k[y_1, \ldots, y_n]$ and then, $f = g(\sigma_1, \ldots, \sigma_n)$ is the unique expression of f as a polynomial in the elementary symmetric functions.*

Proposition 3.5 (Newton's identities)**.** *Let $n \in \mathbb{N}^*$ and $k \in \mathbb{N}$. Then*

$$s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k k\sigma_k = 0$$

for $1 \leq k \leq n$, and for $k > n$:

$$s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{n-1}\sigma_{n-1}s_{k-n+1} + (-1)^n \sigma_n s_{k-n} = 0.$$

Démonstration. We write the generating series of the s_k :

$$\sum_{k\geqslant 1} s_k T^k = \sum_{i=1}^{n}\sum_{k\geqslant 1} x_i^k T^k = \sum_{i=1}^{n} \frac{x_i T}{1 - x_i T}.$$

Let P be a polynomial whose roots are the "inverses" of the x_i : $P(T) := \prod_{i=1}^{n}(1 - x_i T) = \sum_{i=1}^{n}(-1)^k \sigma_k T^k$.

We can calculate the logarithmic derivative of P and conclude :

$$\sum_{k\geqslant 1} s_k T^k = \sum_{i=1}^{n} \frac{x_i T}{1 - x_i T} = -T\frac{P'(T)}{P(T)} = \frac{\sum_{k=0}^{n}(-1)^{k-1}k\sigma_k T^k}{\sum_{k=0}^{n}(-1)^k \sigma_k T^k}.$$

□

Théorème 3.6. *If k is a zero-characteristic field, then every symmetric polynomial in $k[x_1, \ldots, x_n]$ can be written as a polynomial in the s_r, where $s_r = x_1^r + \cdots + x_n^r$, for $r \in \{1, \ldots, n\}$.*

Démonstration. We have $s_1 = \sigma_1$. If we assume that that for some $l \in \mathbb{N}$, $l > 1$, any σ_t, $t \in \{1, \ldots, l-1\}$, can be written as a polynomial in the s_r, where $s_r = x_1^r + \cdots + x_n^r$, for $r \in \{1, \ldots, n\}$, then from Newton's identities :

$$\sigma_r = (-1)^{r-1}\frac{1}{r}(s_r - \sigma_1 s_{r-1} + \cdots + (-1)^{r-1}\sigma_{r-1}s_1),$$

which can be written since $char(k) = 0$, and σ_r is a polynomial in the s_r, where $s_r = x_1^r + \cdots + x_n^r$, for $r \in \{1, \ldots, n\}$. Hence, by induction, any of the σ_r, $r \in \mathbb{N}^*$, is a polynomial in the s_r, where $s_r = x_1^r + \cdots + x_n^r$, for $r \in \{1, \ldots, n\}$, and finally, with the fundamental theorem of symmetric polynomials, it is also true for any symmetric polynomial. □

4 Invariant pour des groupes finis

4.1 Noether's Theorem

$k[x_1, \ldots, x_n]^G$ being defined, we shall study whether, as for symmetric polynomials, $k[x_1, \ldots, x_n]^G$ is finitely generated or not, and if we can find some generators for it.

Définition 4.1. Let $G \subset GL_n(k)$ be a finite matrix group, we define the **Reynolds operator** of G by the map $R_G : k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]$ defined by $R_G(f)(x) = \frac{1}{\sharp G} \sum_{A \in G} f(A.x)$ for all $f \in k[x_1, \dots, x_n]$.

Proposition 4.2. *R_G is clearly a k-linear map such that $R_G(k[x_1, \dots, x_n]) \subset k[x_1, \dots, x_n]^G$.*

If $f \in k[x_1, \dots, x_n]^G$ then $R_G(f) = f$.

Therefore, R_G is a (linear) projection over its image $R_G(k[x_1, \dots, x_n])$.

All this will reveal to be enough to prove Noether's theorem.

Théorème 4.3 (Noether)**.** *Let $G \subset GL_n(k)$ be a finite matrix group, with $char(k) = 0$, then $k[x_1, \dots, x_n]^G = k\left[R_G(x^\beta) : |\beta| \leq |G|\right]$. Hence, $k[x_1, \dots, x_n]^G$ is finitely generated by homogeneous invariant polynomials.*

Démonstration. If $f = \sum_\alpha c_\alpha x^\alpha \in k[x_1, \dots, x_n]^G$, then $f = R_G(f) = R_G\left(\sum_\alpha c_\alpha x^\alpha\right) = \sum_\alpha c_\alpha R_G(x^\alpha)$. Hence, every invariant polynomial is a k-linear combination of the $R_G(x^\alpha)$. We now shall prove that for all α, $R_G(x^\alpha) \in k\left[R_G(x^\beta) : |\beta| \leq |G|\right]$.

We can write that $(x_1 + \dots + x_n)^k = \sum_{|\alpha|=k} a_\alpha x^\alpha$, with the a_α positive natural numbers (and with multinomial formula, we know an expression of the a_α).

If A is a matrix, let A_i denote the i-th row of A. We have by definition $(Ax)^\alpha = (A_1 x)^{\alpha_1} \dots (A_n x)^{\alpha_n}$.

We introduce n new variables $u_1, \dots, u_n$, and we now have $(u_1 A_1.x + \dots + u_n.A_n x)^k = \sum_{|\alpha|=k} a_\alpha (A.x)^\alpha u^\alpha$. If we sum over all $A \in G$, we get : $\sum_{A \in G}(u_1 A_1.x + \dots + u_n A_n.x)^k = \sum_{|\alpha|=k} a_\alpha \left(\sum_{A \in G}(Ax)^\alpha\right) u^\alpha = \sum_{|\alpha|=k} b_\alpha R_G(x^\alpha) u^\alpha$. In fact $b_\alpha = |G| a_\alpha$.

Let $U_A = u_1 A_1.x + \dots + u_n A_n.x$, and $S_k = \sum_{A \in G} U_A^k$, then we have $S_k = \sum_{|\alpha|=k} b_\alpha R_G(x^\alpha) u^\alpha$.

With the last theorem of the previous subsection about symmetric polynomials, any polynomial in the U_A and symmetric in the U_A can be written as a polynomial in the S_k, $0 \leq k \leq |G|$.

Hence, if $k \in \mathbb{N}$, $\sum_{|\alpha|=k} b_\alpha R_G(x^\alpha) u^\alpha = S_k = F(S_1, \dots, S_{|G|})$ for some polynomial $F \in k\left[Y_1, \dots, Y_{|G|}\right]$.

Thus, $\sum_{|\alpha|=k} b_\alpha R_G(x^\alpha) u^\alpha = F\left(\sum_{|\beta|=1} b_\beta R_G(x^\beta) u^\beta, \dots, \sum_{|\beta|=|G|} b_\beta R_G(x^\beta) u^\beta\right)$.

We can expand the last expression and we get for the coefficient corresponding to u^α that $b_\alpha R_G(x^\alpha)$ is a polynomial in the $R_G(x^\beta)$ with $|\beta| \leq |G|$.

Since $char(k) = 0$, $|G| \neq 0$ and $b_\alpha = |G| a_\alpha \neq 0$, we have $R_G(x^\alpha)$ in the desired form.

Therefore,$\forall \alpha, R_G(x^\alpha) \in k\left[R_G(x^\beta) : |\beta| \leq |G|\right]$ and since $R_G(k[x]) = k[x]^\Gamma$, the result is proven. $\square$

Remarque. We can also prove the fact that $k[x_1, \ldots, x_n]^G$ is finitely generated by homogeneous invariant polynomials in any characteristic, by considering Hilbert's Basis Theorem, as long as Reynold's operator is well defined, but this proof does not give any bound considering the degrees of generators.

Now we can provide a criteria to decide, given $f_1, \ldots, f_m$, whether a polynomial f is in $k[f_1, \ldots, f_m]$ or not, and if so to find a way to find a polynomial g so as $f = g(f_1, \ldots, f_m)$.

Proposition 4.4. *We consider the ring $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ with a monomial ordering such that any monomial involving one of the x_i is greater than all the polynomial of $k[y_1, \ldots, y_m]$. Let G be Gröbner basis of $I = \langle f_1 - y_1, \ldots, f_m - y_m \rangle \subset k[x_1, \ldots, x_n, y_1, \ldots, y_m]$.*

Let $f \in k[x_1, \ldots, x_n]$, let g be the remainder of the division of f by G, then $f \in k[f_1, \ldots, f_m]$ if and only if $g \in k[y_1, \ldots, y_n]$ and then, $f = g(f_1, \ldots, f_n)$ is an expression of f as a polynomial in the $f_1, \ldots, f_m$.

4.2 Hironaka decomposition

Invariant rings are not just finitely generated, there are also *Cohen-Macaulay*, which will make them easier to handle.

Théorème 4.5 (Hironaka decomposition)**.** *The invariant ring $k[x]^\Gamma$ of a finite matrix group $\Gamma \subset GL(k^n)$ admits a Hironaka decomposition $k[x]^\Gamma = \bigoplus_{i=1}^t \eta_i k[\theta_1, \ldots, \theta_n]$ where the η_i and the θ_j are invariants polynomials.*

Définition 4.6. The η_i are called *primary invariants* and the θ_j are called *secundary invariants.*

4.3 Hilbert Series

In this subsection, we will study an important tool for more advanced algorithms to compute generators of an invariant ring, the Hilbert series.

Définition 4.7. A vector space V which decomposes into a direct sum of the form $V = \bigoplus_{n \in \mathbb{N}} V_d$ is called a **graded vector space** (or a $\mathbb{N}$-graded vector space, since we might consider indexation over another set). If $V = \bigoplus_{d=k}^{+\infty} V_d$ with $k \in \mathbb{Z}$, we also say that V is a graded vector space.

Définition 4.8. For a graded vector space $V = \bigoplus_{d=k}^{+\infty} V_d$ such that V_d is finite dimensional for all d, we define the **Hilbert series** of V as the formal Laurent series : $H(V, t) = \sum_{d=k}^{+\infty} \dim(V_d) t^d$.

Proposition 4.9. *If f has degree d in $V = k[f]$ seen (naturally) as a graded vector space, then $H(k[f], t) = (1 - t^d)^{-1}$.*

Démonstration. Indeed, if x has degree d, then $\dim V_l = 0$ if l is not divisible by d, and $\dim V_l = 1$ elsewhere. Thus, $H(k[x], t) = \sum_{k \in \mathbb{N}} (t^d)^k = (1 - t^d)^{-1}$. □

From this example, we can easily deduce the Hilbert Series of $k[x_1, \ldots, x_n]$ where the x_i are of degree $d_i > 0$.

Remarque. Let E_1, E_2 be two finite-dimensional vector spaces on k (with dimension d_1 and d_2). Then $E_1 \otimes E_2$ is a vector space of dimension $d_1 \times d_2$.

Indeed, if V and W are two graded vector spaces, the their tensor product $V \otimes W$ can naturally be seen as a graded vector space, with $(V \otimes W)_d = \bigoplus_{d_1+d_2=d} V_{d_1} \otimes W_{d_2}$. Then, as obvious Cauchy product, $H(V \otimes W, t) = H(V, t)H(W, t)$.

Therefore, if we consider $k[x_1, \ldots, x_n]$ where x_i is of degree $d_i > 0$, since $k[x_1, \ldots, x_n] = k[x_1] \otimes \ldots k[x_n]$, then

Proposition 4.10. $H(k[x_1, \ldots, x_n], t) = \frac{1}{(1-t^{d_1})\ldots(1-t^{d_n})}$.

4.4 Molien's Formula

The Hilbert series of an invariant ring can be very easily computed with the so-called Molien's formula. Before enouncing this theorem, we may show a first interesting proposition coming from representation and character theory :

Proposition 4.11. *Let G be a finite group with a reprentation : a morphism $\rho : G \to GL(V)$, with V a finite dimensional k-vector space, with $char(k) = 0$, then $\dim V^G = \frac{1}{\sharp G} \sum_{g \in G} \chi(g)$, where $\chi : G \to \mathbb{C}$, $g \mapsto tr(\rho(g))$ (χ is a character).*

Démonstration. Like we did before, we can define $R_G : V \to V$, $v \mapsto \frac{1}{\sharp G} \sum_{g \in G} \rho(g).v$, which is a linear application.

We still have that $Im(R_G) = V^G$ and R_G is the identity on V^G, thus $\dim V^G = tr(R_g)$. Since the trace is a morphism, $\dim V^G = tr(R_G) = \frac{1}{\sharp G} \sum_{g \in G} \chi(g)$ and the result is proven. □

Théorème 4.12. *Let G be a finite matrix group of $GL_n(k)$ acting on $k[X_1, \ldots, X_n]$, with $char(k) = 0$. Then $H(k[X_1, \ldots, X_n]^G, t) = \frac{1}{\sharp G} \sum_{A \in G} \frac{1}{\det(1-tA)}$.*

Démonstration. Let $A \in G$. We first show that :

$$\sum_{d \in \mathbb{N}} \chi_d(\rho_d(A)) t^d = \frac{1}{det(Id - tA)}.$$

Since G is finite, there exists $n \in \mathbb{N}$ such that $A^n = Id$, and thus, A is diagonaliable, in an algebraic closure of k : there exists $P \in GL_n(\overline{k})$ such that $P^{-1}AP = \begin{bmatrix} a_1 & & O \\ & \ddots & \\ 0 & & a_n \end{bmatrix}$, and thus,

$$\det(Id - tA) = (1 - a_1 t) \dots (1 - a_n t).$$

Now, if we consider V_d the subspace of the homogeneous polynomial of degree d, with $d \in \mathbb{N}$, and if $\alpha \in \mathbb{N}^n$ with $|\alpha| = d$, then $A \cdots (P \cdot x)^\alpha = a_1^{\alpha_1} \dots \alpha_n^{\alpha_n} (P \cdot x)^\alpha$. Hence, we have naturally a basis of eigenvectors, and the aigenvalues are the $a_1^{\alpha_1} \dots a_n^{\alpha_n}$ with $|\alpha| = d$.

The $(P \cdots x)$ are indeed a basis of $k[X_1, \dots, X_n]_d$ since we have a group morphism $\rho_d : GL_n(\overline{k}) \to GL(k[X_1, \dots, X_n]_d)$ and thus $\rho_d(P) \in GL(k[X_1, \dots, X_n]_d$ and $(P \cdot x) = (\rho_d(P)(x))$ is a basis. Thus, we have that, if we consider the obvious homomorphism : $\rho_d : G \to GL(V_d)$, with the previous proposition, $\chi_d(\rho_d(A)) = \sum_{|\alpha|=d} a_1^{\alpha_1} \dots a_n^{\alpha_n}$, et $\dim V_d^G = \frac{1}{\sharp G} \sum_{A \in G} \chi_d(\rho_d(A))$.

If we take one $A \in G$, we then obtain that $\sum_{d \in \mathbb{N}} \chi_d(\rho_d(A)) t^d = \sum_{d \in \mathbb{N}} \sum_{|\alpha|=d} a_1^{\alpha_1} \dots a_n^{\alpha_n} t^d$.

As Cauchy product, we obtain

$$\sum_{d \in \mathbb{N}} \chi_d(\rho_d(A)) t^d = \prod_{j=1}^{n} \sum_{k_j=0}^{+\infty} (a_j t)^{k_j} = \prod_{j=1}^{n} \frac{1}{1 - a_j t} = \frac{1}{det(Id - tA)}.$$

On the other hand, we can sum on all $A \in G$ to obtain

$$\frac{1}{\sharp G} \sum_{A \in G} \sum_{d \in \mathbb{N}} \chi_d(\rho_d(A)) t^d = \sum_{d=0}^{+\infty} \frac{1}{\sharp G} t^d \sum_{A \in G} \chi_d(\rho_d(A)) = \sum_{d=0}^{+\infty} \dim(V_d^G) t^d = H(k\left[X_1, \dots, X_n\right]^G, t).$$

Finally $H(k\left[X_1, \dots, X_n\right]^G, t) = \frac{1}{\sharp G} \sum_{A \in G} \frac{1}{\det(1 - tA)}$.

□

Remarque. This proof is not effective in positive characteristic since we no longer have the fact that the trace of a projector is equal to its rank.

Yet, the result still somehow holds in any characteristic for group whose order is not divisible by the characteristic of the field, with some "lifting to $\mathbb{C}$" morphism to define a determinant and eigenvalues.

Since what we consider is a finite group of matrix, G, of order N. Then the order of any element of G divides N, and therefore, the eigenvalues of the elements of G are all Nth roots of the unity. We can define a group homomorphism between Nth roots of the unity in k and Nth roots of the unity in $\mathbb{C}$.

Then by taking for the trace the sum of the image of the eigenvalues by this morphism, and the determinant to be their product, it can be shown that the result still holds [4].

4.5 Computation of Primary and secondary Invariants

Linear Algebra + dimension ! (+ proba...)
We remark that for some $d \in \mathbb{N}^*$, and if the π_i generates G, then :

$$\bigcap Ker(Sym^d(\pi_i)^- Id_{k[x]}).$$

Algorithm 1 function primary(Pi,R,param), where Pi is a generating set of G, param is an integer parameter, $R = k[X_1, \ldots, X_n]$

```
d :=0 ;i :=0 ;
n :=Rank(R) ; k :=BaseRing(R) ;
P :=∅ ;
repeat
  d :=d+1 ;
  Compute a basis B of k[X_1, ..., X_n]_d^G, with Pi and some linear algebra ;
  while n − i > dim(⟨P ∪ B⟩) do
    if IsFinite(k) then
      Find a new k-linear combination q of B
      if dim(⟨P⟩) > dim(⟨P ∪ {q}⟩) then
        i :=i+1 ; Append( P,q) ;
      end if
      if all elements of Vect(B) have been tried then
        Break the WHILE loop ;
      end if
    else
      i :=i+1 ;
      Find a k-linear combination of B, p_i such that dim(⟨P⟩) >
      dim(⟨P ∪ {p_i}⟩) {and that is the tricky part...}
      Append( P,p_i) ;
    end if
  end while
until i == n
return P ;
```

We have said that if G is a finite matrix group in $GL_n(k)$, then $k[X_1, \ldots, X_n]^G$ is a free module as a module over as a module over $F = k[f_1, \ldots, f_n]$, where the f_i are primary invariants of $k[X_1, \ldots, X_n]^G$.

Therefore, we can write :

$$k[X_1, \ldots, X_n]^G = Fg_1 \oplus \cdots \oplus Fg_s$$

for some g_j. Such decomposition of $k[X_1, \ldots, X_n]^G$ is called a **Hironaka decomposition**.

We have seen that $H(F, t) = \frac{1}{\prod(1-t^{d_i})}$ where d_i is the total degree of f_i. Hence,

$$H(k[X_1, \ldots, X_n]^G, t) = \frac{\sum_{j=1}^{s} t^{e_j}}{\prod_{i=1}^{r}(1 - t^{d_i})}$$

where e_j is the total degree of g_j.

Therefore, if we know the Molien series of $k[X_1, \ldots, X_n]^G$ and the primary invariants, we can deduce the e_j and therefore, have a good idea of where to find the g_j. That is the idea of the following algorithm.

Linear Algebra !

Algorithm 2 function secundary(P,Pi,G,R), where Pi is a generating set of G and P primary invariants of $k[X_1, \ldots, X_n]^G$, $R = k[X_1, \ldots, X_n]$

```
G_i := ∅
G :=grobner(P,R,grevlexord) ;
Calculate the e_1, ..., e_m with P and Molien's formula
for i in {1, ..., m} do
    Compute a basis B of k[X_1, ..., X_n]^G_{e_i}, with Pi and some linear algebra ;
    Find an element of B such that its rest modulo G is linearly independant to
    the rests of the elements of G_i modulo G
end for
return G_i ;
```

Références

[1] Ramis, Warusfel, Moulins et al. Cours de Mathématiques pures et appliquées : Volume 1, Algèbre et Géométrie

[2] Peyré, Gabriel L'algèbre discrète de la transformée de Fourier

[3] Sturmfels, Bernd Algorithms in Invariant Theory

[4] Derksen & Kemper Computational Invariant Theory

[5] Cox, Little & O'Shea Ideals, Varieties, And Algorithms : An Introduction to Computational Algebraic Geometry And Commutative Algebra