ESTRUCTURA DE GALOIS
DE GRUPOS DE MORDELL-WEIL

DANIEL MACIAS CASTILLO

Sea E una curva elíptica definida sobre $\mathbb{Q}$, y sea F una extensión finita y Galois de $\mathbb{Q}$ con grupo de Galois G. El conjunto de puntos F-racionales $E(F)$ de E, denominado grupo de Mordell-Weil de E sobre F, tiene de manera natural una estructura de grupo abeliano (finitamente generado, por el teorema de Mordell-Weil), y además una acción compatible de G, es decir, una estructura de módulo (finitamente generado) sobre el anillo $\mathbb{Z}[G]$, o de módulo de Galois para la extensión $F/\mathbb{Q}$.

Obtener información sobre la estructura del módulo $E(F)$, o de su compleción p-ádica para un número primo p, es un problema algebraico muy interesante que tiene en particular consecuencias directas sobre el comportamiento de los rangos de los grupos de Mordell-Weil de E sobre los cuerpos intermedios de $F/\mathbb{Q}$, y por tanto sobre el estudio de la conjetura de Birch y Swinnerton-Dyer, uno de los 'problemas del milenio'.

El objetivo de este trabajo será adquirir los conocimientos generales de álgebra homológica y cohomología de grupos, así como de la teoría básica de curvas elípticas, necesarios para poder entender y formular problemas concretos dentro de este ámbito. Si el estudiante llega a estar suficientemente familiarizado con ellos, podrá intentar adaptar (una simplificicación de) el resultado [2, Teorema 2.7], y utilizarlo para obtener descripciones explícitas de estas estructuras de Galois en ejemplos concretos.

References

[1] M. F. Atiyah, C. T. C. Wall, Cohomology of Groups In: 'Algebraic Number Theory' (Ed. J. W. S. Cassels and A. Fröhlich), Academic Press, London, (1967) 94-115.

[2] D. Burns, D. Macias Castillo, C. Wuthrich, On the Galois structure of Selmer groups, Int. Math. Res. Notices **2015** (2015) 11909-11933.

[3] P. J. Hilton, U. Stammbach, A course in Homological Algebra, Springer-Verlag, New York, 1970.

[4] J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.