Non-monogenic Division Fields of Ordinary Elliptic Curves

Hanson Smith

University of Colorado, Boulder

Background

A number field K over $\mathbb{Q}$ is *monogenic* if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$.

Background

A number field K over $\mathbb{Q}$ is *monogenic* if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$.

We also say that $\mathcal{O}_K$ admits a *power integral basis*.

Background

A number field K over $\mathbb{Q}$ is *monogenic* if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$.

We also say that $\mathcal{O}_K$ admits a *power integral basis*.

The problem of finding which number fields are monogenic is often called **Hasse's Problem**.

Background

A number field K over $\mathbb{Q}$ is *monogenic* if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$.

We also say that $\mathcal{O}_K$ admits a *power integral basis*.

The problem of finding which number fields are monogenic is often called **Hasse's Problem**.

Some prominent examples of monogenic fields are the cyclotomic fields $\mathbb{Q}(\zeta_n)$.

Background

A number field K over $\mathbb{Q}$ is *monogenic* if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$.

We also say that $\mathcal{O}_K$ admits a *power integral basis*.

The problem of finding which number fields are monogenic is often called **Hasse's Problem**.

Some prominent examples of monogenic fields are the cyclotomic fields $\mathbb{Q}(\zeta_n)$.

In other words, the $\mathbb{G}_m$ division fields are monogenic.

Background

A number field K over $\mathbb{Q}$ is *monogenic* if $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in K$.

We also say that $\mathcal{O}_K$ admits a *power integral basis*.

The problem of finding which number fields are monogenic is often called **Hasse's Problem**.

Some prominent examples of monogenic fields are the cyclotomic fields $\mathbb{Q}(\zeta_n)$.

In other words, the $\mathbb{G}_m$ division fields are monogenic.

What about division fields of other groups?

Results

Results

There are plenty of division fields of elliptic curves that aren't monogenic over $\mathbb{Q}$.

Results

There are plenty of division fields of elliptic curves that aren't monogenic over $\mathbb{Q}$.

Sample Theorem: (S.) Let E be an elliptic curve over $\mathbb{Q}$ with trace of Frobenius ± 2 modulo 2. Suppose

$n \in \{5, 13, 15, 17, 41, 51, 65, 85, 91, 105, 117, 145, 195, 205, 255, 257, 315, 455\}$

and that the representation $\rho_{E,n} : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is surjective. Then $\mathbb{Q}(E[n])$ is **not** monogenic over $\mathbb{Q}$.

Results for $p = 2$

a_2	σ_2	non-monogenic n
1	$\begin{bmatrix} 4 & -14 \\ 1 & -3 \end{bmatrix}$	11
-1	$\begin{bmatrix} 3 & -14 \\ 1 & -4 \end{bmatrix}$	11, 23
2	$\begin{bmatrix} 3 & -5 \\ 1 & -1 \end{bmatrix}$	5, 13, 15, 17, 41, 51, 65, 85, 91, 105, 117, 145, 195, 205, 255, 257, 273, 315, 455, 565, 585, 771, 819
-2	$\begin{bmatrix} 1 & -5 \\ 1 & -3 \end{bmatrix}$	5, 13, 15, 17, 41, 51, 65, 85, 91, 105, 117, 145, 195, 205, 255, 257, 273, 315, 455, 565, 585, 771, 819

Table 1: Using the splitting of 2 in $\mathbb{Q}(E[n])$ to show non-monogeneity for $n < 1000$

Results for $p = 3$

a_3	σ_3	non-monogenic n
1	$\begin{bmatrix} 6 & -33 \\ 1 & -5 \end{bmatrix}$	5, 40
-1	$\begin{bmatrix} 5 & -33 \\ 1 & -6 \end{bmatrix}$	5, 23, 40
2	$\begin{bmatrix} 5 & -18 \\ 1 & -3 \end{bmatrix}$	4, 11, 22, 136, 272
-2	$\begin{bmatrix} 3 & -18 \\ 1 & -5 \end{bmatrix}$	4, 22, 136, 272
3	$\begin{bmatrix} 3 & -3 \\ 1 & 0 \end{bmatrix}$	7, 14, 28, 52, 56, 91, 104, 182, 259, 266, 364, 518, 532, 703, 728, 949
-3	$\begin{bmatrix} 0 & -3 \\ 1 & -3 \end{bmatrix}$	7, 14, 28, 52, 56, 91, 104, 182, 259, 266, 364, 518, 532, 703, 728, 949

Table 2: Using the splitting of 3 in $\mathbb{Q}(E[n])$ to show non-monogeneity for $n < 1000$

Thank You

Thank you for listening. Please send me an email at hanson.smith@colorado.edu if you have any questions that aren't answered here.