Computing traces in finite extensions of $\mathbb{Q}$.

We give an effective method for computing trace of any element of $K/\mathbb{Q}$, where K is a finite extension of $\mathbb{Q}$. As the characteristic of $\mathbb{Q}$ is 0, it is known that any such extension is primitive, i.e., $K = \mathbb{Q}[\alpha]$ for some $\alpha \in K$. Thus the properties of K are completely determined by the minimum polynomial f of α. We assume that only the minimum polynomial f is given, so $K = Q[x]/(f)$. To avoid confusion, we denote by α the equivalence class $[x]$ of x in K.

Let n be the degree of f. In order to be able to compute the trace of any element of K, it is enough being able to do this for the elements $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ as the trace map is linear. It is known that the trace of $a \in K$ is given by the sum $\sigma_1(a)+\sigma_2(a)+...+\sigma_n(a)$, where σ_i are all the embeddings of K into $\overline{\mathbb{Q}}$ in some order. Hence the trace of 1 is just n. On the other hand, for any $a \in K$, the expression $(x - \sigma_1(a))...(x - \sigma_n(a))$ defines a polynomial with coefficients in $\mathbb{Q}$. The coefficient preceding x^{n-1} is just $-(\sigma_1(a)+...+\sigma_n(a))$, which is just the negative of the trace of a! For α this polynomial is just its minimum polynomial f, so the trace of α can be determined just by looking at f.

Next we show how to compute the trace of α^i. Let ξ be a primitive root of unity of order i. Now $(x - a)(x - \xi a)(x - \xi^2 a)...(x - \xi^{i-1} a) = x^i - a^i$. Thus the polynomial $(x^i - \sigma_1(\alpha^i))...(x^i - \sigma_n(\alpha^i))$ is given by the product of polynomials $(x - \xi^j \sigma_1(\alpha))...(x - \xi^j \sigma_n(\alpha))$, where j runs over the numbers $0..i-1$. For a fixed j, the polynomial is of form

$$x^n - \xi^j a_{n-1} x^{n-1} + \xi^{2j} a_{n-2} x^{n-2} + ... + \xi^{nj} a_0,$$

where a_i are the coefficients of f. Now one can just simply take the product of these polynomials, and the trace of α^i is given by the coefficient preceding $x^{j(n-1)}$ times -1.