REPORTS @SCM
AN ELECTRONIC JOURNAL OF THE SOCIETAT CATALANA DE MATEMÀTIQUES

Geometric methods in monogenic extensions

Francesc Pedret
Universitat Politècnica de Catalunya
francesc.pedret@upc.edu

Resum *(CAT)*
Un cos de nombres K és monogen si el seu anell d'enters està generat per un sol element com a $\mathbb{Z}$-àlgebra. En el cas cúbic, determinar si K és monogen o no és equivalent a resoldre l'equació diofàntica $|I_K(X,Y)| = 1$ sobre $\mathbb{Z}$, on I_K és la forma índex del cos. Una solució entera determina un punt racional a la corba de gènere 1 $I_K(X,Y) = Z^3$. Mitjançant aquesta construcció, es pot demostrar que K determina una $\mathbb{F}_3$-òrbita en $H^1(\mathbb{Q}, E[3])$, on E és la corba el·líptica definida per $Y^2 = 4X^3 + \mathrm{Disc}(K)$. Donem la construcció explícita d'aquesta òrbita pel cas de cossos cúbics purs i caracteritzem la suma de cocicles associats a cossos no isomorfs.

Keywords: *monogenity, diophantine equations, elliptic curves, Galois cohomology.*

Abstract

It is well known, due to the primitive element theorem, that any number field K is generated by a single algebraic number over $\mathbb{Q}$. One would think that the analogous statement should hold for the ring of integers $\mathcal{O}_K$, so that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some algebraic integer $\alpha \in \mathcal{O}_K$. However, Dedekind found the first counterexample for this assumption in 1878 (see [2]). When there exists such α, K is said to be *monogenic*. Today, for $n \geq 3$, it is expected that, when ordered by discriminant, the set of monogenic number fields of degree n has measure 0 (see [1]).

After choosing a suitable integral basis of $\mathcal{O}_K$, we can associate a degree $n(n-1)/2$ homogeneous form I_K on $n-1$ variables to K called the *index form* of K. This form allows to characterize the monogenity of K by a diophantine equation: K is monogenic if, and only if, there exist $x_1, \dots, x_{n-1} \in \mathbb{Z}$ such that $I_K(x_1, \dots, x_{n-1}) = \pm 1$. When $n = 3$, I_K is a binary cubic homogeneous form and its discriminant is equal to the discriminant of K (see [3]). Thus, the projective curve $C_K : I_K(X,Y) = Z^3$ is smooth and an integral solution to the index form equation gives rise to a rational point on C_K. Therefore, we focus on studying the existence of rational points on C_K.

For non-zero $r \in \mathbb{Q}$, let E^r denote the elliptic curve given by $Y^2 = 4X^3 + r$. Let $D = \mathrm{Disc}(K)$. In recent work of Alpöge, Bhargava, and Shnidman (see [1]), they defined a rational map $\pi_K \colon C_K \to E^{-27D}$ and a 3-isogeny $\phi_D \colon E^D \to E^{-27D}$ such that (C_K, π_K) is a ϕ_D-covering of E^{-27D}. As a consequence, C_K is a homogeneous space for E^D. The ϕ_D-coverings of E^{-27D} are parametrized by $H^1(\mathbb{Q}, E^D[\phi_D])$,

where $E^D[\phi_D] = \ker(\phi_D)$, and homogeneous spaces for E^D are parametrized by the Weil–Châtelet group $H^1(\mathbb{Q}, E^D)$, whose trivial class consists of the homogeneous spaces for E^D which have a rational point. These cohomology groups are related by the Kummer exact sequence

$$E^{-27D}(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, E^D[\phi_D]) \xrightarrow{\iota} H^1(\mathbb{Q}, E^D),$$

where ι is given, in terms of ϕ_D-coverings and homogeneous spaces, by $\iota(C_K, \pi_K) = C_K$. Thus, (C_K, π_K) is in the kernel of ι if, and only if, C_K has a rational point. Therefore, by analysing this kernel, we can study the monogenity of families of number fields with discriminant D. We apply this theory in order to give bounds for the total number of monogenic cubic number fields with the same discriminant in terms of E^D.

Since (C_K, π_K) is a ϕ_D-covering, it determines a class $\alpha_K \in H^1(\mathbb{Q}, E^D[\phi_D])$. When K is a Dedekind type I field, i.e. when $K = \mathbb{Q}(\sqrt[3]{hk^2})$, where h, k are coprime, square-free integers such that $hk^2 \not\equiv \pm 1$ modulo 9, we prove that the cocycle

$$\xi_K : \sigma \longmapsto \log_\omega \left(\frac{\sigma(\sqrt[3]{hk^2})}{\sqrt[3]{hk^2}} \right) (0 : \sqrt{D} : 1)$$

is a representative of α_K, where ω is a third root of unity. Using this expression, given Dedekind type I fields K_1 and K_2 with the same discriminant, we find an expression for the ϕ_D-covering associated to $\xi_{K_1} + \xi_{K_2}$, determining also when this covering corresponds to a Dedekind type I field.

Acknowledgements

The author would like to thank Jordi Guàrdia for his guidance during this project. The author also gratefully acknowledges the Universitat Politècnica de Catalunya and Banco Santander for the financial support of his predoctoral FPI-UPC grant.

References

[1] L. Alpöge, M. Bhargava, A. Shnidman, A positive proportion of cubic fields are not monogenic yet have no local obstruction to being so, Preprint (2020). arXiv:2011.01186.

[2] R. Dedekind, Ueber den Zusammenhang zwischen der Theorie der ideale und der Theorie der höheren Congruenzen, *Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen* **23** (1878).

[3] W. T. Gan, B. Gross, G. Savin, Fourier coefficients of modular forms on G_2, *Duke Math. J.* **115(1)** (2002), 105–169.