

Problema 9

EJERCICIO 0.14: Elabora un programa, en el lenguaje de programación que desees, que calcule el grupo de Galois de un polinomio de grado 5 sobre el cuerpo de los números racionales. El polinomio dado no tiene por qué ser irreducible.

Solución:

Describimos a continuación los aspectos más relevantes de la implementación de este problema en Sage.

Nosotros hemos programado la clasificación de los grupos de Galois de los polinomios desde grado 2 hasta grado 5.

El caso 2 y 3 no tienen dificultad.

Para el caso 4 sugerimos utilizar la función `discriminant()` de la que nos provee Sage ya que o bien la fórmula de los apuntes es errónea o bien la traslación de la fórmula que nosotros hicimos era errónea pero daban resultados distintos. Una condición útil para comprobar que la fórmula es correcta es que vale cero si y sólo si dos coeficientes valen cero.

Otro aspecto interesante es la comprobación de la hipótesis c de la proposición 17.2 de los apuntes. Este apartado comprueba que el grupo de Galois es C_4 comprobando la pertenencia de dos raíces a un cuerpo extensión por la raíz del discriminante. A la hora de llevar esto a la práctica nos ha resultado útil la observación de Keith Konrad en sus notas *Galois groups of cubics and quartics (not it characteristic 2)* que reduce esta comprobación a comprobar que las raíces multiplicadas por el discriminante del polinomio son cuadrados de números racionales.

Para estudiar la factorización de polinomios en cuerpos extensión debemos agradecer a la comunidad de `ask.sagemath.org` sus ideas si bien para obtener una solución en especial recomendamos las siguientes cuestiones:

- Factorization of $f \in \mathbb{Q}[X]$ in field extension $\mathbb{Q}(\alpha)$.
- Extension field adjoining two roots.

Como observación final notaremos que hemos utilizado en el código que \mathbb{Q} es un cuerpo perfecto y por tanto todo irreducible es separable, esto es, tiene raíces distintas. Esto por ejemplo en el caso de la clasificación de C_5 .

El programa completo se encuentra en el archivo *galois.ipynb*. También contiene algunos ejemplos para comprobar la implementación. En particular, tenemos infinitos ejemplos de cíclicas dadas por la expresión de la quintica de Emma Lehmer. A este respecto recomendamos en `ask.sagemath.org` la pregunta *Any more cyclic quintics*. En concreto, notaremos que la segunda fórmula no puede ser utilizada para parámetros arbitrarios.