Université de Limoges

Sujet de projet M1 CRYPTIS - Calcul formel

Nombres algébriques et résultant

Contexte. Ce projet porte sur l'analyse des nombres algébriques sur un corps, *i.e*, les éléments d'une extension de corps qui sont annulés par un polynôme à coefficients dans le corps de base. À titre d'exemple, $\sqrt{2}$ est un nombre algébrique sur $\mathbb{Q}$, car annulé par $X^2 - 2 \in \mathbb{Q}[X]$. On remarque de plus, qu'il n'existe pas de polynôme de degré strictement inférieur à 2 qui annule $\sqrt{2}$ (pourquoi ?). Le polynôme unitaire de degré minimal annulant le nombre algébrique α est appelé le *polynôme minimal* de α. De plus, il s'avère que l'ensemble des nombres algébriques forment une extension du corps de base, *i.e*, la somme, l'opposé et le produit et l'inverse de nombres algébriques sont des nombres algébriques. Il existe des preuves constructives de ce résultat : étant donnés deux entiers algébriques dont on connaît les polynômes minimaux, on peut construire un polynôme annulant leur somme à l'aide d'un résultant.

Objectif du projet. L'objectif de ce projet est d'abord de se familiariser avec la notion de nombre algébrique, puis ensuite d'implémenter le calcul de polynômes annulateurs grâce au résultant. En particulier, le rapport devra contenir un résumé des aspectes théoriques du sujet (définition d'un nombre algébrique, preuve de la stabilité selon les opérations arithmétiques, etc), une partie contenant votre implémentation et sa description, et enfin quelques illustrations de votre implémentation par des exemples. On vous encourage également à aller plus loin. Par exemple, votre implémentation pourrait permettre de calculer le polynôme minimal de la somme, du produit, de l'opposé et de l'inverse d'un nombre algébrique, ou bien vos exemples pourraient également faire intervenir des polynômes à coefficients dans un corps fini.

Référence. Une point de départ est le chapitre 12 de "Mathématiques L3 algèbre", écrit sous la direction de Aviva Szpirglas.