USS: Introduction to mathematical cryptography
Thursday August 4 problems

The canonical embedding

For these problems, consider $K = \mathbb{Q}(\sqrt[3]{2})$, the field generated by the element α such that $\alpha^3 = 2$. This is of degree 3 over $\mathbb{Q}$, and note that the ring of integers of K is monogenic and generated by α. If you do not know about them already, you might want to read about complex third roots of unity before starting this problem.

1. How many real embeddings does K have? How many complex embeddings? What does each embedding do to α?
2. Give a basis of the lattice $\Lambda = \sigma(R)$, where R is the ring of integers of K and σ is the canonical embedding.
3. Compute the image of the following elements under the canonical embedding: 1, α, $1 + \alpha$, $\alpha + \alpha^2$.
4. Compare the multiplication of the image of elements under the canonical embedding to the multiplication of elements when expressed as a polynomial in α. In particular, if elements are stored as vectors, which multiplication is simpler to express?

Error distributions

Once again, consider $K = \mathbb{Q}(\sqrt[3]{2})$. Compare the PLWE error distribution, where coefficients of the polynomial in α are chosen at random according to a discrete Gaussian distribution, to the RLWE error distribution, which for simplicity you can assume chooses the coordinates of the elements, expressed in a basis for Λ, at random according to a discrete Gaussian distribution. Are the two distributions the same?

Dual lattices

One topic we unfortunately will not be able to get to is dual-RLWE, where the secret and/or errors belong to the dual lattice $\Lambda^\vee$ of Λ. To introduce this lattice we will need some setup: Define the **trace** of an element $\alpha \in K$ to be the sum

$$\mathrm{Tr}(\alpha) = \sum_{\sigma_i} \sigma_i(\alpha),$$

where the σ_i run through all embeddings (real and complex) of K into $\mathbb{C}$. Then the **dual ring** to R, the ring of integers of K is the ring of elements

$$R^\vee = \{\alpha \in K : \mathrm{Tr}(\alpha\beta) \in \mathbb{Z} \text{ for all } \beta \in R\}.$$

The dual lattice $\Lambda^\vee$ is then the canonical embedding of $R^\vee$.

1. Prove that $R \subset R^\vee$ for all fields K.
2. Consider $K = \mathbb{Q}(\sqrt[3]{2})$. Find an element that is in $R^\vee$ but not in R.