CALCUL D'UN SYSTÈME DE GÉNÉRATEURS DE
L'IDÉAL DES RELATIONS ENTRE LES RACINES D'UN POLYNÔME

Les algorithmes classiques de recherche de groupe de Galois d'un polynôme $f$ unitaire, à coefficients dans un corps $K$ et séparable, utilisent la factorisation de certaines résolvantes. Le problème que nous nous posons est de "compléter" ce genre d'algorithmes de telle sorte que l'on obtienne explicitement les relations entre les racines de $f$. En clair, si l'on écrit

$$f = T^n - a_1 T^{n-1} + \cdots + (-1)^n a_n \qquad \in K[T]$$

il s'agit de trouver un idéal maximal de l'algèbre des polynômes $K[X_1, \ldots, X_n]$ contenant l'idéal $\Sigma$ (idéal des relations symétriques de $f$) engendré par les polynômes $\sigma_1 - a_1, \ldots, \sigma_n - a_n$ où $\sigma_i$ désigne le $i$-ième polynôme symétrique élémentaire en $X_1, \ldots, X_n$. Ce problème revient à trouver un idéal maximal de l'algèbre-quotient (nommée l'algèbre de décomposition universelle de $f$)

$$D = K[X_1, \ldots, X_n]/\Sigma$$

en raison de la correspondance entre les idéaux de $D$ et ceux de $K[X_1, \ldots, X_n]$ contenant $\Sigma$.

L'algèbre de décomposition universelle d'un polynôme séparable possède la propriété fondamentale d'être une algèbre galoisienne sur $K$ pour le groupe symétrique $S_n$ : en effet, il s'agit d'une algèbre étale (i.e. de dimension finie et séparable) et l'ensemble des points invariants sous l'action de $S_n$ est exactement $K$. Étant donné un idéal maximal $M$ de $D$, le quotient $D/M$ est un corps de décomposition de $f$, si bien que le stabilisateur $\mathrm{Stab}_{S_n}(M)$ (appelé également groupe de décomposition de $M$) est égal au groupe de Galois de $f$.

La théorie des algèbres galoisiennes donne un cadre tout-à-fait approprié pour prouver de nombreux résultats en théorie de Galois "classique". Par exemple, voici une propriété permettant de construire un idéal $I$ de $D$ tel que le quotient $D/I$ soit une algèbre galoisienne sur $K$ de groupe de Galois $\Gamma \subset S_n$ où $\Gamma$ contient le groupe de Galois du polynôme $f$, désigné par $\mathrm{Stab}_G(M)$.

**Propriété.** *Soit $D$ une algèbre galoisienne de groupe $G$ sur un corps $K$, $x \in D$ dont la résolvante $L = \prod_{y \in G.x}(T - y)$ est supposée séparable, $P \in K[T]$ un polynôme irréductible divisant $L$ et $M$ un idéal maximal contenant $y = P(x)$. Notons $O_x$ et $O_y$ les orbites respectives de $x$ et $y$ sous l'action de $\mathrm{Stab}_G(M)$, et enfin $I$ l'idéal de $D$ engendré par l'orbite $O_y$. Alors $D/I$ est une algèbre galoisienne dont le groupe de Galois est $\Gamma = \mathrm{Stab}_G(O_x)$ ($\Gamma$ contient $\mathrm{Stab}_G(M)$).*

Dans la pratique, on peut construire les orbites $O_x$ et $O_y$ sans connaître l'idéal maximal $M$, ou même son stabilisateur $\mathrm{Stab}_G(M)$.

**Autre version de cette propriété.** *Soit $D$ une algèbre galoisienne de groupe $G$ sur un corps $K$, $x \in D$ dont la résolvante $L = \prod_{y \in G.x}(T - y)$ est supposée séparable, deux polynômes $P, Q \in K[T]$ tels que $L = PQ$, et $E \subset G.x$ de cardinal $\deg(P)$. Si l'idéal $I \subset D$ engendré par l'ensemble $P(E)$ est propre, (ce qui est équivalent $\prod_{z \in E} Q(z) \neq 0$), alors $D/I$ est une algèbre galoisienne dont le groupe de Galois est $\Gamma = \mathrm{Stab}_G(E)$.*

Avec cette propriété, si $D$ est l'algèbre de décomposition universelle d'un polynôme $f$ séparable, nous sommes en mesure faire du calcul relatif par rapport au groupe $\Gamma$ (en calculant une base de Gröbner de $I$ par exemple), car $I$ contient toutes les relations $\Gamma$-invariantes entre les racines de $f$ dans le quotient $D/M$ où $M$ est un idéal maximal quelconque contenant $I$.

Enfin, on montre facilement que $\Gamma$ est le groupe de Galois de $f$ si et seulement si $I$ est un idéal maximal. Si ce n'est pas le cas, on recommence le processus (factorisation d'une nouvelle résolvante et utilisation de la propriété ci-dessus) pour déterminer un idéal $I'/I$ de $D/I$ tel que $D/I'$ soit encore une algèbre galoisienne de groupe $\Gamma' \subset \Gamma$.