PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, Number 1, March 2020, pages TBD

# Kummer Theory for Number Fields

Antonella Perucca, Pietro Sgobba, Sebastiano Tronto

Let $K$ be a number field, and $G$ a finitely generated subgroup of $K^\times$ having positive rank $r$. We may suppose without loss of generality that $G$ is torsion-free. For any $M$ and $N$ with $N \mid M$ we want to compute the degree over $K(\zeta_M)$ of the Kummer extension $K\left(\zeta_M, \sqrt[N]{G}\right)$. This degree $\deg(M,N)$ divides $N^r$ and it is known that the quotient

$$C(M,N) := \frac{N^r}{\deg(M,N)}$$

divides a constant which is independent of $M$ and $N$ (a direct proof can be found in [2]). The ratio $C(M,N)$ can be seen as a failure of maximality for the Kummer extension: it is in fact the product over all prime divisors $\ell$ of $N$ of two numbers, namely the *$\ell$-adic failure*

$$C(\ell^n,\ell^n) = \frac{\ell^{nr}}{\left[K\left(\zeta_{\ell^n},\ \sqrt[\ell^n]{G}\right) : K\left(\zeta_{\ell^n}\right)\right]}$$

where $n = v_\ell(N)$, and the *adelic failure* (with respect to $\ell$)

$$\left[K\left(\zeta_{\ell^n},\ \sqrt[\ell^n]{G}\right) \cap K\left(\zeta_M\right) : K\left(\zeta_{\ell^n}\right)\right] .$$

The $\ell$-adic failure is explicitly computable [1]: the algorithm involves the choice of a suitable basis of $G$, where the generators show all the divisibility properties of $G$. For example, if $G = \langle 12, 18\rangle = \langle 6^3, 18\rangle$

over $\mathbb{Q}$, it is convenient to use the latter basis to compute the 3-adic failure. To control the adelic failure we make use of Schinzel's Theorem on abelian radical extensions. For example, the adelic failure for $G = \langle 5 \rangle$ is due to the fact that $\sqrt{5} \in \mathbb{Q}(\zeta_5)$.

For $K = \mathbb{Q}$, there are explicitly computable integers $M_0$ and $N_0$ such that

$$C(M, N) = C(\gcd(M, M_0), \gcd(N, N_0))$$

for all $M$ and $N$. In particular there are formulas (with a case distinction) describing $C(M, N)$ for all $M$ and $N$. Moreover, there is a concrete and efficient algorithm to compute these degrees for all $M$ and $N$. Such an algorithm has been implemented in Sagemath by Tronto.

## References


[1] C. Debry and A. Perucca: *Reductions of algebraic integers*, Journal of Number Theory, vol. 167 (2016), 259–283.

[2] A. Perucca and P. Sgobba: *Kummer Theory for Number Fields and the Reductions of Algebraic Numbers*, International Journal of Number Theory, doi:10.1142/S179304211950091X.



Antonella Perucca, Pietro Sgobba, Sebastiano Tronto
Mathematics Research Unit
University of Luxembourg
6, avenue de la Fonte
4364 Esch Luxembourg.
email: antonella.perucca@uni.lu, pietro.sgobba@uni.lu, sebastiano.tronto@uni.lu