Introduction to Number Theory

Math 110 | Winter 2023

Xu Gao

February 6, 2023

What we have seen last week

- ***Diophantine approximation***: approximate irrational numbers by rational numbers.
- ***Dirichlet's approximation theorem***: $\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{2b^2}$.
- ***Ford circle***: a circle of diameter $\frac{1}{b^2}$ atop the rational point $\frac{a}{b}$. ← reduced
- ***Kissing fractions*** ($\frac{a}{b} \heartsuit \frac{c}{d}$): $\left|\det \begin{pmatrix} a & c \\ b & d \end{pmatrix}\right| = |ad - bc| = 1$.
- ***Mediant***: $\frac{a}{b} \vee \frac{c}{d} := \frac{a+c}{b+d}$.
- ***Farey sequence***: repeatedly taking mediants, containing all reduced fractions.

Today's topics

- Finish proving Dirichlet's approximation theorem.
- Higher Diophantine equations

Dirichlet’s approximation theorem

Dirichlet's approximation theorem

Theorem 11.1 (Dirichlet, 1840)

Let α be an **irrational** *number, Then there are infinitely many fractions $\frac{a}{b}$ such that*

$$\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{2b^2}.$$

To prove Dirichlet's approximation theorem, it is sufficient to show that a vertical line atop an irrational point crosses infinitely many Ford circles.

Lemma 11.2

The following process generates all reduced fractions (in geometric words, all Ford circles):

1. *Start with integers, namely fractions of the form* $\frac{n}{1}$ *(in geometric words, Ford circles atop integer points).*
2. *Whenever you have two kissing fractions* $\frac{a}{b}$ *and* $\frac{c}{d}$*, generate their* **mediant** $\frac{a}{b} \vee \frac{c}{d}$ *(in geometric words, whenever you have two Ford circles tangent to each other, generate the third one atop the mediant).*

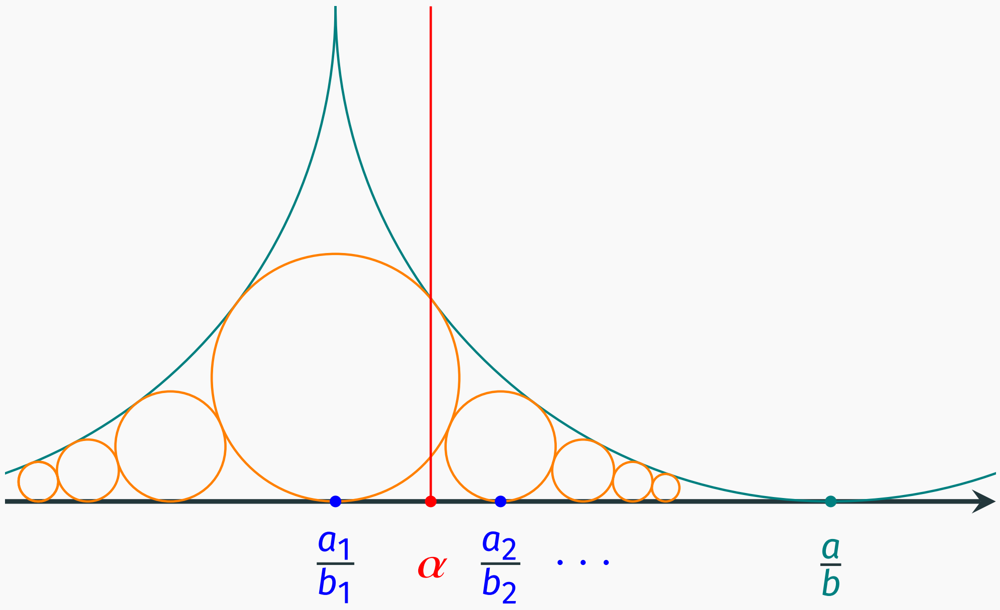
Proof of the theorem

(Dirichlet's Approximation Theorem)

Proof. We prove the theorem using the recursive process in the Farey sequence.

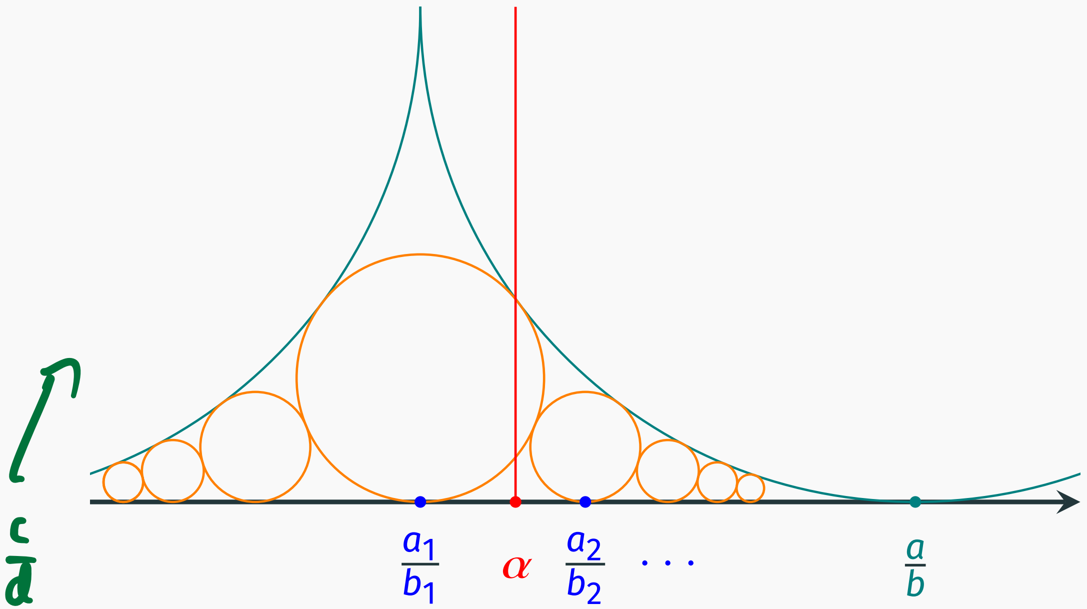
- At the base step, the vertical line $x = \alpha$ must cross one of the Ford circles atop some $\frac{n}{1}$ since α is irrational.
- Whenever the vertical line $x = \alpha$ crosses a Ford circle (saying, atop $\frac{a}{b}$) and falls into the mesh triangle below it, then it must cross another Ford circle inside the mesh triangle.
- The process will go on forever as the Farey sequence and thus produce infinitely many Ford circles crossed by the line $x = \alpha$.

Proof of the theorem



The proof boils down to show the following: Suppose the vertical line $x = \alpha$ crosses the Ford circle atop $\frac{a}{b}$, then it also crosses a Ford circle inside the mesh triangle below.

Proof of the theorem



Suppose the mesh triangle is given by the Ford circles atop $\frac{a}{b}$ and $\frac{c}{d}$. Then we know that α must leave between $\frac{a}{b}$ and $\frac{c}{d}$ since the vertical line $x = \alpha$ crosses the mesh triangle. We may assume $\frac{a}{b} > \alpha > \frac{c}{d}$.

Consider the following sequence of fractions:

$$\frac{a_0}{b_0} := \frac{c}{d}, \frac{a_1}{b_1} := \frac{a}{b} \vee \frac{c}{d}, \cdots, \frac{a_n}{b_n} := \frac{a}{b} \vee \frac{a_{n-1}}{b_{n-1}}, \cdots$$

Then the Ford circle atop each $\frac{a_n}{b_n}$ $(n > 0)$ is tangent to the one atop $\frac{a}{b}$ and all of them leave inside the mesh triangle.

Proof of the theorem

Note that

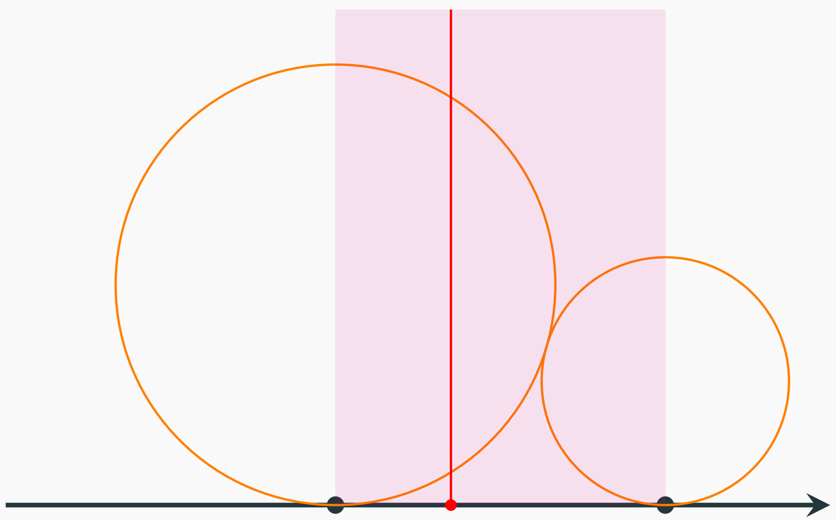
$$\frac{a_n}{b_n} = \frac{a \cdot n + c}{b \cdot n + d}.$$

Hence, the sequence of rational numbers $(\frac{a_n}{b_n})_{n \in \mathbb{Z}}$ is monotonously increasing and has the limit $\frac{a}{b}$. Then, since $\frac{a}{b} > \alpha > \frac{c}{d}$, there must be a positive integer n such that

$$\frac{a_n}{b_n} > \alpha > \frac{a_{n-1}}{b_{n-1}}.$$

Namely, the vertical line $x = \alpha$ crosses the strip between $\frac{a_n}{b_n}$ and $\frac{a_{n-1}}{b_{n-1}}$.

Proof of the theorem



But notice that $\frac{a_n}{b_n} \heartsuit \frac{a_{n-1}}{b_{n-1}}$. Namely, the Ford circles atop $\frac{a_n}{b_n}$ and $\frac{a_{n-1}}{b_{n-1}}$ are tangent to each other. Hence, to cross the strip between $\frac{a_n}{b_n}$ and $\frac{a_{n-1}}{b_{n-1}}$, the vertical line $x = \alpha$ must cross one of the two Ford circles! Thus, we find a Ford circle inside the initial mesh triangle and is crossed by the line $x = \alpha$ as desired.

Higher Diophantine equations

Higher Diophantine equations

Question (Diophantine equations)

≥ 2

Given a multivariable integer polynomial P, find integer (or rational) solutions $\mathbf{x} = (x_i)_i$ of the equation

$$P(\mathbf{x}) = 0.$$

Example 11.3 (Pythagorean Triples)

Find all triples of integers (a, b, c) such that

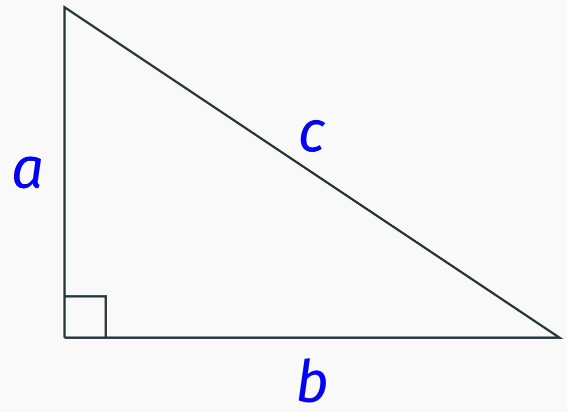
$$a^2 + b^2 = c^2. \qquad X^2 + Y^2 - Z^2 := P$$

Example 11.3 (Pythagorean Triples)

Find all triples of integers (a, b, c) such that

$$a^2 + b^2 = c^2.$$

The terminology comes from the ***Pythagorean theorem***:



To figure out all solutions of 11.3, we first note that

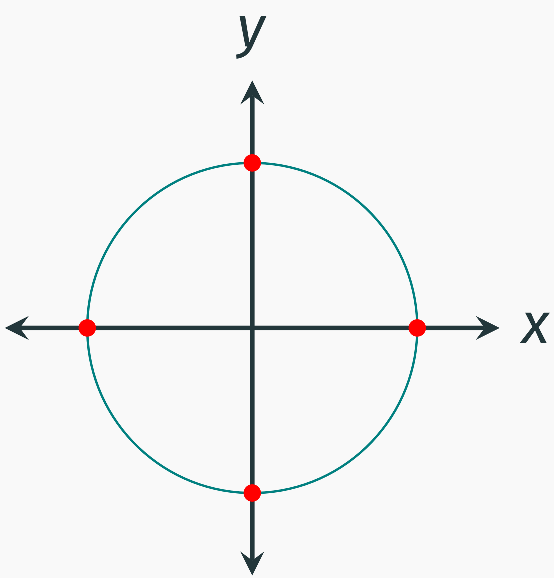
- $(0,0,0)$ is a solution (the *trivial solution*) of the equation

$$a^2 + b^2 = c^2.$$

- Any *nontrivial* solution (a, b, c) gives a ***rational*** solution $\left(\frac{a}{c}, \frac{b}{c}\right)$ of the equation

$$X^2 + Y^2 = 1.$$

Recall that the equation $X^2 + Y^2 = 1$ defines the unit circle.



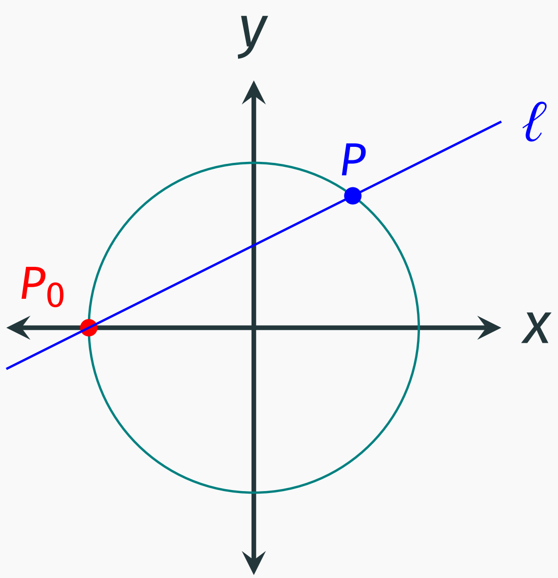
The ***rational*** solutions of the equation correspond to the ***rational points*** on the unit circle.

coordinates are rational

For instance, $(1, 0)$, $(0, 1)$, $(-1, 0)$, and $(0, -1)$ are four obvious rational points on the unit circle.

The question is: what are all the rational points on the unit circle?

We start with a specific rational point, saying $P_0 = (-1, 0)$. Draw a (non-vertical) line ℓ through P_0, then it intersects with the unit circle by a point $P = (x, y)$.



If P is a rational point, then the ***slope*** of ℓ is

$$\frac{y - 0}{x - (-1)} = \frac{y}{x + 1},$$

which is a rational number. ∵ $\mathbb{Q}$ is closed under +, div

Higher Diophantine equations

Conversely, suppose the ***slope*** of ℓ is a rational number t. Then the intersection point $P = (x, y)$ satisfies the system of equations:

$$\begin{cases} y = t(x+1), \\ x^2 + y^2 = 1. \end{cases}$$

$x \neq -1 \Leftarrow P \neq P_0$

Solving it, we get:

$$\begin{aligned} & x^2 + t^2(x+1)^2 = 1 \\ \iff & x^2 - 1 + t^2(x+1)^2 = 0 \\ \iff & x - 1 + t^2(x+1) = 0 \\ \iff & x = \frac{1-t^2}{1+t^2}. \end{aligned}$$

$x^2 - 1 = (x+1)(x-1)$

div by $x+1$

$y = t \cdot (x+1)$

Hence, $P = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ is a rational point.

$t = \frac{m}{n}$

$P = \left(\frac{n^2-m^2}{n^2+m^2}, \frac{2mn}{n^2+m^2} \right)$

We thus proved the following.

Lemma 11.4

Fix a rational point $P_0 = (-1, 0)$ on the unit circle. Then the rational points on the unit circle other than P_0 are one-one corresponding to lines through P_0 with slope $t \in \mathbb{Q}$. $\leftrightsquigarrow$ $t \in \mathbb{Q}$

This lemma allows we to parameterize the solution set

$$\{(x, y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 1\}$$

in $\mathbb{Q} \cup \{\infty\}$ (where P_0 corresponds to ∞).

Theorem 11.5 (Pythagorean Triples)

The Pythagorean triples are given by

$$\left\{(a,b,c)\in\mathbb{Z}^3 \;\middle|\; a^2+b^2=c^2\right\}$$
$$=\mathbb{Z}\cdot\left\{(n^2-m^2,2mn,m^2+n^2) \;\middle|\; (m,n)\in\mathbb{Z}^2\right\}$$

nonzero

Proof. Up to scales, the Pythagorean triples (a,b,c) correspond to rational points $(\frac{a}{c},\frac{b}{c})$ and thus correspond to $\frac{m}{n}\in\mathbb{Q}\cup\{\infty\}$. □

$$P=\left(\frac{n^2-m^2}{n^2+m^2},\ \frac{2mn}{n^2+m^2}\right)$$

$\frac{1}{0}$

Question

Find all triples of integers (a, b, c) *such that*

$$a^2 + b^2 = N \cdot c^2.$$

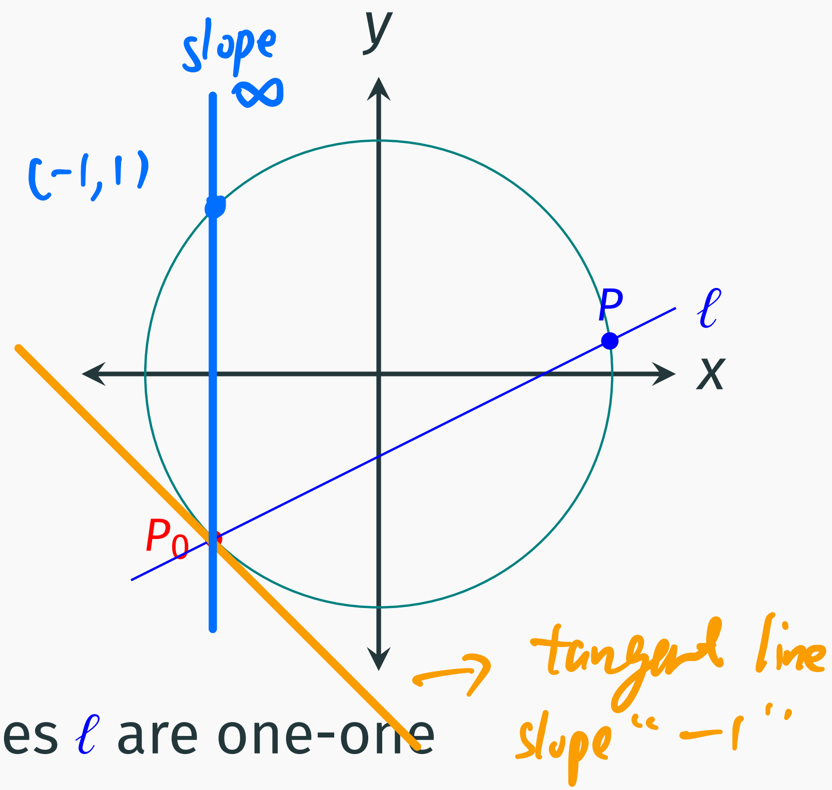
Or, equivalently, find all rational points on the circle

$$X^2 + Y^2 = N.$$

N.B. $\underline{\overset{N_1}{\overset{\shortparallel}{(a^2 + b^2)}}}\,\underline{\overset{N_2}{\overset{\shortparallel}{(c^2 + d^2)}}} \overset{\Rightarrow}{=} \underline{\overset{N}{\overset{\shortparallel}{(ac - bd)^2 + (ad + bc)^2}}}$. Hence, it is sufficient to consider only N = primes.

$N = N_1 \cdot N_2$

When $N = 2$. We can find some specific rational points on the circle $X^2 + Y^2 = 2$. For instance, $P_0 = (-1, -1)$.
Draw a line ℓ through P_0. Then it intersects with the circle by a point $P = (x, y)$.



The points P and the slopes of the lines ℓ are one-one corresponding via:

$$\left(\frac{1+2t-t^2}{1+t^2}, \frac{t^2+2t-1}{1+t^2}\right) \leftrightsquigarrow t \in \cancel{\mathbb{Q}}. \quad \mathbb{Q} \cup \{\infty\} \setminus \{-1\}$$

$$\left(\frac{n^2+2nm-m^2}{n^2+m^2}, \frac{m^2+2mn-n^2}{n^2+m^2}\right) \rightsquigarrow \frac{m}{n}$$

We thus conclude similarly:

1. The rational points on the circle $X^2 + Y^2 = 2$ are parameterized in $\mathbb{Q} \cup \{\infty\}$ (where P_0 corresponds to $\cancel{\infty}\,-1$) via

$$t \in \overset{\mathbb{Q}\cup\{\infty\}}{\cancel{\mathbb{Q}}} \longmapsto \left(\frac{1+2t-t^2}{1+t^2}, \frac{t^2+2t-1}{1+t^2}\right).$$

2. We thus have

$$\left\{(a,b,c) \in \mathbb{Z}^3 \,\middle|\, a^2 + b^2 = 2c^2\right\}$$
$$= \mathbb{Z} \cdot \left\{(n^2 + 2mn - m^2, m^2 + 2mn - n^2, m^2 + n^2) \,\middle|\, (m,n) \in \mathbb{Z}^2\right\}$$

After Class Work

In the proof of Dirichlet's theorem, if we consider the mesh triangle enclosed by three tangent Ford circles rather than the mesh triangle under two tangent Ford circles, we may have a better bound:

Theorem 11.6

Let α *be an* **irrational** *number, Then there are infinitely many fractions* $\frac{a}{b}$ *such that*

$$\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{\sqrt{5}b^2}.$$

For details, you can find the paper "*Fractions*" by L. Ford.

See Canvas

Terminology

The solution set of a *polynomial* equation (more generally, a system of *polynomial* equations) with coefficients in (a ring) R is called an ***algebraic set defined over*** R.

Example 11.7

$\left\{(a, b, c) \in \mathbb{Z}^3 \,\middle|\, a^2 + b^2 = c^2\right\}$ is an algebraic set **in** $\mathbb{Z}^3$ **defined over** $\mathbb{Z}$.

$\left\{(x, y) \in \mathbb{Q}^2 \,\middle|\, x^2 + y^2 = 1\right\}$ is an algebraic set **in** $\mathbb{Q}^2$ **defined over** $\mathbb{Z}$.

Terminology

Let $x_1, \cdots, x_k$ be unknowns. Then the ***total degree*** of a monomial $C{x_1}^{n_1} \cdots {x_k}^{n_k}$ is $n_1 + \cdots + n_k$.

A polynomial is ***homogeneous*** if the total degrees of its terms are all the same.

Example 11.8

$x^2 + y^2 = z^2$ is a homogeneous polynomial equation defined over $\mathbb{Z}$, while $x^2 + y^2 = 1$ is not a homogeneous polynomial equation.

Terminology

An algebraic set is ***projective*** if it can be defined by homogeneous polynomial equations. Note that projective algebraic sets are stable under nonzero multiplication.

Example 11.9

The algebraic set $\left\{(a, b, c) \in \mathbb{Z}^3 \,\middle|\, a^2 + b^2 = c^2\right\}$ is projective.

Usually, we would rather put a projective algebraic set in a ***projective space***.

Terminology

An ***equivalence relation*** on a set S is a relation $\sim$ satisfying

- (***reflexivity***) for all $a \in S$, $a \sim a$;
- (***symmetry***) for all $a, b \in S$, if $a \sim b$, then $b \sim a$;
- (***transitivity***) for all $a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

N.B. Compare the notions of ***equivalence relation*** and ***partial order***. The property ***symmetry*** is almost the opposite of ***antisymmetry***.

Example 11.10

In a vector space V (over a field such as $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$), two vectors $x, y \in V$ are ***homothetic*** if there is a nonzero number $r \in \mathbb{R}$ such that $y = rx$. "Being homothetic" is an equivalence relation.

Terminology

Let S be a set and $\sim$ an equivalence relation on it. An ***equivalence class*** in S is a subset E such that:

- E is nonempty;
- Any two $a, b \in E$ have relation $\sim$;
- For any $a \in S$, if $a \sim b$ for some $b \in E$, then $a \in E$.

Then the set of equivalence classes in S is called the ***quotient set of*** S ***up to*** $\sim$, denoted by $S/\sim$.

We usually use $[a]$ to denote the equivalence class of $a \in S$.

Terminology

Let R be a field such as $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$. The quotient set

$$\mathbf{P}^n(R) := (R^{n+1} \setminus \{(0, \cdots, 0)\})/\text{homothety}$$

is called the ***n-dimensional projective space over*** R. When $n = 1$, it is called the ***projective line***.

Example 11.11

The projective line $\mathbf{P}^1(\mathbb{Q})$ can be identified with the set $\mathbb{Q} \cup \{\infty\}$. One way to do this is mapping $[a : b]$ $(b \neq 0)$ to $\frac{a}{b}$ and $[1 : 0]$ to ∞.