CTNT 2020

Computations in Number Theory Research

ONLINE!

Def. A number field is a finite degree field extension of $\mathbb{Q}$.

ex $\mathbb{Q}(i) = \{a+bi : a,b \in \mathbb{Q}\}$ is an extension of degree 2

as a vector space over $\mathbb{Q}$, $\mathbb{Q}(i)$ is a 2-dimensional vector space

ex $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a,b,c \in \mathbb{Q}\}$

is an extension of degree 3 over $\mathbb{Q}$.

ex i is a root of an irreducible polynomial, namely x^2+1.
$-i$ is the second root of x^2+1.
Since i and $-i$ are both in $\mathbb{Q}(i)$, the extension $\mathbb{Q}(i)/\mathbb{Q}$ is Galois

ex $\sqrt[3]{2}$ is a root of x^3-2. The other roots are $\rho\sqrt[3]{2}$ and $\rho^2\sqrt[3]{2}$, where $\rho^3 = 1$ is a 3rd root of unity. Since $\rho\sqrt[3]{2}$ is not in $\mathbb{Q}(\sqrt[3]{2})$, the ext'n $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is NOT Galois.

CTNT 2020

Computations in Number Theory Research

ONLINE!

Def An elliptic curve is a smooth projective curve of genus 1 with a point O over K.

over a field K

↳ Every elliptic curve is given by a Weierstrass equation:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

with coefficients $a_i \in K$.

↳ The Mordell-Weil theorem says $E(K) = \{$ points on E w/ coefficients in $K\}$ form a finitely generated abelian gp, when K is a number field.

$$\rightarrow E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^{R_{E/K}}$$

Theorem (Mazur) Let E be an elliptic curve over $\mathbb{Q}$. Then:

$$E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & N = 1, \dots, 10, \text{ or } 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & M = 1, 2, 3, 4 \end{cases}$$