Lecture Notes On Abstract Algebra (Week 10)

Guohua PENG (彭国华)
email: peng@scu.edu.cn

Contents

1 Lecture 18 (Nov 7, 2023): Algebraic Extensions

1.1 Degree of A Field Extension

Recall every F-module is also called a vector space over F.

Basic Observation Every extension field of F is a vector space over F.

Definition 1.1. *Let K/F be an extension of fields. The dimension of the vector space K over F is called the* **degree** (扩张次数) *of the extension K/F, written $[K : F]$. We say that K is* **finite** *over K if $[K : F]$ is finite. Otherwise, K is called an* infinite extension *over F.*

$$\boxed{[K : F] = \dim_F(K).}$$

Example 1.1. 1. For $F = \mathbb{Q}(i)$, where $i = \sqrt{-1}$, we have $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Actually $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ and $1, i$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(i)$.

2. Let n be a positive integer. By Eisenstein criterion, $x^n - 2$ is irreducible over $\mathbb{Q}$. Then $\alpha = \sqrt[n]{2}$ is an algebraic number of degree n. And Theorem 2.2 in last lecture implies that the extension degree $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$.

3. The field $F(x)$ is infinite extension over F. Similarly, $[\mathbb{R} : \mathbb{Q}] = \infty$.

Theorem 1.1. *Let $\alpha \in K$ be algebraic over F of degree n. Then $[F(\alpha) : F] = n$.*

Proof. Let $m(x)$ be the minimal polynomial of α over F. Theorem 2.2 in last lecture shows that $1, \alpha, \ldots, \alpha^{n-1}$ span the F-vector space $F(\alpha)$. Assume

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$$

for some $a_0, a_1, \ldots, a_{n-1} \in F$. Then $f(\alpha) = 0$ with $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in F[x]$. By Proposition 2.3 in last lecture, we have $m(x) \mid f(x)$. But $\deg m(x) = n$. Hence $f(x) = 0$, yielding $a_0 = a_1 = \cdots = a_{n-1} = 0$. This implies that $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent over F and then $[F(\alpha) : F] = n$. □

If we use $\deg_F(\alpha)$ to denote the degree of the minimal polynomial of an algebraic element α over F, the above corollary says

$$\boxed{[F(\alpha):F] = \deg_F(\alpha).}$$

Corollary 1.1. *Let K/F be an extension of fields and $\alpha \in K$ an algebraic element over F. For any intermediate field M with $F \subseteq M \subseteq K$,*

$$[M(\alpha):M] \leq [F(\alpha):F].$$

$$\begin{tikzcd}
 & M(\alpha) \arrow[dl, dash] \arrow[dr, dash] & \\
M \arrow[dr, dash] & & F(\alpha) \arrow[dl, dash] \\
 & F &
\end{tikzcd}$$

Proof. Clearly $\alpha \in K$ is an algebraic element over M. Let $m_1(x), m_2(x)$ be the minimal polynomial of α over F and M respectively. Then $m_1(x) \in M[x]$ and $m_1(\alpha) = 0$ implies $m_2(x) \mid m_1(x)$. Hence $[M(\alpha):M] \leq [F(\alpha):F]$, by Theorem 1.1. □

1.2 Finite Extensions

Theorem 1.2. *Let K/F be an extension of fields. Then $\alpha \in K$ is algebraic over F if and only if $F(\alpha)/F$ is a finite extension.*

Proof. If α is algebraic of degree n, then $1, \alpha, \ldots, \alpha^{n-1}$ span the vector space $F(\alpha)$ over F. Hence $F(\alpha)/F$ is a finite extension.

Conversely, if $F(\alpha)/F$ is a finite extension, then $1, \alpha, \alpha^2, \ldots$ must be linearly dependent over F. Thus there exist some elements $a_0, a_1, \ldots, a_{m-1}, a_m$ in F such that

$$a_0 \cdot 1 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} + a_m\alpha^m = 0, \text{ and } a_m \neq 0.$$

This shows that α is a root of the nonzero polynomial

$$m(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0.$$

Consequently α is algebraic over F. □

Remark 1.1.

1. The minimal value of m in the above proof of necessity is just the degree of α. Actually, the minimal m is the positive integer such that $1, \alpha, \ldots, \alpha^{m-1}$ are linearly independent, but $1, \alpha, \ldots, \alpha^{m-1}, \alpha^m$ are linearly dependent. Hence α^m is a linear combination of $1, \alpha, \ldots, \alpha^{m-1}$. That is, there exist $a_0, a_1, \ldots, a_{m-1} \in F$ such that

   $$\alpha^m = b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1}.$$

   It follows that $m(x) = x^m - b_{m-1}x^{m-1} - \cdots - b_1 x - b_0$ is the minimal polynomial of α.

2. The necessity of the above theorem may be proved in another way. Assume $[F(\alpha):F] = n$ and $\alpha_1, \alpha_2, \ldots, \alpha_n$ is an F-basis of $F(\alpha)$. The map

   $$\begin{aligned} \tau_\alpha : F(\alpha) &\to F(\alpha) \\ u &\mapsto \alpha u. \end{aligned}$$

defines a linear transformation of $F(\alpha)$. Let $m(x)$ be the characteristic polynomial of τ_α. Then Hamilton-Cayley Theorem implies

$$m(\alpha) = m(\tau_\alpha)(1) = 0.$$

That is, α is a root of $m(x)$. So α is algebraic over F.

Corollary 1.2. *If α is algebraic over F, then so is every element of $F(\alpha)$. In particular, $[F(u) : F] \leq [F(\alpha) : F]$ for every $u \in F(\alpha)$.*

Example 1.2. It's easy to see that $\alpha = \sqrt[5]{3}$ is an algebraic number of degree 5. Then $\beta = 2 - \alpha + 2023\alpha^4$ is also an algebraic number with degree less than 5. What's the minimal polynomial of β?

Theorem 1.3 (**Transitivity of Extension Degree**)**.** *Let $F \subseteq M \subseteq K$ be finite extensions of fields. Then*

$$[K : F] = [K : M][M : F].$$

Main idea of the proof. Let $\varepsilon_1, \ldots, \varepsilon_n$ be a basis of M as a vector space over F and let $\eta_1, \ldots, \eta_m$ be a basis of K over M. The main step is to prove that $\{\varepsilon_i\eta_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis of K over F.

$$\begin{tikzcd}
K \arrow[d, dash] \\
M \arrow[d, dash] \\
F
\end{tikzcd}$$

Corollary 1.3. *If K/F is a finite extension, then there exist algebraic elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ such that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. In other words, a finite extension field is finitely generated.*

Proof. Firstly, if $K \neq F$ we can choose $\alpha_1 \in K \setminus F$ and then $1 < [F(\alpha_1) : F] \leq [K : F]$. If $F(\alpha_1) \neq K$ we can choose $\alpha_2 \in K \setminus F(\alpha_1)$ and then $[F(\alpha_1) : F] < [F(\alpha_1, \alpha_2) : F] \leq [K : F]$. If $F(\alpha_1, \alpha_2) \neq K$, we can choose α_n in the same way. This process will terminate, since $[K : F]$ is finite. That is, we can choose $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ to achieve $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. □

Corollary 1.4. *Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ be algebraic elements over F. Then*

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F].$$

Proof. For $n = 2$, we have $[F(\alpha_1, \alpha_2) : F] = [F(\alpha_1, \alpha_2) : F(\alpha_1)][F(\alpha_1) : F]$. Taking $M = F(\alpha_1)$ in Corollary 1.1, we get $[F(\alpha_1, \alpha_2) : F(\alpha_1)] = [F(\alpha_1)(\alpha_2) : F(\alpha_1)] \leq [F(\alpha_2) : F]$. Thus

$$[F(\alpha_1, \alpha_2) : F] \leq [F(\alpha_1) : F][F(\alpha_2) : F].$$

$$\begin{tikzcd}
 & F(\alpha_1, \alpha_2) & \\
F(\alpha_1) \arrow[ur, dash] & & F(\alpha_2) \arrow[ul, dash] \\
 & F \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

Inductively, we can prove the general case. □

If $\alpha, \beta \in K$ are algebraic over F, then $F(\alpha, \beta)/F$ is a finite extension by the above results. Hence every element in $F(\alpha, \beta)/F$ is algebraic over F. In particular, we have

Corollary 1.5. *Let K/F be an extension of fields. If $\alpha, \beta \in K$ are algebraic over F and $\beta \neq 0$, then $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ are also algebraic over F.*

Definition 1.2. *Let K/F be a field extension. If every element of K is algebraic over F, then K/F is called* **algebraic extension** (代数扩张)*. Otherwise, K/F is called* **transcendental** (超越扩张)*.*

Theorem 1.4. *1. A finite extension is algebraic.*

2. If K/M and M/F are algebraic extension, then K/F is also an algebraic extension.

Proof. 1. Let K/F be a finite extension. For every $\alpha \in K$, $[F(\alpha) : F] \leq [K : F]$. It follows that $[F(\alpha) : F]$ is finite. Hence α is algebraic by Theorem 1.2. So K/F is algebraic.

2. Let $\alpha \in K$ and let $m(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be the minimal polynomial of α over M. Then $F(\alpha) \subseteq F(a_0, \ldots, a_{n-1}, \alpha)$ and

$$\begin{aligned}[F(a_0, \ldots, a_{n-1}, \alpha) : F] &= [F(a_0, \ldots, a_{n-1})(\alpha) : F(a_0, \ldots, a_{n-1})][F(a_0, \ldots, a_{n-1}) : F] \\ &\leq n \prod_{i=0}^{n-1} [F(a_i) : F] \\ &< \infty.\end{aligned}$$

It follows that $[F(\alpha) : F] < \infty$, hence α is algebraic over F.

□

Corollary 1.5 shows that all algebraic elements in K form an intermediate field of K/F. This intermediate field is called the **algebraic closure** of F in K (F 在K 中的代数闭包). *The algebraic closure of F in K is always an algebraic extension over F.*

Remark 1.2. But an algebraic extension is not necessarily finite. For example, let K be the set of all algebraic numbers. Then K is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and $K/\mathbb{Q}$ is an algebraic extension, while it's not a finite extension.

Exercises

1. What's the difference between algebraic extensions and finite extensions?
2. Let K_1, K_2 be two intermediate subextensions of K/F and $[K_i : F] < \infty$, $i = 1, 2$.
   (a) Show that
   $$[K_1K_2 : F] \leq [K_1 : F][K_2 : F].$$
   (b) If $[K_1 : F]$ and $[K_2 : F]$ are relatively prime, then $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.
   (c) If $K_1 \cap K_2 = F$, is it true that $[K_1K_2 : F] = [K_1 : F][K_2 : F]$?
3. Let K/F be a finite extension. Show that K is the algebraic closure of F in K.
4. Describe the algebraic closure of $\mathbb{Q}$ in $\mathbb{R}$.
5. Let $\overline{\mathbb{Q}}$ denote the set of all algebraic numbers.

(a) For every $\alpha \in \mathbb{C}\backslash\overline{\mathbb{Q}}$, show that α is transcendental over $\mathbb{Q}$.

(b) Show that $\overline{\mathbb{Q}}/\mathbb{Q}$ is an infinite extension.

(c) Let $\alpha \in \mathbb{C}$ be a root of a polynomial $f(x) \in \overline{\mathbb{Q}}[x]$. Show that α is an algebraic number. Deduce that $\overline{\mathbb{Q}}$ is algebraically closed.

(d) Show that $\overline{\mathbb{Q}}$ is the algebraically closure of $\mathbb{Q}$ in $\mathbb{C}$.

(e) Let F be an intermediated field of $\overline{\mathbb{Q}}/\mathbb{Q}$ such that $[F : \mathbb{Q}]$ is finite. Show that $\overline{\mathbb{Q}}$ is also an algebraic closure of F in $\mathbb{C}$.

2 Lecture 19 (Nov 9, 2023): Construction Using Straightedge and Compasses

Compass and straightedge or ruler-and-compasses construction is the construction of lengths or angles using only an idealized ruler and compass.

The ruler to be used is assumed to be infinite in length, has no markings on it and only one edge, and is known as a straightedge (直尺, 平尺). The compasses is assumed to collapse when lifted from the page, so may not be directly used to transfer distances. In other words, a compasses can not leave the plane simultaneously (This is an unimportant restriction, as this may be achieved indirectly, see Corollary 2.2).

Every point constructible using straightedge and compasses may be constructed using compasses alone. A number of ancient problems in plane geometry impose this restriction.

The Greeks showed how to perform some geometric constructions, such as bisecting angles or dividing segments into any number of equal parts, using just a compasses and straightedge under certain constraints (for example, the two legs of a compasses can not leave the plane simultaneously). There are some constructions that aren't possible in this setting: duplicating the cube (constructing a length whose cube is twice the cube of a given length), trisecting an angle, and squaring a circle. The impossibility of these constructions can be deduced fairly easy using the theory of field extensions.

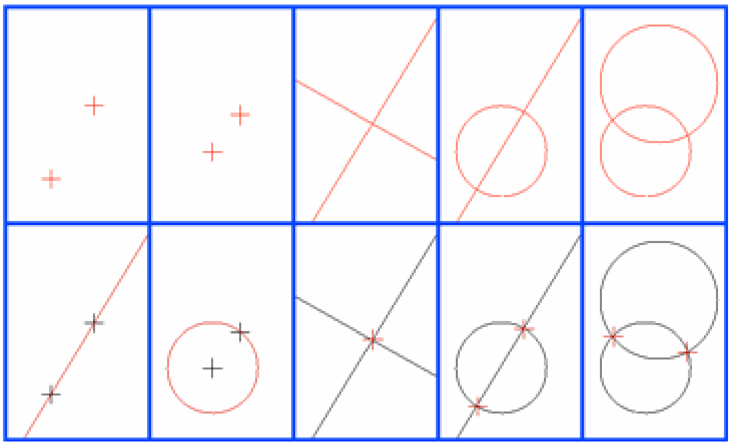
Clearly we can use straightedge and compasses alone to draw

- a line adjoining two points;
- a circle with a given center and radius;
- the intersection point of two lines;
- the intersection points of a line and a circle;
- the intersection points of two circles.

Definition 2.1. *Let P_0 and P_1 be the points of the Euclidean plane given by $P_0 = (0, 0)$ and $P_1 = (1, 0)$. We say that a point P on the plane is* **constructible using straightedge and compasses alone** (可用直尺和圆规作出) *if there exists a sequence of points $P_0, P_1, \ldots, P_n$ such that $P_n = P$ and each P_j $(j \geq 2)$ is one of the following:*

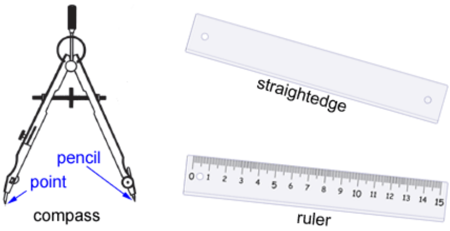
1. *the intersection of two distinct straight lines, each passing through at least two points belonging to the set $\{P_0, P_1, \ldots, P_{j-1}\}$;*

2. *the point of intersection of two distinct circles, where each circle is centred on a point of the set $\{P_0, P_1, \ldots, P_{j-1}\}$ and passes through another point of the set;*



The basic constructions

3. *the point at which a straight line joining two points belonging to the set $\{P_0, P_1, \ldots, P_{j-1}\}$ intersects a circle which is centred on a point of this set and passes through another point of the set.*



Lemma 2.1. *We can use straightedge and compasses alone to draw*

1. *the midpoint of any line segment;*
2. *a line passing through a given point and perpendicular to a given line;*
3. *a line parallel to a given line from a given point outside the given line.*

Proof. 1. Let P and Q be constructible points in the plane. Let S and T be the points where the circle centred on P and passing through Q intersects the circle centred on Q and passing through P. Then S and T are constructible points in the plane, and the point R at which the line ST intersects the line PQ is the midpoint of the line segment PQ. Thus this midpoint is a constructible point.

2. Let A be a point lying outside of a line ℓ. Let B, C be the intersection points of ℓ with a circle centred on A and with sufficient lengthy radius. The two circles centred at B, C and with radius AB will intersect at another point D. Then the line AD will be perpendicular to ℓ.

   If A is on the line ℓ, the perpendicular line can be constructed in a similar way.

3. Let A be a point lying outside of a line ℓ. We can first construct the line ℓ_1 passing through A and perpendicular to ℓ. Secondly construct the line ℓ_2 passing through A and perpendicular to ℓ_1. Then ℓ_2 is the line parallel to ℓ.

□

Corollary 2.1. *If any three vertices of a parallelogram in the plane are constructible, then so is the fourth vertex.*

Proof. Let the vertices of the parallelogram listed in anticlockwise (or in clockwise) order be A, B, C and D, where A, B and D are constructible points. We must show that C is also constructible.

By Lemma 2.1, we first construct the line ℓ_1 which passes B and is parallel to the line AD. Then construct the line ℓ_2 which passes D and is parallel to the line AB. Now C is the intersection point of two lines ℓ_1 and ℓ_2. □

Definition 2.2. *A real numbers x is said to be* **constructible by using straightedge and compasses alone** (可用直尺和圆规作出的数) *if the point $(x, 0)$ is constructible using straightedge and compasses alone.*

$$\boxed{\text{A point } (x,y) \text{ is constructible} \iff x \text{ and } y \text{ are constructible}}$$

In virtue of Lemma 2.1, we can bisect an angle and all rational number are constructible (why?). Consequently the square roots of a positive rational number is also constructible (how?). More precisely, if we accept the number 0 and 1,

- all rational numbers are constructible using straightedge and compasses alone.

It seems that the positive rational numbers are the most natural object in our real world.

Notice that the two legs of a compasses can not leave the plane simultaneously. But we have

Corollary 2.2. *The distance can be summed up. In particular, the distance can be transferred.*

Proof. Let $AB = x, CD = y$. We show that a segment with length $x + y$ is constructible.

Assume $B \neq C$. We first construct a line ℓ_1 which passes through C and is parallel to the line AB. Let E be the right-hand intersection point of the line ℓ_1 and the circle centred on C with radius $CD = y$. We have $CE = y$. Construct the line ℓ_2 which passes through E and is parallel to the line BC. Let F be the intersection point of ℓ_2 and the line AB. Then $AF = x + y$.

If $B = C$, the $x + y$ is achieved by drawing a circle centred on C with radius $CD = y$. □

Theorem 2.1. *Let $(x, y) \in \mathbb{R}^2$ be a constructible point of the Euclidean plane. Then $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r$ for some non-negative integer r.*

Proof. Let $P = (x, y)$ and let $P_0, P_1, \ldots, P_n$ be a finite sequence of points of the plane with the properties listed above. Let $P_j = (x_j, y_j) \in \mathbb{R}^2$ and set $K_0 = K_1 = \mathbb{Q}$ and $K_j = K_{j-1}(x_j, y_j)$ inductively for $j = 2, 3, \ldots, n$. Straightforward coordinate geometry shows that, for each j, the real numbers x_j and y_j are both roots of linear or quadratic polynomials with coefficients in K_{j-1}. It follows that $[K_{j-1}(x_j) : K_{j-1}] = 1$ or 2 and $[K_{j-1}(x_j, y_j) : K_{j-1}(x_j)] = 1$ or 2 for each j. It follows from the Tower Law (Transitivity of Extension Degree) that $[K_n : \mathbb{Q}] = 2^s$ for some non-negative integer s. But $[K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(x, y)][\mathbb{Q}(x, y) : \mathbb{Q}]$. We deduce that $[\mathbb{Q}(x, y) : \mathbb{Q}]$ divides 2^s, and therefore $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r$ for some non-negative integer r. □

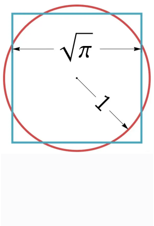
Corollary 2.3. *If $x \in \mathbb{R}$ is constructible, then $[\mathbb{Q}(x) : \mathbb{Q}]$ is a power of 2.*

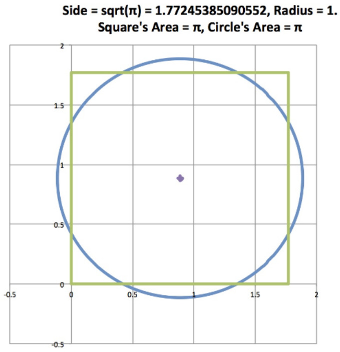
The problem "doubling the cube" owes its name to a story concerning the citizens of Delos, who consulted the oracle at Delphi in order to learn how to defeat a plague sent by Apollo. According to Plutarch, it was the citizens of Delos who consulted the oracle at Delphi, seeking a solution for their internal political problems at the time, which had intensified relationships among the citizens. The oracle responded that they must double the size of the altar to Apollo, which was a regular cube. The answer seemed strange to the Delians and they consulted Plato, who was able to interpret the oracle as the mathematical problem of doubling the volume of a given cube, thus explaining the oracle as the advice of Apollo for the citizens of Delos to occupy themselves with the study of geometry and mathematics in order to calm down their passions.

According to Plutarch, Plato gave the problem to Eudoxus and Archytas and Menaechmus, who solved the problem using mechanical means, earning a rebuke from Plato for not solving the problem using pure geometry. This may be why the problem is referred to in the 350s BC by the author of the pseudo-Platonic Sisyphus as still unsolved. However another version of the story says that all three found solutions were too abstract to be of practical value.

A significant development in finding a solution to the problem was the discovery by Hippocrates of Chios that it is equivalent to finding two mean proportionals between a line segment and another with twice the length. In modern notation, this means that given segments of lengths a and $2a$, the duplication of the cube is equivalent to finding segments of lengths r and s so that $\frac{a}{r} = \frac{r}{s} = \frac{s}{2a}$. In turn, this means that $r = a \cdot \sqrt[3]{2}$. But Pierre Wantzel proved in 1837 that the cube root of 2 is not constructible; that is, it cannot be constructed with straightedge and compass.

Example 2.1 (Squaring the circle, 化圆为方)**.** We know that π is not algebraic over the field $\mathbb{Q}$ of rational numbers. Therefore $\sqrt{\pi}$ is not algebraic over $\mathbb{Q}$. It then follows from Theorem 2.3 it is not possible to give a geometrical construction for obtaining a square with the same area as a given circle, using straightedge and compasses alone. Thus it is not possible to "square the circle" using straightedge and compasses alone.





Example 2.2 (Doubling the cube, 倍立方)**.** We know that $\sqrt{2}$ is constructible. It is not difficult to see that if it were possible to construct two points in the plane with distance $\sqrt[3]{2}$ apart, then the point $(\sqrt[3]{2}, 0)$ would be constructible. But it follows from Theorem 2.3 that this is impossible, since $\sqrt[3]{2}$ is a root of the irreducible monic polynomial $x^3 - 2$, and therefore $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. We conclude that there is no geometric construction using straightedge and compasses alone that will construct from a line segment in the plane a second line segment such that a cube with the second line segment as an edge will have twice the volume of a cube with the first line segment as an edge.

Example 2.3 (Trisecting the angle, 三等分角)**.** We show that there is no geometrical construction for the trisection of an angle of $\frac{\pi}{3}$ radians (i.e, 60°) using straightedge and compasses alone.

Note that if a angle θ is constructible, then $\sin\theta$ and $\cos\theta$ are also constructible (why?). Assume an angle of $\frac{\pi}{3}$ radians could be trisected using straightedge and compasses alone. Then $a = \cos\frac{\pi}{9}$ and $b = \sin\frac{\pi}{9}$ are constructible. Consequently the point (a, b) would be constructible. Now

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$$

for any angle θ. On setting $\theta = \frac{\pi}{9}$ we deduce that $4a^3 - 3a = \frac{1}{2}$ or $8a^3 - 6a - 1 = 0$. Thus $a = \cos\frac{\pi}{9}$ is a root to the polynomial

$$f(x) = 8x^3 - 6x - 1.$$

Now put $g(x) = f(x + \frac{1}{2})$. An easy computation shows that $g(x) = 8x^3 + 12x^2 - 3$. An immediate application of Eisenstein's criterion for irreducibility shows that the polynomial $g(x)$ is irreducible over $\mathbb{Q}$, and so is $f(x)$ (one can prove the irreducibliity of $f(x)$ directly by considering the possible rational roots). Thus $f(x) = 8x^3 - 6x - 1$ is the minimal polynomial of $a = \cos\frac{\pi}{9}$ and so $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. It now follows from Theorem 2.3 that the point $(\cos\frac{\pi}{9}, \sin\frac{\pi}{9})$ is not constructible using straightedge and compasses alone. Therefore it is not possible to trisect an angle of $\frac{\pi}{3}$ radians using straightedge and compasses alone. Consequently there is no geometrical construction for the trisection of an arbitrary angle using straightedge and compasses alone.

It's impossible to trisect an arbitrary angle, double the cube or square the circle by using straightedge and compasses alone.
古希腊三大问题: 倍立方, 三等分任意角和化圆为方, 在尺规作图背景下均不可解.

Which of the real numbers are constructible by using straightedge and compasses alone? We already know that all rational numbers are constructible. A real number like $\sqrt{2}, \sqrt{3}$ is also constructible. We will see that all constructible real numbers form a subfield of $\mathbb{R}$.

Theorem 2.2. *Let K denote the set of all constructible real numbers by using straightedge and compasses alone. Then*

(1) K is a subfield of $\mathbb{R}$ which contains $\mathbb{Q}$. And

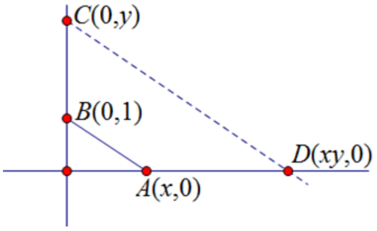
(2) if $x \in K$ and $x > 0$ then $\sqrt{x} \in K$.

Proof. By Lemma 2.1, a point (x, y) is constructible using straightedge and compasses alone if and only if $x \in K$ and $y \in K$.

Clearly $0 \in K$ and $1 \in K$. Let x and y be real numbers belonging to K.

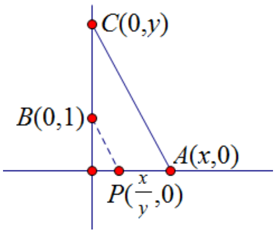
Notice that the point $A(x, 0)$ is constructible. The circle centred on the origin and passing through $(x, 0)$ intersects the x-axis at $(-x, 0)$. Thus $(-x, 0)$ is a constructible point, and thus $-x$ belongs to K. It follows $x - y \in K$, by Corollary 2.2.

Let x and y be real numbers belonging to K and $y \neq 1$. Then the points $A(x, 0)$, $B(0, 1)$ and $C(0, y)$ are constructible. By Lemma 2.1, we can construct the line ℓ_1 passing through C and parallel to the line AB. Let D be the intersection of ℓ_1 and the x-axis. Then the coordinate of D is $(xy, 0)$. This means that the point $(xy, 0)$ is constructible, and thus $xy \in K$.



Similarly, if $y \neq 0$, we set P to be the intersection point of x-axis and the line ℓ_2 passing through B and parallel to the line AC. Then $P = (\frac{x}{y}, 0)$. It follows $\dfrac{x}{y} \in K$.

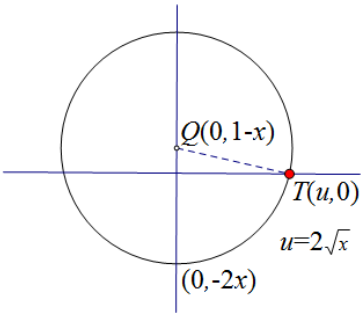
The above results show that K is a subfield of $\mathbb{R}$.



Suppose $x \in K$ and $x > 0$. Then $1-x, 1+x \in K$ and $Q(0, 1-x)$ is a constructible point. Notice that $|1-x| < 1+x$. Thus the circle centred on Q with radius $1+x$ intersects the x-axis at a point $T(u, 0)$ with $u > 0$. Therefore

$$u^2 = (1+x)^2 - (1-x)^2 = 4x,$$

by Pythagoras' Theorem. It follows $u = 2\sqrt{x}$. Thus $2\sqrt{x} \in K$ and hence $\sqrt{x} = \frac{2\sqrt{x}}{2} \in K$, as required.



□

能尺规作出的数恰好是从 0, 1 出发, 通过有限次的加、减、乘、除和开方运算而得到的数.

Remark 2.1. If x, y are constructible and $y \neq 0$, there are many ways to construct xy and $\frac{x}{y}$.

The above theorems can be applied to the problem of determining *whether or not it is possible to construct a regular n-sided polygon with a straightedge and compasses, given its center and one of its vertices.* The impossibility of trisecting an angle of 60° shows that a regular 18-sided polygon is not constructible using straightedge and compasses alone.

Now if one can construct a regular n-sided polygon then one can easily construct a regular $2n$-sided polygon by bisecting the angles of the n-sided polygon. Thus the problem reduces to that of determining which regular polygons with an odd number of sides are constructible. Moreover it is not difficult to reduce down to the case where n is a power of some odd prime number:

> *Let $n = 2^s p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ be prime decomposition, where $p_1, p_2, \ldots, p_t$ are distinct odd primes. Then a regular n-sided polygon is constructible if and only if every $p_i^{e_i}$-sided polygon is constructible.*

It is not difficult to see that the geometric problem of constructing a regular n-sided polygon using straightedge and compasses is equivalent to the algebraic problem of finding a formula to *express the n-th roots of unity in the complex plane in terms of integers or rational numbers by means of algebraic formulae which involve finite addition, subtraction, multiplication, division and the successive extraction of square roots.* Thus the problem is closely related to that of expressing the roots of a given polynomial in terms of its coefficients by means of algebraic formulae which involve only finite addition, subtraction, multiplication, division and the successive extraction of p-th roots for appropriate prime numbers p. This is exactly the "radical solution" problem (根式求解问题), which can be solved by the Galois theory.

In fact, techniques of Galois Theory show that

> a regular n-sided polygon is constructible using straightedge and compasses if and only if $n = 2^s p_1 p_2 \cdots p_t$, where $p_1, p_2, \dots, p_t$ are distinct Fermat primes.
> 只有正 $2^s p_1 p_2 \cdots p_t$ 边形才可用尺规作出, 其中 $p_1, p_2, \dots, p_t$ 为不同的费马素数.

Remark 2.2.

1. Gauss discovered that a regular 17-sided polygon was constructible in 1796, when he was 19 years old.

2. A *Fermat prime* is a prime number that is of the form $2^k + 1$ for some integer k. If $k = uv$, where u and v are positive integers and v is odd, then $2^k + 1 = w^v + 1 = (w+1)(w^{v-1} - w^{v-2} + \cdots - w + 1)$, where $w = 2^u$, and hence $2^k + 1$ is not prime. Thus any Fermat prime is of the form $2^{2^n} + 1$ for some non-negative integer n. Denote $F_n = 2^{2^n} + 1$. Fermat observed in 1640 that F_n is prime when $n \leq 4$. These Fermat primes have the values $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ and $F_4 = 65537$. Fermat conjectured that all the numbers F_m were prime. As of 2020, the only known Fermat primes are F_0, F_1, F_2, F_3, and F_4. If there are any more, they have at least two billion decimal digits. Moreover, $F_5 = 641 \times 6700417$, $F_{16} = 2^{65536} + 1 = 825753601 \times 188981757975021318420037633 \approx 10^{20000}$ (Brent in 1996). It is known that F_n is composite for $5 \leq n \leq 32$, although amongst these, complete factorizations of F_n are known only for $0 \leq n \leq 11$, and there are no known prime factors for $n = 20$ and $n = 24$. The largest Fermat number known to be composite is $F_{3329780}$, and its prime factor $193 \times 2^{3329782} + 1$, a megaprime, was discovered in July 2014. In fact, until January 14, 2017, only F_0 to F_{11} have been completely factored, and 336 prime factors of Fermat numbers are known, and 292 Fermat numbers are known to be composite. On Aug 12th, 2021, Erwin Doescher discovered that $749893 \times 2^{66648} + 1$ is a factor of F_{66643}. For more information, see http://www.fermatsearch.org/news.html

3. The five Fermat primes 3, 5, 17, 257 and 65537 provide only 31 constructible regular polygons with an odd number of sides.

Exercises

1. Show that a point $P(a, b)$ in the plane is constructible if and only if the real numbers a and b are constructible.

2. Show that it's possible to bisect an angle using straightedge and compasses alone.

3. Show that a line can be constructed to pass through a given point and perpendicular to a given line, by using straightedge and compasses alone.

4. Show that a line can be constructed to pass through a given point and parallel to a given line, by using straightedge and compasses alone.

5. Show that a angle of $\frac{\pi}{3}$ radians is constructible using straightedge and compasses alone.

6. Show that if $(a, 0)$ and $(b, 0) \in \mathbb{R}^2$ are constructible using straightedge and compasses alone, where $b \neq 0$, so are the points $(a \pm b, 0), (b^{-1}, 0)(ab, 0)$ and $(ab^{-1}, 0)$.

7. Show that if $(a, 0)$ is constructible using straightedge and compasses alone, where $a \geq 0$, so is the point $(\sqrt{a}, 0)$.

8. Show that it's impossible to construct a cube with quintuple the volume of a given cube using straightedge and compasses alone.

9. Write out the steps to construct $\frac{3}{5}$ by using straightedge and compasses alone.

10. Write out the steps to construct $\sqrt{15}$ by starting with 0 and 1 with the help of straightedge and compasses alone.

11. Write out the steps to construct $\sqrt{2023}$ by starting with 0 and 1 with the help of straightedge and compasses alone.

12. Assume an angle $\theta \neq \frac{\pi}{2}$ is constructible using straightedge and compasses alone. Show that $\tan\theta$ is also constructible using straightedge and compasses alone.

13. Construct a regular 5-sided polygon by using straightedge and compasses alone.

14. Show that the subfield K in Theorem 2.2 is an infinite algebraic extension of $\mathbb{Q}$.

15. Let $F/\mathbb{Q}$ be a finite subextension of $K/\mathbb{Q}$, where K is the subfield in Theorem 2.2. Show that $[F : \mathbb{Q}]$ is a power of 2.

Homework Exercise 1, 2, 4, 5, 8 on page 242.