# Algebra 2

IMPA, August – December 2020

---

## Part I: Galois theory

### 1 Motivation

#### 1.1 Constructions with ruler and compass

Knowledge of ancient Greece:

- natural numbers $1, 2, 3, \ldots$
- ratios $\frac{p}{q}$ of natural numbers $p$ and $q$
- square roots

Approach: Constructions by ruler & compass

Question: Which numbers are constructible with ruler & compass?

Definition:

Given (constructed) points $0, 1, P_1, \ldots, P_n$ in the Euclidean plane $\mathbb{R}^2$, we call a point $Q \in \mathbb{R}^2$ constructible from $P_1, \ldots, P_n$ if it can be derived in terms of the following operations:

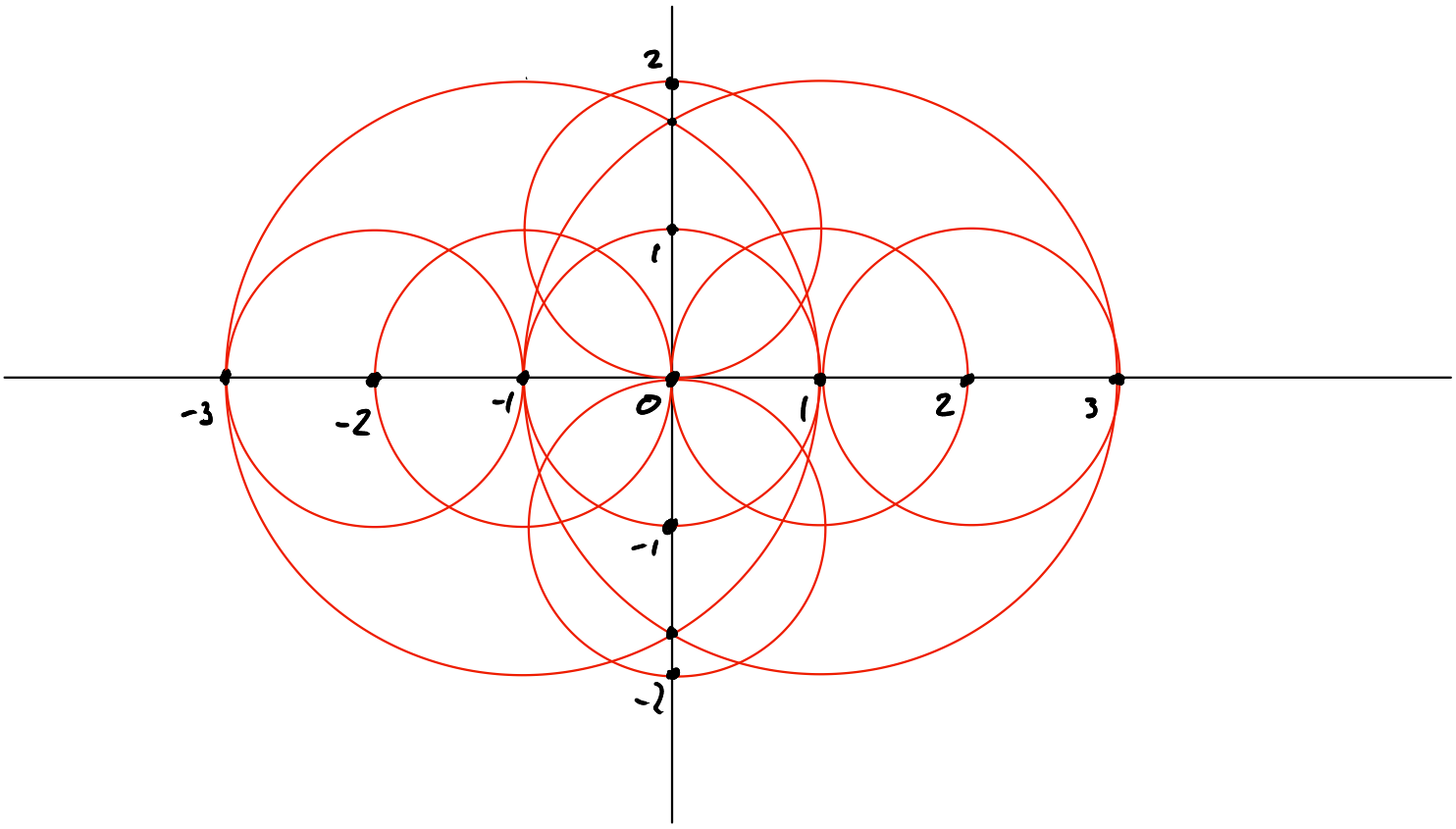
(1) draw a line through two constructed points;

(2) draw a circle around a constructed point whose radius equals the distance between two constructed points;

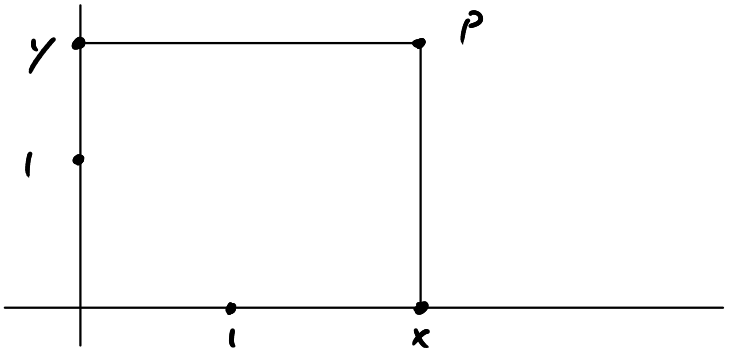
(3) call intersection points of lines and circles constructed points.

Def: A positive real number is constructible if it occurs as the distance between two points in $\mathbb{R}^2$ that are constructible from 0 and 1.

Coordinates: given 0 and 1 in the plane:




Rem: In particular note that we can draw orthogonal lines. Thus knowing a point $P$ is equivalent to knowing its coordinates $x$ and $y$:

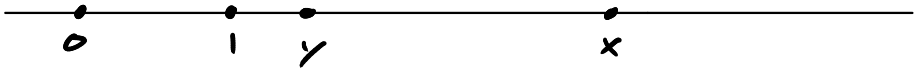



(Details are left as an exercise.)

Thus constructible points $P \in \mathbb{R}^2$ correspond to constructible real numbers $x \in \mathbb{R}_{\geq 0}$.

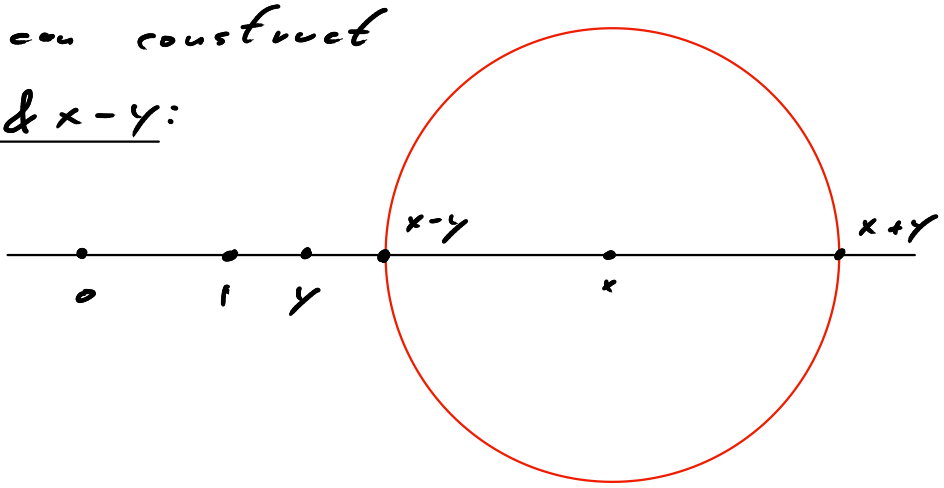
# Arithmetic operations

Given

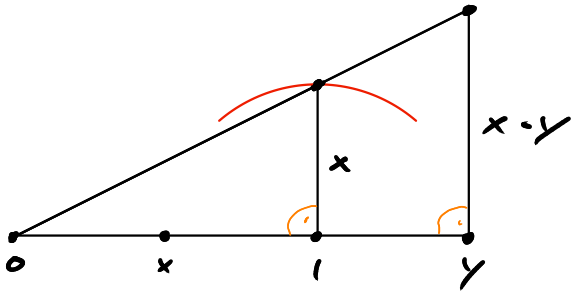



we can construct

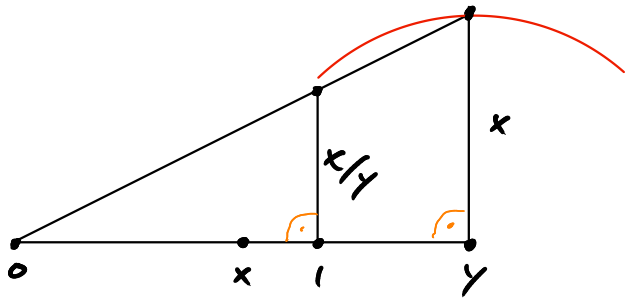
**$x+y$ & $x-y$:**




**$x \cdot y$:**

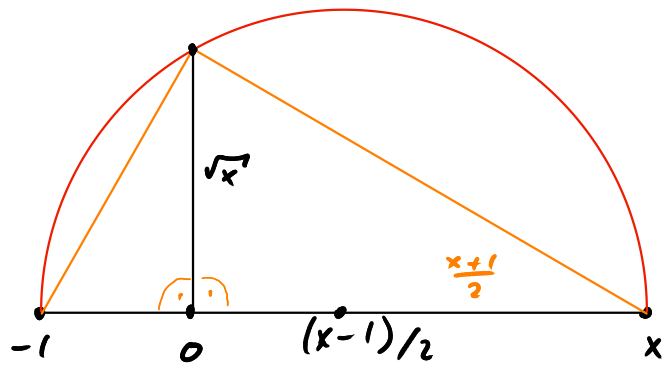



**$x / y$:**



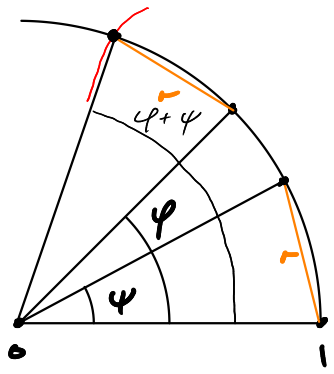

**Conclusion:** constructible numbers together with their additive inverses form a subfield of $\mathbb{R}$ that contains $\mathbb{Q}$, and more:

**$\sqrt{x}$:**

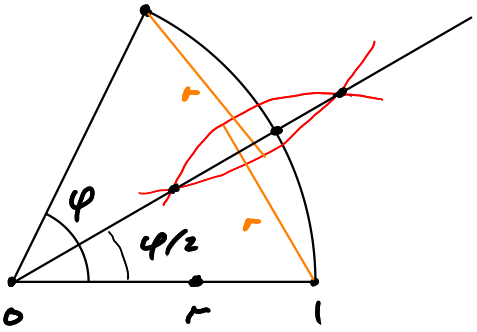



(Details left as an exercise!)

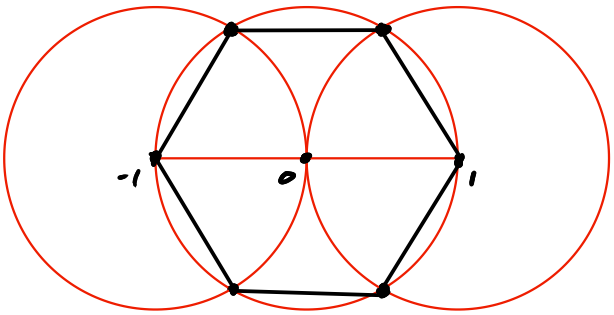
$\varphi + \psi$:




$\varphi/2$:




Euclid constructed regular $n$-gons for all $n \geq 3$ of the form $n = 2^r \cdot 3^i \cdot 5^j$ with $r \geq 0$ and $i, j \in \{0, 1\}$. For example, the regular hexagon can be constructed as follows:




Problem of the antique:

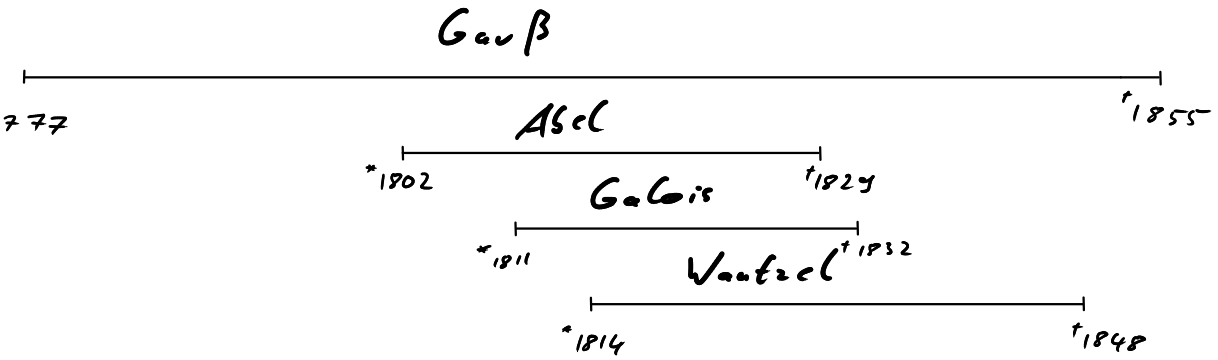
(1) Double the cube: given a cube with volume $V$ and side length $a$, can we construct a cube with volume $2V$, i.e. its side length $b = \sqrt[3]{2} \cdot a$?

(2) Trisect the angle: given a angle $\varphi$, can we construct $\varphi/3$?

(3) Square the circle: given a circle with area $A$ and radius $r$, can we construct a square with area $A$, i.e. its side length $a = \sqrt{\pi} \cdot r$?

(4) For which $n \geq 3$ is it possible to construct a regular $n$-gon?

Answers:




Gauß 1796: Construction of the regular 17-gon.

Wantzel 1837: - Construction of the regular 257-gon and 65537-gon;
- $\sqrt[3]{2}$ is not constructible;
- trisecting an angle is not possible.

Lindemann 1882: $\pi$ is "transcendental"
$\Rightarrow$ not constructible
$\Rightarrow$ squaring the circle is not possible.

## 1.2 Equations of low degree

Degree 2: $aX^2 + bX + c = 0$

has two solutions

$$X = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Degree 3: (Ferro, Tartaglia, Cardano)

→ Ars Magna 1545

$$aX^3 + bX^2 + cX + d = 0$$

replacing $X$ by $Y = X - \frac{b}{3a}$ yields

$$Y^3 + pY + q = 0$$

for some $p, q$. If $\Delta = \frac{q^2}{4} + \frac{p^3}{27} > 0$, then

$$Y = \sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}}$$

is a solution.

Degree 4: Formula by Ferrari, in Ars Magna

Degree 5: No formula

1799 Ruffini (incomplete proof)
1824 Abel
1845 Wantzel (classified with Galois theory)

## 1.3 What is Galois theory?

Study roots of polynomials

$$f = T^n + c_{n-1}T^{n-1} + \dots + c_0$$

with coefficients in a field $K$.

Fact: There is a smallest field $L$ containing $K$ and all roots of $f$.

**Def:** • $Aut_K(L) = \left\{ \sigma : L \to L \;\middle|\; \begin{array}{l} \sigma \text{ bijective, } \sigma(a) = a \;\; \forall a \in K \\ \sigma(a+b) = \sigma(a) + \sigma(b), \\ \sigma(ab) = \sigma(a)\cdot\sigma(b) \quad \forall a, b \in L \end{array} \right\}$

• $[L : K] = \dim_K L$

• $L$ is <u>Galois over $K$</u> if $\# Aut_K(L) = [L:K]$ and $[L:K]$ is finite; in this case, $Gal(L/K) := Aut_K(L)$ is called the <u>Galois group of $L$ over $K$.</u>

**<u>Thm</u>** (Galois, 1833)

$L/K$ Galois

$G = Aut_K(L)$

Then the maps

$$\left\{ \begin{array}{c} \text{intermediate fields} \\ K \subset E \subset L \end{array} \right\} \xleftrightarrow{1:1} \left\{ \begin{array}{c} \text{subgroups} \\ H < G \end{array} \right\}$$

$$E \longmapsto Aut_E(L)$$

$$L^H = \{ a \in L \mid \sigma(a) = a \;\; \forall \sigma \in H \} \longmapsfrom H$$

are mutually inverse bijections.

Moreover, $E$ is Galois over $K$ if and only if $Aut_E(L)$ is a normal subgroup of $G$.