Cyclic Field Extensions and Groups on Conics

Rose-Hulman Undergraduate Mathematics Conference

Connor Lane

August 2, 2024

Outline

- Introduction to field and Galois theory
- The group structure on a conic
- The main result

Fields and Field Exensions

"Definition" (field)

A **field** *is a set K where you can reasonably talk about the operations $(+, -, \times, \div)$ and they have the properties you would expect.*

- Some examples include $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$

Definition (Field Extensions)

A field extension L/K is a pair of fields L, K such that $K \subseteq L$.

- Examples: $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$
- For any field K, we can define $K(\alpha) = (a_0 + a_1\alpha + \ldots + a_n\alpha^n : a_i \in K)$.

Automorphisms and Galois Groups

Definition (Automorphism Group)

Let L be a field, then $\mathrm{Aut}(L)$ is the set

$$\{\sigma : L \to L | \sigma(\alpha+\beta) = \sigma(\alpha)+\sigma(\beta), \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta), \sigma(1) \neq 0\}$$

Definition (Galois Group)

For an extension of fields L/K, define

$$\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) : \sigma(k) = k \quad \forall k \in K\}$$

- Example: $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, c\}$ where $\mathrm{id}(a+bi) = a+bi$ and $c(a+bi) = a-bi$.
- Important fact: if $\sigma, \tau \in \mathrm{Gal}(L/K)$, then $\sigma \circ \tau \in \mathrm{Gal}(L/K)$.

Cyclic Extensions

Definition (Degree of an Extension)

The degree of an extension L/K is the dimension of L as a vector space over K, and is written $[L : K]$.

- Intuitively, you should think of the degree as the relative size of L compared to K.
- Example: $[\mathbb{C} : \mathbb{R}] = 2$

Definition (Cyclic Extension)

Let L/K be an extension of fields. L/K is called cyclic if there is some $\sigma \in \mathrm{Gal}(L/K)$ such that $\{\sigma^k\} = \mathrm{Gal}(L/K)$, and $|\mathrm{Gal}(L/K)| = [L : K]$.

- Such a σ is called a generator.
- Example: $\mathbb{C}/\mathbb{R}$ is cyclic. $\sigma = c$ satisfies the definition.

A More Complicated Example

- Define $K = \mathbb{Q}(i)$, and $L = K(\sqrt[4]{2})$.
- We have $\mathrm{Gal}(L/K) = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$.

$$\begin{aligned}
\mathrm{id}(a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8}) &= a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8} \\
\sigma_1(a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8}) &= a_0 + ia_1\sqrt[4]{2} - a_2\sqrt[4]{4} - ia_3\sqrt[4]{8} \\
\sigma_2(a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8}) &= a_0 - a_1\sqrt[4]{2} + a_2\sqrt[4]{4} - a_3\sqrt[4]{8} \\
\sigma_3(a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8}) &= a_0 - ia_1\sqrt[4]{2} - a_2\sqrt[4]{4} + ia_3\sqrt[4]{8}
\end{aligned}$$

- σ_1 works as a generator: $\sigma_1^1 = \sigma_1$ $\sigma_1^2 = \sigma_2$, $\sigma_1^3 = \sigma_3$, $\sigma_1^4 = \mathrm{id}$.
- L/K is cyclic of degree 4.

Kummer Theory

- My work is primarily inspired by Kummer theory

Definition (Contains all nth roots of unity)

Let K be a field. K is said to contain all nth roots of unity if it contains n solutions to the polynomial $x^n - 1$.

Theorem (Kummer, 1840s)

Let K be a field that contains all nth roots of unity. Then all degree n cyclic extensions of K are given by

$$K(\sqrt[n]{\alpha})/K$$

where $\alpha \in K$.

Points on a Curve

- An algebraic curve is two-variable polynomial equation of the form $C : p(x, y) = 0$
- Example: $C : x^2 - y = 0$, is an algebraic curve.

Definition (K points)

For a field K and algebraic curve $C : p(x, y) = 0$, we write

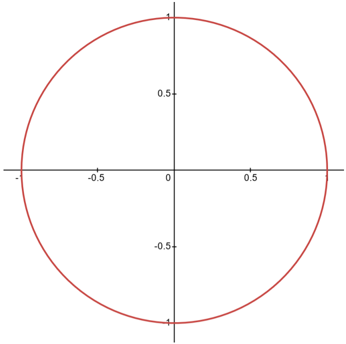
$$C(K) := \{(x_0, y_0) \in K^2 : p(x_0, y_0) = 0\}$$

The set $C(K)$ is called the K points of C.

- We will primarily be interested in the curve $C : \alpha x^2 + \beta y^2 - 1 = 0$

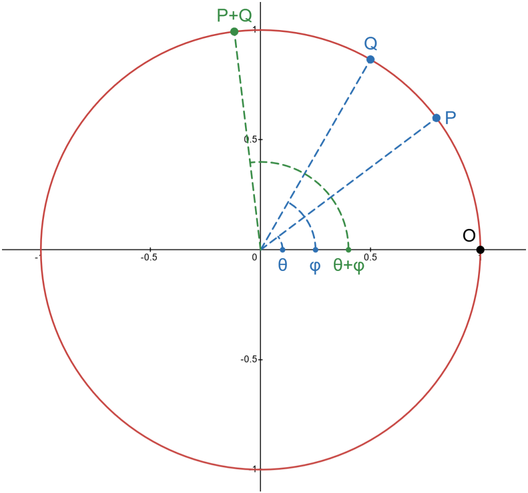
Example: The Circle

- When $K = \mathbb{R}$, we can visualize that K points of C via its graph.
- Example: $C : x^2 + y^2 - 1 = 0$ has the following $\mathbb{R}$ points.



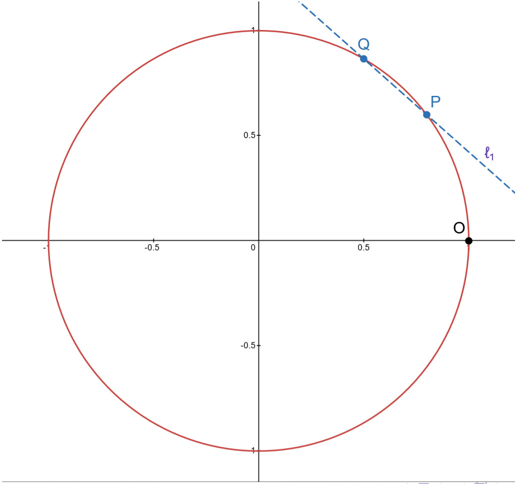
Adding points on a Circle

- There is a notion of "adding" points on a circle.

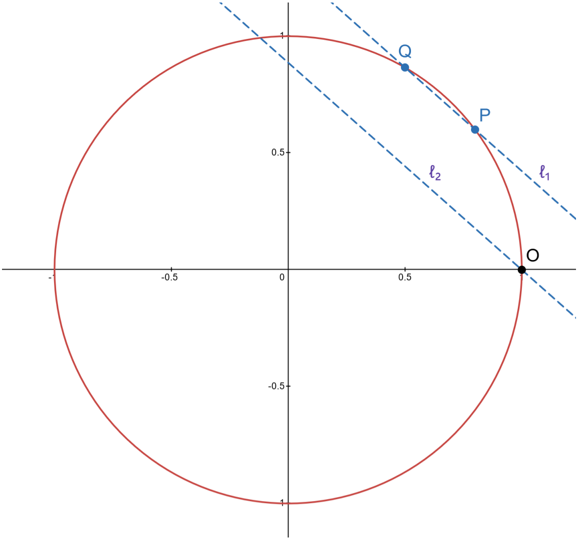


Adding Points on a Circle: Another Way (1)

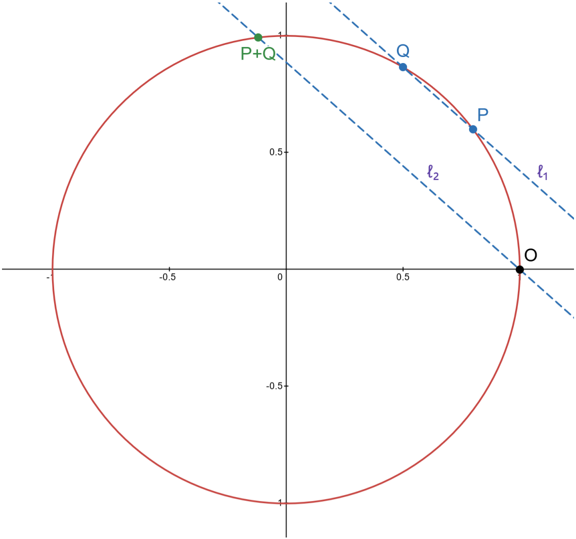
- The notion of "angle" is too specific to $\mathbb{R}$, so we want to find an alternative method of adding points



Adding Points on a Circle: Another Way (2)



Adding Points on a Circle: Another Way (3)

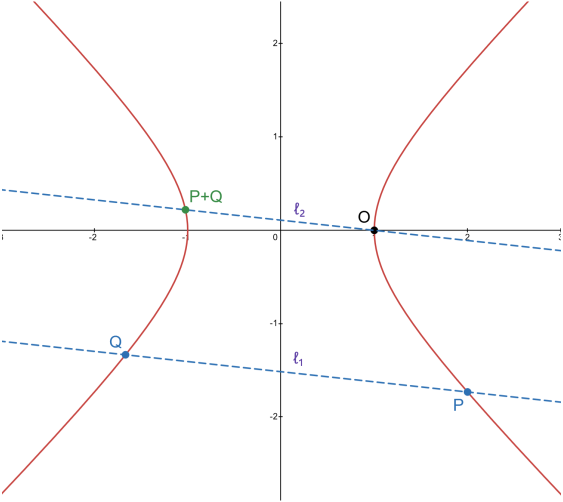


Why use lines?

- The advantage of lines is that they are more general.
- "The line between two points" is completely algebraic: it's the unique algebraic curve $\ell : ax + by + c = 0$ such that $P, Q \in \ell(K)$.
- "Parallel lines" is just that $\ell : ax + by + c = 0$ and $\ell' : a'x + b'y + c' = 0$ obey $\frac{a}{b} = \frac{a'}{b'}$
- "The other intersection" is guarenteed to be well-defined by **Bézout's Theorem** from Algebraic Geometry
- Most remarkably: This generalizes to arbitrary curves $C : \alpha x^2 + \beta y^2 - 1 = 0$

Adding points on a hyperbola

If we are on $C : x^2 - y^2 - 1 = 0$, the same process allows us to add points.



Some notation

- Let K be a field and $C : \alpha x^2 + \beta y^2 - 1 = 0$ be a conic with distinguished point O.

Definition

For $P \in C(K)$ and $n \in \mathbb{N}$, define

$$nP := \underbrace{P + \cdots + P}_{n \text{ times}}$$

- We will need the following technical condition.

Definition (n-torsion of $C(K)$)

$$C(K)[n] := \{P \in C(K) : nP = O\}$$

We say $C(K)$ *has all n-torsion* if $|C(K)[n]| = n$.

The Main Theorem

- Let:
  - K be a field with $\mathrm{char}(K) \neq 2$
  - $n \in \mathbb{N}$ an *odd* integer with $\mathrm{char}(K) \nmid n$
  - $C : \alpha x^2 + \beta y^2 - 1 = 0$ a curve with distinguished point $O \in C(K)$
  - $C(K)$ has all n torsion

Theorem (Lane, 2023)

All cyclic degree n extensions of K are of the form

$$K(x, y)/K$$

Where $Q = (x, y) \in C$ obeys $nQ = P \in C(K)$.

Comparison with Kummer Theory

- There are many parallels between this theorem and Kummer theory, and we list them here.

	Kummer Theory	Conics
Group	$(K \setminus \{0\}, \times)$	$(C(K), +)$
Must contain	all roots of unity	all n-torsion
"Division"	$\sqrt[n]{\alpha}$	Q where $nQ = P$
Adjoins	$\sqrt[n]{\alpha}$	coordinates of Q
Classifies	cyclic extensions	odd deg. cyclic extensions

- Moreover, their proofs use similar methods.

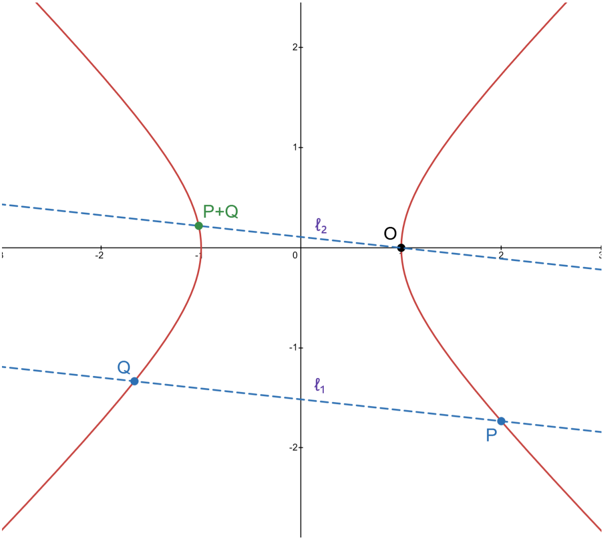
Acknowledgements and Sources

- This project was done as part of a class on Galois cohomology run by Dr. All
- I'd like to thank Dr. All and Shyam Ravishankar for their feedback on this project
- Aden Shaw, Alexa Renner, Ben Lyons, Shyam Ravishankar, and Nathan Chen gave feedback on these slides.

- I used various lecture notes from courses I have taken, along with

Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg.
Cohomology of Number Fields.
Springer-Verlag, 2013.

Questions?



Brief discussion of proof methods

- The main technical tool of this proof is Galois cohomology.
- Let $\bar{K}$ be the separable closure of K. We have this exact sequence:

$$0 \longrightarrow C(\bar{K})[n] \longrightarrow C(\bar{K}) \xrightarrow{[n]} C(\bar{K}) \longrightarrow 0$$

- Taking $\mathrm{Gal}(\bar{K}/K)$-cohomology, we obtain via the long exact sequence

$$C(K) \xrightarrow{[n]} C(K) \xrightarrow{\delta} H^1(\bar{K}/K, C(\bar{K})[n]) \longrightarrow H^1(\bar{K}/K, C(\bar{K}))$$

- This yields an injection

$$\delta : C(K)/nC(K) \to H^1(\bar{K}/K, C(\bar{K})[n]) \simeq \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\bar{K}/K), C(K)[n])$$

- Analyzing $H^1(\bar{K}/K, C(\bar{K}))$, we can show this is an isomorphism when n is odd