Constructible Numbers, Division Points and Class Field Theory

Tyler Genao

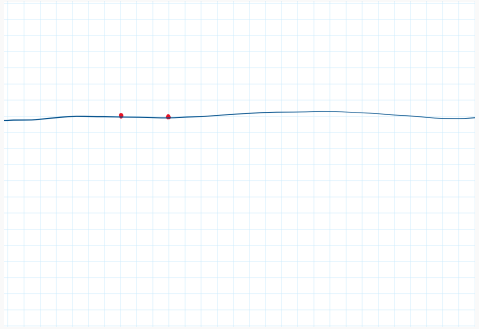
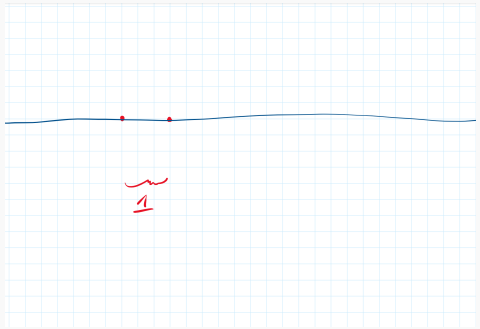
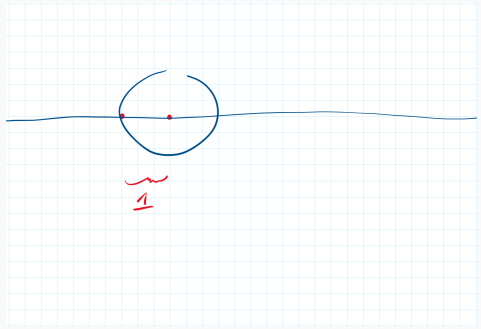
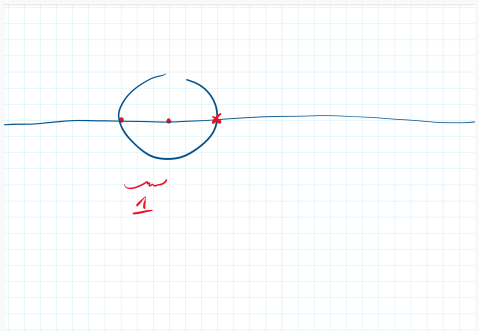
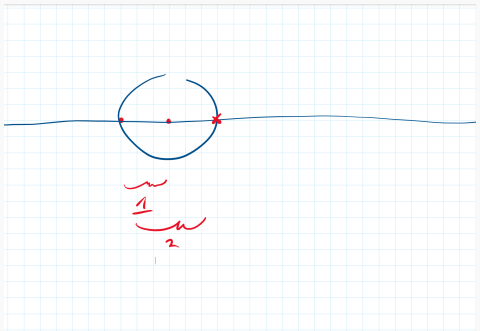
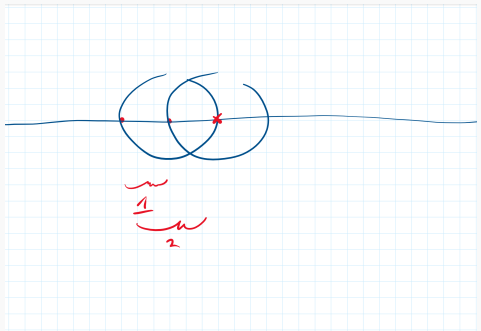
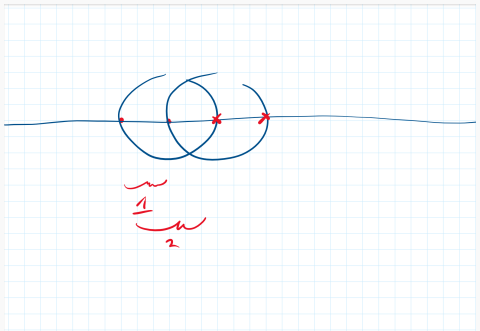
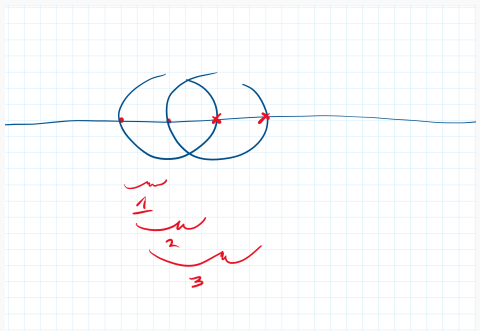
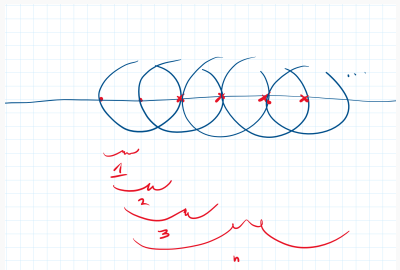
April 14, 2020

- Broadly speaking, **class field theory** is the study of abelian extensions of number fields, function fields and local fields, such as $\mathbb{Q}(i)$, $\mathbb{F}_p(t)$, $\mathbb{Q}_p$ and so on.
- We will focus our study on *number fields*, e.g. finite extensions K of $\mathbb{Q}$.
- We will see that abelian Galois extensions of K can be described by their arithmetic: namely, the behavior of prime ideals of their number rings.
- Explicit class field theory (describing all abelian extensions explicitly) is usually very hard, but we will see some of this for $\mathbb{Q}$ and imaginary quadratic fields.

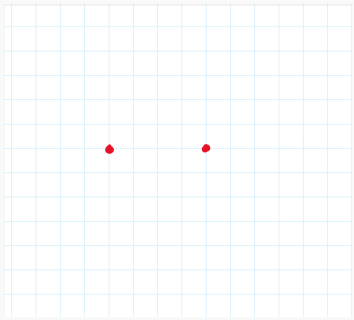
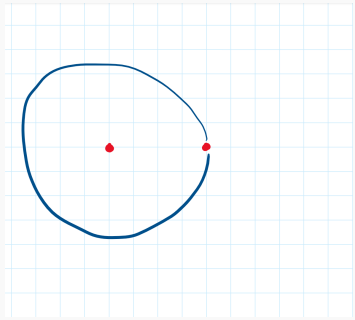
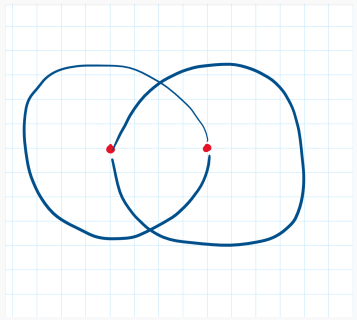
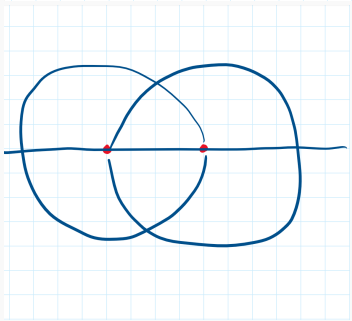
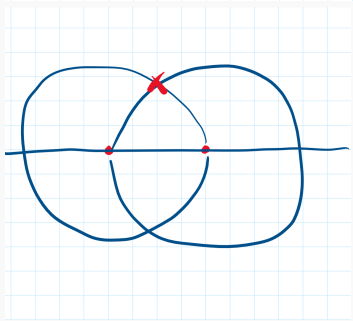
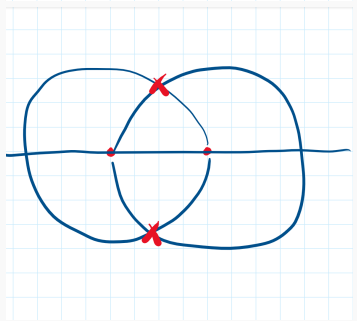
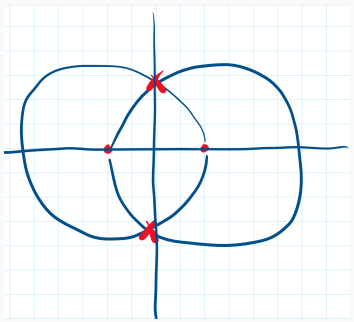
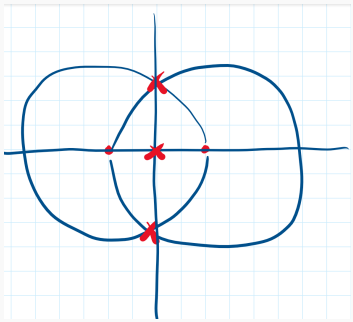
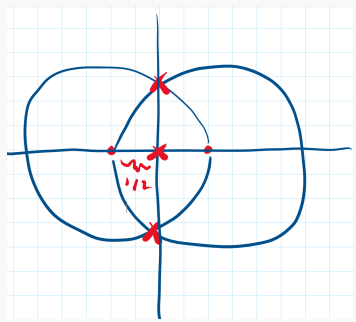
- During antiquity, geometry saw important development from many Ancient Greece mathematicians, like Pythagoras and Euclid.
- Their interests in geometry included **straightedge and compass constructions:** what geometric objects (lengths, angles, polygons) can be constructed using only an idealized straight line, and a compass?

- How to play this game:
- Start with the points $(0,0)$ and $(1,0)$ in $\mathbb{R}^2$. In straightedge and compass constructions, one can only use the following basic constructions on pre-existing points, lines and circles:
  1. Create an infinite line through two distinct points; **(straightedge)**
  2. For two distinct points, draw a circle centered at one which contains the other; **(compass)**
  3. determine the points of intersection between two distinct lines, a line and a circle, or two distinct circles. **(determination)**
- Given these rules, what types of points can we determine in a finite amount of steps?
- Call such points **constructible**, and the polygons made from such points **constructible polygons.**
- Call a number $a \in \mathbb{R}$ a **constructible number** if there is a constructible point with x or y-coordinate equal to a.

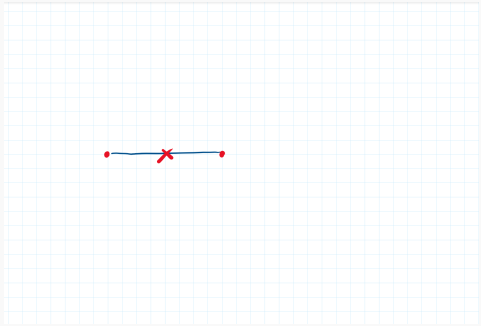
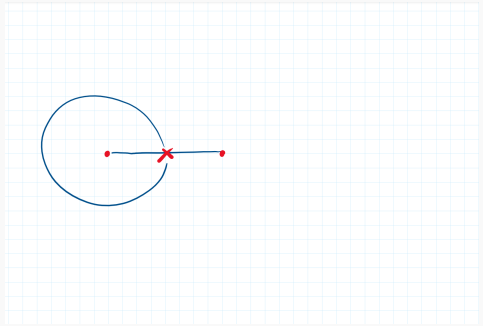
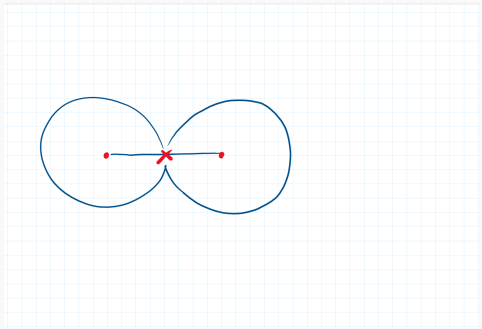
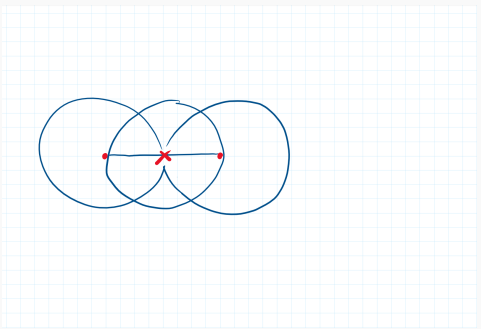
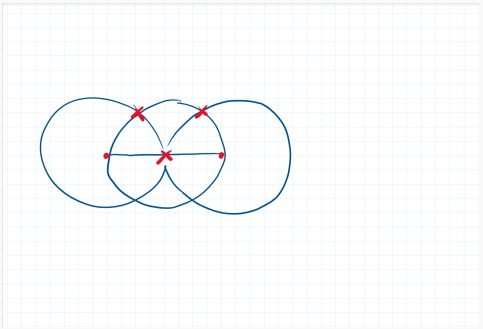
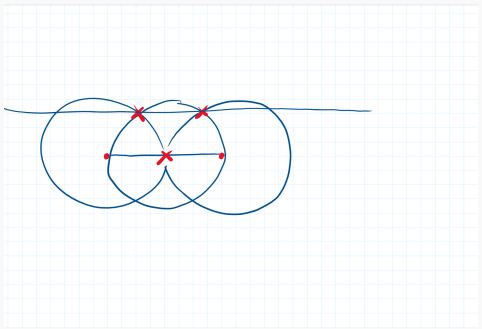
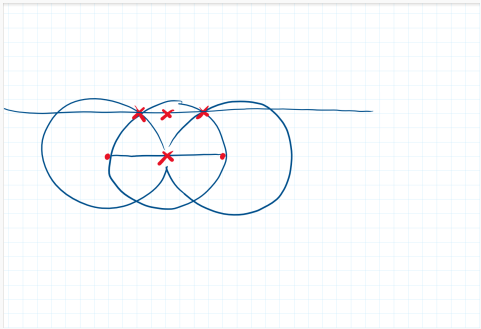
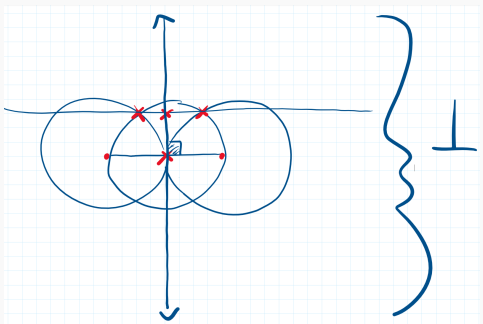
Constructibility of $\mathbb{N}$:

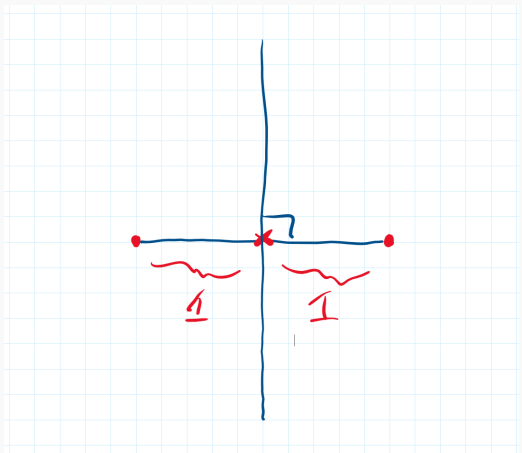
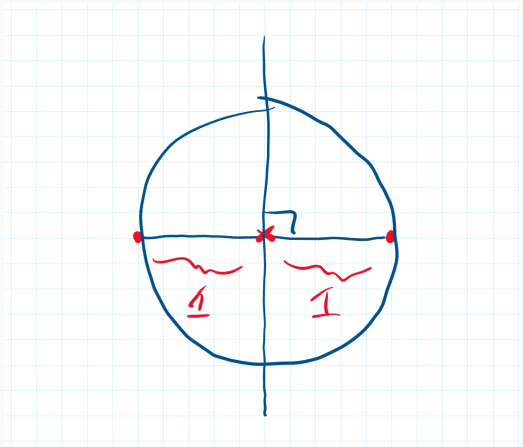
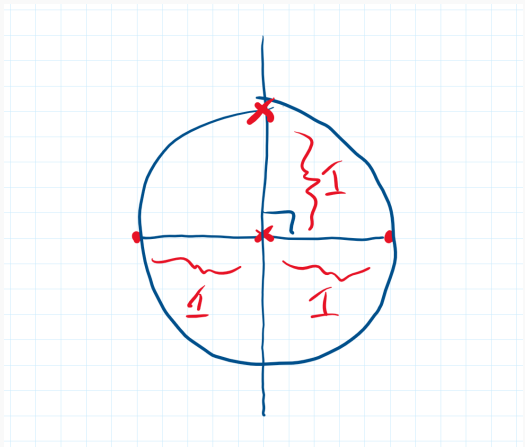
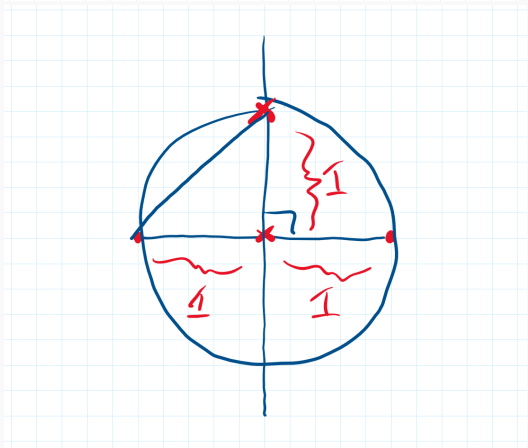
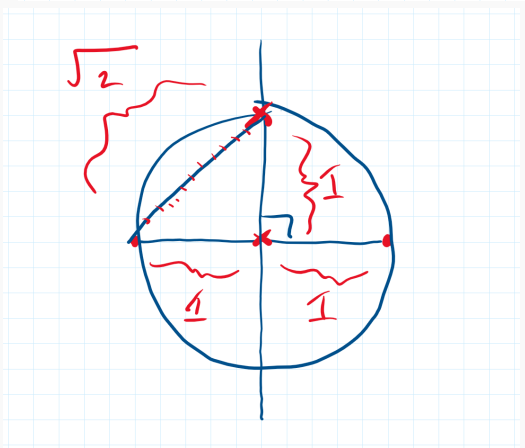
Constructibility of $\frac{1}{2}$ (bisecting lines is constructible):

Perpendicular lines to a constructible point are constructible:

Constructibility of $\sqrt{2}$:

- Let us extend constructibility to $\mathbb{C}$: call $x + iy \in \mathbb{C}$ a **constructible number** if $(x, y) \in \mathbb{R}^2$ is a constructible point.
- The set $F \subseteq \mathbb{C}$ of constructible numbers is a field; so if a, b are constructible then so are $a \pm b$, ab, a/b.
- F is also closed under taking square roots.

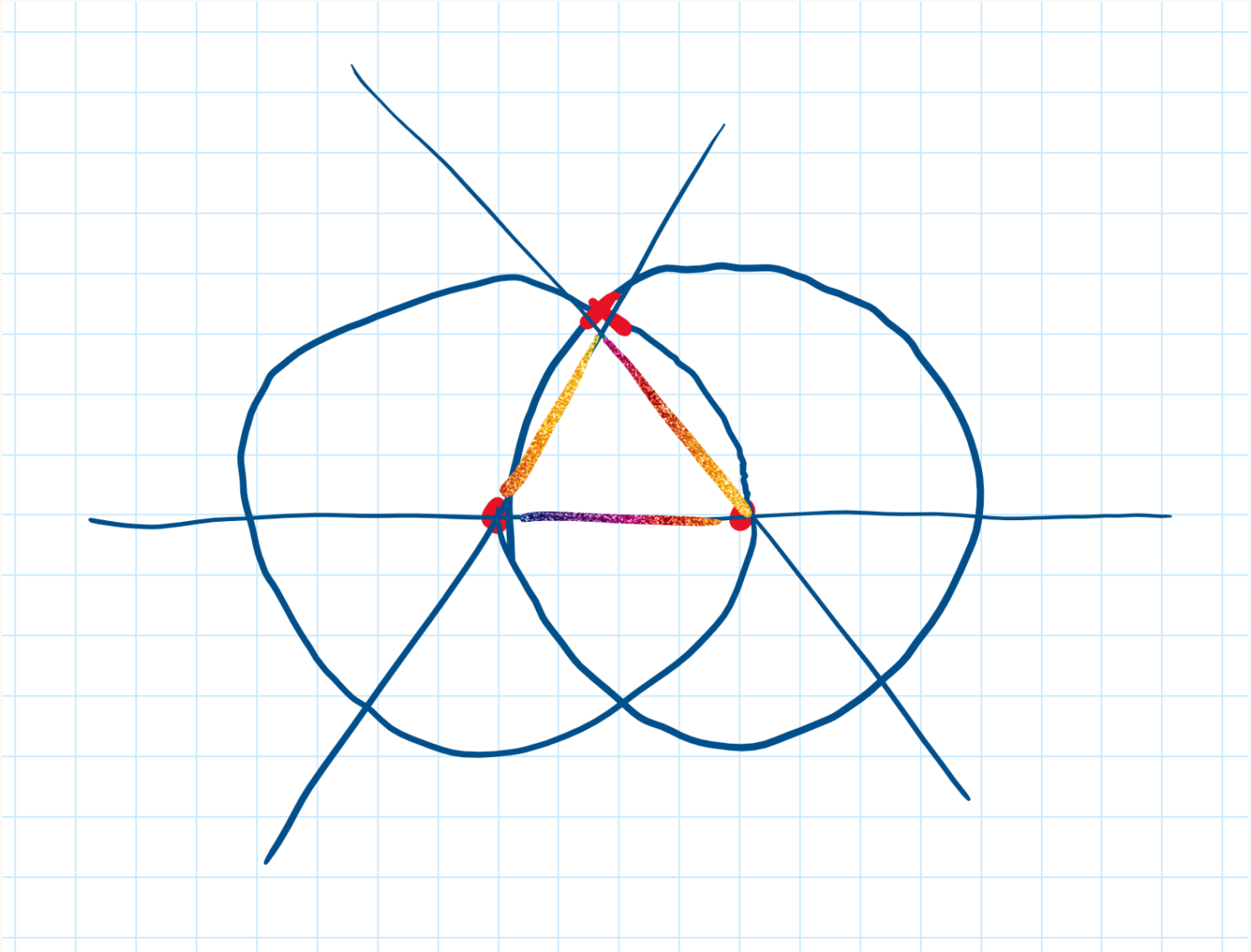
- More than a millennium after Greek antiquity, Gauss publishes the *Disquisitiones Arithmeticae* (or *Higher Arithmetic*), notable for making rigorous the field of number theory. (It also started the format *Theorem-Proof-Corollary* for textbooks.)
- Although concerning itself in large part with modular arithmetic, the last section focuses on "equations defining a circle."
- It was in this section that Gauss was able to show the following:

- Recall that *Fermat primes* are primes of the form $F_r := 2^{2^r} + 1$ where $r \geq 0$.
  - The first few Fermat primes are $3, 5, 17, 257, 65537, \ldots$.

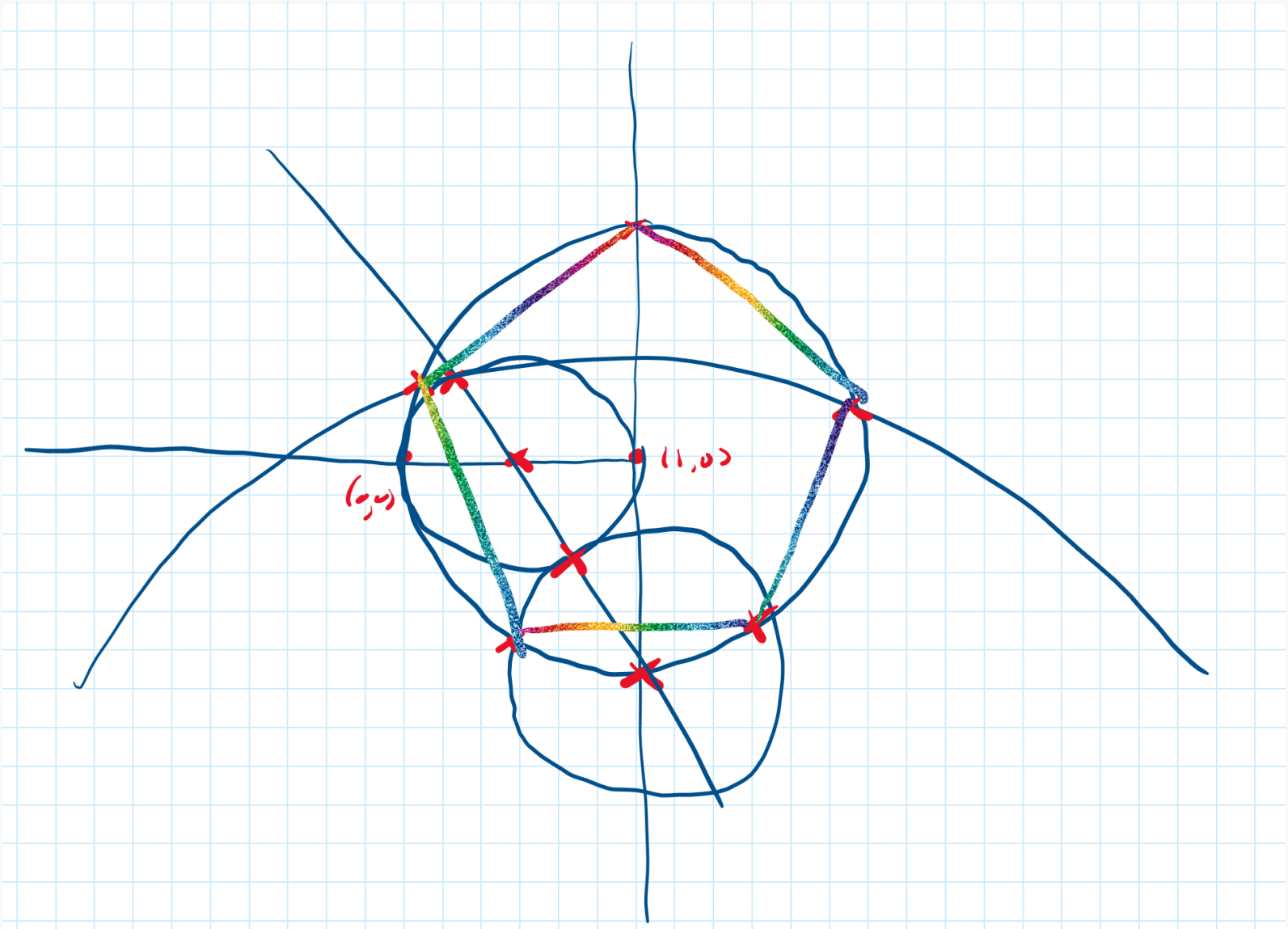
Theorem 1 (Gauss).

A regular n-gon can be constructed by straightedge and compass if n is a product of a power of two with a squarefree product of Fermat primes.

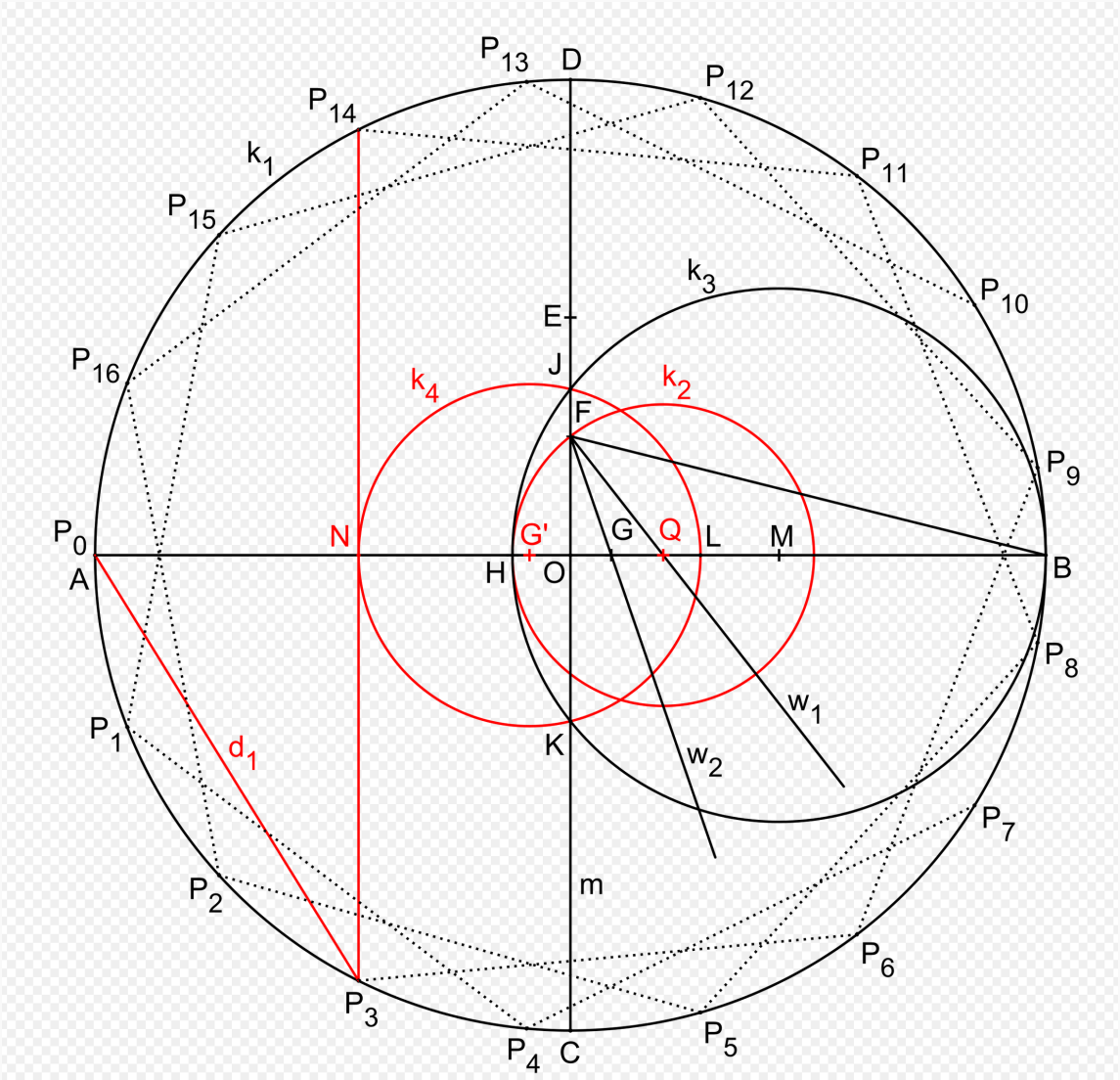
Constructibility of a regular 3-gon:



Constructibility of a regular 5-gon (interior to a circle):



Constructibility of a regular 17-gon (cf. Wikipedia):



- Recall that the n'th roots of unity are the complex numbers $\zeta \in \mathbb{C}$ which satisfy $\zeta^n = 1$.
- Gauss' construction of the regular n-gon involves dividing the unit circle into n arcs of equal length, the "division points" being the n'th roots of unity

$$e^{2\pi ik/n} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right)$$
$$\rightsquigarrow \left(\cos\left(\frac{2\pi k}{n}\right), \sin\left(\frac{2\pi k}{n}\right)\right) \in \mathbb{R}^2, \ k = 0, 1, \ldots, n-1.$$

  (This tells us that the n'th roots of unity for such n are constructible numbers.)
- The proof also illustrates that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is an *abelian extension*, namely $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ has abelian Galois group.

- At the beginning of Section 7 in *Disquisitiones*, Gauss explains that his methods of proof apply not only to circular functions, but also to other **transcendental functions** – functions, like sin and exp, that don't satisfy polynomial equations.
  - For example, he references transcendental functions which depend on the integral $\int \frac{dx}{\sqrt{1-x^4}}$. Such functions are called *elliptic functions.*
- Inspired by Gauss' work and claim, Abel proved an analogous result for dividing the arclength of a lemniscate.

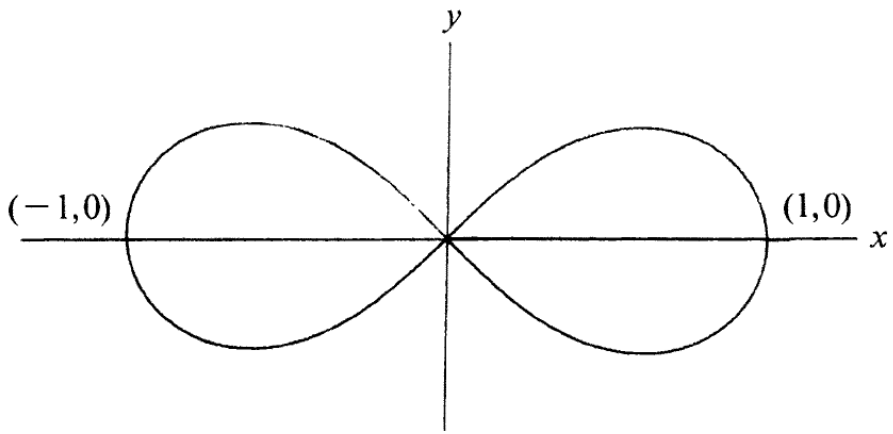


FIG. 1

- By calculus, if we set
$$\frac{L}{2} := \int_0^1 \frac{dx}{\sqrt{1-x^4}}$$
then the arclength of our lemniscate is $2L$. Compare this to the arclength 2π of the unit circle.
- Abel constructs functions $\mathrm{sinlemn}(r)$ and $\mathrm{coslemn}(r)$, which give points on the lemniscate; compare to $\sin(r)$ and $\cos(r)$, which give points on the circle.
- Abel shows that $\mathrm{sinlemn}$ can be extended to a meromorphic function on $\mathbb{C}$, and is periodic w.r.t. the complex lattice
$$\mathbb{Z}2L + \mathbb{Z}2Li := \{2aL + 2bLi : \ a, b \in \mathbb{Z}\}.$$
Call such functions **elliptic,** or **doubly periodic.**
  - Compare this to $\sin(z)$ being periodic w.r.t. $\mathbb{Z}2\pi$.

- Our question is: for what integers $n > 0$ is $\mathrm{sinlemn}(2L/n)$ constructible? E.g., for what values of n are the n-division points for the lemniscate constructible?
- Compare to constructible values of $\sin((2\pi)/n)$, e.g. for which n is the primitive n'th roots of unity $\zeta_n \rightsquigarrow (\cos(2\pi/n), \sin(2\pi/n)) \in S^1$ constructible?
- Abel proves an analogous result to constructibility of the regular n-gon:

Theorem 2 (Abel's Theorem).

The arc of a lemniscate can be divided into n equal parts iff n is a product of a power of 2 and distinct Fermat primes.

- **Main takeaway:** in Gauss' construction, the "dividing points" of the circle were the n'th roots of unity, and such division points generate abelian Galois extensions of $\mathbb{Q}$. Is there a similar interpretation for the "n-division points" on the lemniscate?
- **Yes:** as we will see, we can translate constructibility of $\mathrm{sinlemn}(z)$ to constructibility of $\wp(z)$, which will make this a question about n-torsion points on elliptic curves.

- Let Λ be a *complex lattice*: a discrete rank 2 $\mathbb{Z}$-submodule of $\mathbb{C}$.
  - For example, $\Lambda := \mathbb{Z} + i\mathbb{Z} := \{a + bi : \ a, b \in \mathbb{Z}\}$ is the Gaussian integers.
- We define the *Weierstrass $\wp$-function* on $\mathbb{C}$ as

$$\wp(z) := \wp(z, \Lambda) := \frac{1}{z^2} - \sum_{w \in \Lambda} \left[\frac{1}{w^2} - \frac{1}{(z-w)^2} \right].$$

- As it turns out, one has that
  1. $\wp$ is meromorphic on $\mathbb{C}$;
  2. $\wp$ is doubly periodic on the lattice Λ; so $\forall w \in \Lambda$, $\wp(z + w) = \wp(z)$ for $z \in \mathbb{C}$ where $\wp$ is defined;
  3. $\wp$ and its derivative satisfy an *elliptic curve equation* $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$, where $g_2 := g_2(\Lambda), g_3 := g_3(\Lambda) \in \mathbb{C}$.
- One is also afforded a complex-analytic group isomorphism

$$\mathbb{C}/\Lambda \xrightarrow{\sim} E_\Lambda(\mathbb{C}) : y^2 = 4x^3 - g_2 x - g_3$$

given by the $\wp$-function:

$$z \mapsto (\wp(z), \wp'(z)).$$

Theorem 3.
For a complex number $z \in \mathbb{C}$, $sinlemn(z)$ is constructible iff $\wp(z)$ is constructible.

- So for us, to check constructibility of $\mathrm{sinlemn}(2L/n)$ it suffices to study the values $\wp(2L/n)$, and ultimately the n-torsion points on an elliptic curve.
- With the above isomorphism, the n-torsion points on E_Λ corresponds to the n-torsion on the torus $\mathbb{C}/\Lambda$:

$$(\mathbb{C}/\Lambda)[n] := \{z \in \mathbb{C} : n(z+\Lambda) = (0+\Lambda)\} = \{z \in \mathbb{C} : nz \in \Lambda\}.$$

  We observe that $(\mathbb{C}/\Lambda)[n] = \frac{1}{n}\Lambda/\Lambda$.
  - For example, $(\mathbb{C}/[1,i])[n] = [\frac{1}{n}, \frac{i}{n}]/[1,i]$.
- The conclusion is that the n-torsion of $E := E_\Lambda$ for a lattice $\Lambda = [2L, 2Li]$ is

$$E[n] = \left\{ \left(\wp\left(\frac{2aL+2bLi}{n}\right), \wp'\left(\frac{2aL+2bLi}{n}\right)\right) : 0 \le a, b < n \right\}.$$

  Observe that $\wp(2L/n)$ corresponds to the x-coordinate of n-torsion point $(\wp(2L/n), \wp'(2L/n))$.

- To recap: one has a group isomorphism

$$\exp : (\mathbb{R}/2\pi\mathbb{Z}, +) \xrightarrow{\sim} (S^1, \cdot)$$

by $\theta \mapsto e^{i\theta}$. The n-division points $\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$ of our circle correspond to the n-torsion points of S^1 as a group, which under this isomorphism correspond to the n-torsion points $\{0, \frac{2\pi}{n}, \frac{4\pi}{n} \ldots, \frac{2\pi(n-1)}{n}\}$ of $\mathbb{R}/2\pi\mathbb{Z}$.
  - Thus, the abelian extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is generated by the n-torsion points on S^1.
- In the lemniscate case: Abel constructed a function $\mathrm{sinlemn}$ periodic w.r.t. the lattice $\Lambda := [2L, 2Li]$. One has $\mathrm{sinlemn}(z)$ is constructible iff $\wp(z)$ is constructible. Following that, we noted a group isomorphism

$$(\mathbb{C}/[2L, 2Li], +) \xrightarrow{\sim} (E_\Lambda, +)$$

by $z \mapsto (\wp(z), \wp'(z))$.
- **Question:** is the extension $\mathbb{Q}(E_\Lambda[n])/\mathbb{Q}$ generated by the n-torsion points on E_Λ abelian?

- **No.**
- **BUT:** Just as in Gauss' proof of constructibility of the regular n-gon, Abel's proof essentially constructs an abelian extension replacing $\mathbb{Q}$ with $\mathbb{Q}(i)$. That is, $\mathbb{Q}(i)(E_\Lambda[n])/\mathbb{Q}(i)$ is abelian.
  - For those in the know, observe that $E_{[L,Li]} \cong E := E_{[1,i]}$ has complex multiplication by $\mathbb{Z}[i] = [1, i]$ which has class number one. Thus, $K := \mathbb{Q}(i)$ is the Hilbert class field of itself, and $\mathbb{Q}(E[n])/K = K(E[n])/K$.

- Kronecker was greatly inspired by Abel's work on n-division points on the lemniscate, and how it generated an abelian extension of $\mathbb{Q}(i)$.
- In the mid 19th century, he announced the proof of a theorem characterizing abelian extensions of $\mathbb{Q}$.

Theorem 4 (Kronecker-Weber; 1853, 1886, 1896).

Any abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field $\mathbb{Q}(\zeta_n)$.

- Kronecker's proof was missing the case where the degree is a power of two; Weber offered a proof $\sim$30 years later, but it was also incorrect. Hilbert provided the first complete proof at the end of the 19'th century.

- Also following Abel's work, Kronecker produced abelian extensions for **any** imaginary quadratic field using special values of elliptic and modular functions.
- It was **Kronecker's Jugendtraum** (Kronecker's dream of youth) that any abelian extension of any imaginary quadratic field lies in one of the extensions he created.
- For example, he believed that every abelian extension of $\mathbb{Q}(i)$ lied in some $\mathbb{Q}(i)(\mathrm{sinlemn}(2L/n))$.

- What exactly were the abelian extensions of imaginary quadratic K that Kronecker constructed?
- Recall that $\mathrm{SL}_2(\mathbb{Z})$ is the set of integer matrices with determinant 1.
  - Such matrices define *linear fractional transformations* on the upper half plane $\mathbb{H}$.
- A **modular function** is a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ so that f is "$\mathrm{SL}_2(\mathbb{Z})$-invariant"; that is, for any linear fractional transformation $M \in \mathrm{SL}_2(\mathbb{Z})$ one has

$$f(M \cdot z) = f(z), \ \forall z \in \mathbb{H}.$$

  - For those in the know, note that modular functions define functions on $X(1)(\mathbb{C})$, the moduli space of complex elliptic curves.

- The main example of a modular function is the **modular j-invariant** $j : \mathbb{H} \to \mathbb{C}$, given by

$$j(\tau) := \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots$$

  where $q := e^{2\pi i \tau}$.
- The modular j-invariant agrees with the j-invariant of an elliptic curve: $j(\tau) = j(E_{[1,\tau]})$ for any $\tau \in \mathbb{H}$.
- **Kronecker's Jugendtraum** is that all abelian extensions of an imaginary quadratic field K are given by adjoining to K special values of the modular function $j(\tau)$.
  - This statement is still wrong, as one needs special values of both $j(\tau)$ and $\wp(z)$ – these will correspond to both the j-invariant and the n-torsion on an elliptic curve, respectively.
  - The actual abelian extensions of $E := E_{[1,\tau]}$ will be contained in abelian extensions of K that look like

$$K(j(E), x(E[n]))$$

    where $x(E[n]) \rightsquigarrow \wp\left(\frac{a+b\tau}{n}\right)$ are the x-coordinates of the n-torsion points.

- Kronecker noticed some interesting things about the abelian extensions $K(j(E))/K$ he was creating.
  1. The Galois group $\mathrm{Gal}(K(j(E))/K)$ is isomorphic to the class group $\mathrm{Cl}(K)$;
  2. $K(j(E))/K$ is an unramified extension;
  3. all ideals of K become principal in $K(j(E))$.
- About a decade later, Hilbert conjectured the following generalization: for **any** number field L, there is a unique finite abelian extension L_1 so that
  1. $\mathrm{Gal}(L_1/L) \cong \mathrm{Cl}(L)$;
  2. L_1/L is unramified, and maximal w.r.t. this property;
  3. every ideal of L becomes principal in L_1;
  4. a prime $\mathfrak{p}$ of L splits in L_1 iff $\mathfrak{p}$ is principal.
- What is the connection to ramification and splitting?

- In his study of primes, Kronecker conjectured that a Galois extension L of $\mathbb{Q}$ is characterized by how primes $p \in \mathbb{Z}$ split in L.
  - For example, $\mathbb{Q}(i)$ is the only Galois extension of $\mathbb{Q}$ so that $p \in \mathbb{Z}$ splits in $\mathbb{Q}(i)$ iff $p \equiv 1 \pmod 4$.
- It was M. Bauer who proved this in 1903. Let $S_{L/K}$ be the set of prime ideals of K which split in L.

Theorem 5.
Let L_1, L_2 be Galois extensions of a number field K. Then $S_{L_1/K} \subseteq S_{L_2/K}$ iff $L_2 \subseteq L_1$. In particular, $L_1 = L_2$ iff $S_{L_1/K} = S_{L_2/K}$.

- T. Takagi was a Japanese mathematician who, in his 1903 thesis, proved Kronecker's Jugendtraum for $\mathbb{Q}(i)$ using special values of $\mathrm{sinlemn}$, just as Kronecker had hoped.
- It was Takagi who also proved the main theorems of general class field theory, along with contributions from Weber.
- It involves generalized class groups, and a modulus which will "modulate" the splitting behavior.

- For a number field K, a **modulus** $\mathfrak{m}$ is an integral ideal of K together with a squarefree product of real embeddings $K \hookrightarrow \mathbb{R}$.
  - For example, $n\mathbb{Z}$ is a modulus for $\mathbb{Q}$; so is $n\mathbb{Z} \cdot \infty$, where $\infty : \mathbb{Q} \hookrightarrow \mathbb{R}$ is the usual embedding.
  - An imaginary quadratic field K has no real embeddings, since the identity and conjugation embeddings cannot send K into $\mathbb{R}$. So a modulus here is just an integral ideal of K., e.g. an ideal $I \subseteq \mathcal{O}_K$.
- We usually write a modulus as $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is the integral data and $\mathfrak{m}_\infty$ is the infinite data.
- Recall that for a number field K, its *class group* $\mathrm{Cl}(K)$ is

$$\mathrm{Cl}(K) := \frac{\mathcal{I}(K)}{\mathcal{P}(K)}$$

where

$$\mathcal{I}(K) := \{\text{Ideals} \neq 0\}$$

and

$$\mathcal{P}(K) := \{\text{Principal ideals} \neq 0\}.$$

  - This corresponds to the trivial modulus $\mathfrak{m} = 1 := \mathcal{O}_K$.

- We will construct more general "$\mathfrak{m}$-ideal class groups" as follows.
- Consider the set of nonzero ideals $I \subseteq K$ whose prime factorization does not include any primes which divide $\mathfrak{m}$:

$$\mathcal{I}_{\mathfrak{m}}(K) := \{I \neq 0 \subseteq K : \ \forall \mathfrak{p} \mid \mathfrak{m} \ v_{\mathfrak{p}}(I) = 0\}.$$

So $\mathcal{I}_{\mathfrak{m}}(K)$ is generated by the primes not dividing $\mathfrak{m}$.
  - $\mathcal{I}_1(K) = \mathcal{I}(K)$.
  - For $K = \mathbb{Q}$, $\mathcal{I}_{6\mathbb{Z}}(\mathbb{Q}) = \{\text{fractional ideals } \frac{a}{b}\mathbb{Z} : 6 \nmid a, 6 \nmid b\}$.
- Next, consider the set of principal ideals with a generator congruent to 1 mod $\mathfrak{m}_0$ and positive under real embeddings. Namely,

$$\mathcal{P}_{\mathfrak{m}}(K) := \{I \neq 0 \subseteq K : \ \exists \alpha \in K \text{ so that } I = \alpha\mathcal{O}_K, \alpha \equiv 1 \pmod{\mathfrak{m}_0}$$
$$\text{and } \forall \infty \mid \mathfrak{m}_\infty \ \infty(\alpha) > 0\}.$$

Some facts:
  - $\mathcal{P}_1(K) = \mathcal{P}(K)$.
  - For $K = \mathbb{Q}$, we have $(2) \in \mathcal{P}_{3\mathbb{Z}}(\mathbb{Q})$ but $(3) \notin \mathcal{P}_{3\mathbb{Z}}(\mathbb{Q})$.
- Certainly $\mathcal{P}_{\mathfrak{m}}(K) \subseteq \mathcal{I}_{\mathfrak{m}}(K)$. Their quotient is the **$\mathfrak{m}$-ideal class group**

$$\mathrm{Cl}_{\mathfrak{m}}(K) := \frac{\mathcal{I}_{\mathfrak{m}}(K)}{\mathcal{P}_{\mathfrak{m}}(K)}.$$

- For a number field K and a modulus $\mathfrak{m}$ in K, call any subgroup $H \subseteq \mathrm{Cl}_{\mathfrak{m}}(K)$ a **congruence subgroup mod** $\mathfrak{m}$.
  - Congruence subgroups correspond to intermediate subgroups $\mathcal{P}_{\mathfrak{m}}(K) \subseteq H_0 \subseteq \mathcal{I}_{\mathfrak{m}}(K)$. We will interchange H and H_0.
- Each congruence subgroup H contains (an infinite amount of) prime ideals. As we will see, this will be the splitting information we'll need for our *class fields*.
- For a congruence subgroup H, a **class field** is a finite abelian extension K_H/K with splitting information the set of primes in H: namely,

$$\mathfrak{p} \subseteq K \text{ splits completely in } K_H \Leftrightarrow \mathfrak{p} \in H.$$

- Class fields are unique, by Bauer's result.
- As an example, the class field of $H_0 := \mathcal{P}_{(4)\infty}(\mathbb{Q})$ is $\mathbb{Q}(i)$, since for a prime $p \in \mathbb{Z}$ one has $p \in H$ iff $p > 0$ and $p \equiv 1 \pmod 4$.

Theorem 6 (Class Field Theory. Takagi, 1920).

Let K be a number field.

1. *(Existence) For each congruence subgroup $H \subseteq Cl_{\mathfrak{m}}(K)$, there is a* **class field** *for H: namely, a finite abelian extension K_H/K so that*

$$\mathfrak{p} \subseteq K \text{ splits completely in } K_H \Leftrightarrow \mathfrak{p} \in H.$$

2. *(Isomorphism) One has $G(K_H/K) \cong H$.*
3. *(Completeness) Any finite abelian extension of K is a class field for some congruence subgroup H.*
4. *(Comparison) If $H_1, H_2 \subseteq Cl_{\mathfrak{m}}(K)$, then $L_{H_1} \subseteq L_{H_2}$ iff $H_2 \subseteq H_1$.*

Class field theory for $\mathbb{Q}$.

- Let us prove the Kronecker-Weber Theorem: **every abelian extension of $\mathbb{Q}$ is contained in some cyclotomic field $\mathbb{Q}(\zeta_n)$.**
- **Step 1:** The class field for $\mathbb{Q}$ of modulus $(n)\infty$ is the cyclotomic field $\mathbb{Q}(\zeta_n)$.
  - By algebraic number theory, a prime $p \in \mathbb{Z}_{>0}$ splits in $\mathbb{Q}(\zeta_n)$ iff $p \equiv 1 \pmod{n}$.
  - Then we observe that $p \equiv 1 \pmod{n}$ iff $(p) \in \mathcal{P}_{(n)\infty}(\mathbb{Q})$.
  - So by definition, $\mathbb{Q}(\zeta_n)$ is the class field for $(n)\infty$.
- **Step 2:** Let $K/\mathbb{Q}$ be abelian. By Class Field Theory, K corresponds to a congruence subgroup H for some modulus $\mathfrak{m}$.
- Any modulus for $\mathbb{Q}$ is of the form (n) or $(n)\infty$. Note that $\mathcal{P}_{(n)\infty}(\mathbb{Q}) \subseteq \mathcal{P}_{(n)}(\mathbb{Q})$.
- We thus have $\mathcal{P}_{(n)\infty}(\mathbb{Q}) \subseteq H$ for some n, so by Comparison we get $\mathbb{Q}_H = K \subseteq \mathbb{Q}_{(n)\infty} = \mathbb{Q}(\zeta_n)$. QED.

- Following the above, we have an explicit class field theory for $\mathbb{Q}$: for example, we know that the $(n)\infty$-class fields are the cyclotomic fields $\mathbb{Q}(\zeta_n)$.
  - Such extensions are generated by special values of e^z on n-torsion $0, \frac{2\pi}{n}, \ldots, \frac{2\pi(n-1)}{n}$ of $\mathbb{R}/2\pi\mathbb{Z}$.
- One also has an explicit class field theory of imaginary quadratic fields K, described by complex multiplication.
  - The $\mathfrak{m}$-class fields are generated by special values of $j(z)$ on quadratic numbers $\tau \in \mathbb{H}$ and $\wp(z)$ on n-torsion $\frac{a+b\tau}{n}$, $0 \leq a, b < n$ on $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$, for a particular τ.
- Following this theme, for a number field K what other special values of transcendental functions must we look at to generate class fields for K?
- This is the question of **Hilbert's Twelfth Problem.** There is much work to be done on this front.

References

[1] Keith Conrad, *History of Class Field Theory*.
https://kconrad.math.uconn.edu/blurbs/gradnumthy/cfthistory.pdf.
[2] J.S. Milne, *Class Field Theory*. Version 4.02.
https://www.jmilne.org/math/CourseNotes/CFT.pdf.
[3] Michael Rosen, *Abel's Theorem on the Lemniscate*. Amer. Math. Monthly, Vol. 88 (1981), 387–395.
[4] Joseph Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151, Springer, 1994.