The Root of Algebraic Extensions (2006)

1. Constructions of numbers

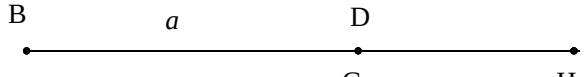
Four operations and extraction of square root

Renè Descartes (1596~1650) wrote the Discourse on Method, whose separate volume, the Geometry is not known well in Japan. He defined four or five operations of segments, addition, subtraction, multiplication, division, and extraction of root and showed that all of the results of operations are acceptable as segments in geometry as follows.

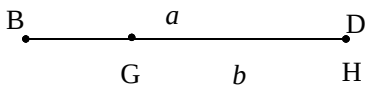
Remark. We are to use the compass and the straight edge implements to draw figures in geometry from classical Greek times.

1) Addition and subtraction of segment

We can construct addition and subtraction as follows.



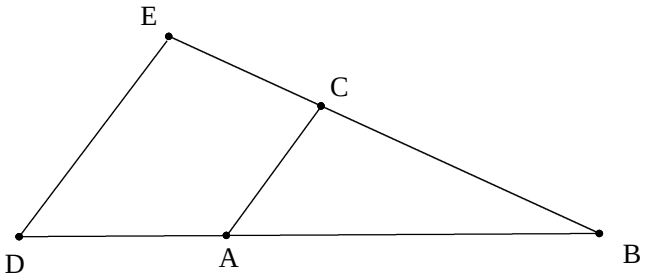
$a + b = BH$



$a - b = BG \quad (a > b)$

1) Multiplication and division of segment

Let $AB = e$ (*unit*), $DB = a$ on the given straight line, and $BC = b$, $BE = c$ on the straight line through the point B. Draw a straight line BC from the point B.



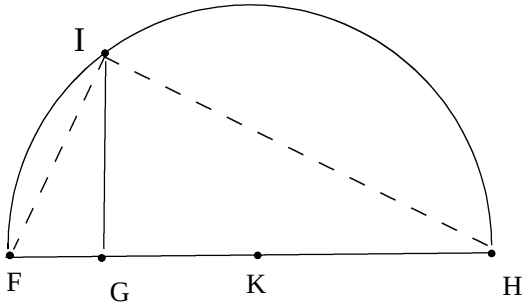
$\triangle ABC \backsim \triangle DBE$

$\therefore$ CB : BE = AB : DB

$\therefore$ $BE = a \times b$, $CB = \dfrac{c}{a}$

2) Extraction of square root

Let $FG = e$ (*unit*), $GH = a$ on the given straight line and K is the mid point of FH.



Draw a circle with the center K and the radius FH, and from the point I, draw a straight line at right angles to FH.

$\triangle FGI \backsim \triangle IGH$

$\therefore$ FG : GI = GI : GH

$\therefore$ $GI = \sqrt{a}$

In this way, using the implements, we are able to construct the numbers which are made by four operations and extraction.

2. Algebraic numbers and algebraic extensions

As I mentioned before, we are to use the straight edge and compass on the occasion of construction in geometry. Setting those restrictions, ancient Greeks were confronted with the following difficulties.

(1) It is impossible to divide an angle into three equal parts, with straight edge and compass alone. (Trisection of the angle)

(2) It is impossible to construct a cube whose volume is equal to double volume of a given cube. (Duplication of the cube)

(3) It is impossible to construct a square whose area is equal to that of a given circle. (Quadrature of the circle)

Setting such restrictions, and solving those difficulties, we have been developing mathematics.

1) Ruler-Compass Constructions

We interpret the construction as follows.

A point set S is given on the plane and to repeat the following operations finitely.

(1) Draw a line passing through different two points on a plane.

(2) Draw a circle centered at a fixed point on a plane with a given radius.

(3) Add an intersection of the two straight lines to a point set S.

(4) Add intersection of a straight line and a circle to a point set S.

(5) Add intersection of two circles to a point set S.

In the case of (3), we are able to get the intersection of the straight lines AB, CD from the coordinates of four points A, B, C, and D by four operations.

In the case (4), we are able to get the intersection of the straight line AB and a circle P from the coordinates of A, B, the center and radius of the circle P by four operations.

In the case of (5), we are able to reduce (4) by subtracting both sides to the circles' equations.

Repeating construction finitely, we have gotten a new real number, and have verified the number and it's operations by the construction. However, from the stage of the acknowledgement of the complex number, we understood the need to verify them by solving algebraic equation. So we may define the constructible number as follows.

Definition. Let $f(x)$ be a polynomial with rational coefficients $a_1, a_2, a_3, \cdots, a_n$.

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$$

We call any root of $f(x)$ an algebraic number.

Remark. Constructible numbers are algebraic numbers but the opposite is not true for example $\sqrt[3]{a}$.

Theorem. If a, b are algebraic numbers, then $a + b$, $a-b$, ab, $\frac{a}{b}$ $(b \neq 0)$ are algebraic numbers.

Proof. The polynomials $f(x)$, $g(x)$ over Q (the rational numbers), and the roots are a, b respectively.

$f(x) = x^n + p_1 x^{n-1} + \cdots + p_{n-1}x + p_n$, $g(x) = x^m + q_1 x^{m-1} + \cdots + q_{m-1} x + q_m$

Because a *and* b are algebraic numbers. $f(a) = 0$, $f(b) = 0$

$\therefore a^n = -(p_1 a^{n-1} + \cdots + p_{n-1} a + p_n)$, $b^m = -(q_1 b^{m-1} + \cdots + q_{m-1} b + q_m)$

$a^{-1} = -p_n^{-1}(a^{n-1} + p_1 a^{n-2} + \cdots + p_{n-1})$

$a^{n+1} = -(p_1 a^{n-1} + \cdots + p_{n-1} a + p_n)a = -\{p_1(-(p_1 a^{n-1} + \cdots + p_{n-1} a + p_n)) + \cdots + p_n a\}$

$b^{-1} = -q_m^{-1}(b^{m-1} + q_1 b^{m-2} + \cdots + q_{m-1})$

$b^{m+1} = -\{q_1(b^{m-1} + \cdots + q_{m-1} b + q_m) b\} = -\{q_1(-(q_1 b^{m-1} + \cdots + q_{m-1} b + q_m)) + \cdots + q_m b\}$

a^p, b^q, $a^i b^j$ are linear combinations of a^k, b^h, *and* $a^k b^h$
$(k = 0, 1, 2, \cdots, n\text{-}1 \quad h = 0, 1, 2, \cdots, m\text{-}1)$.

The extension field $Q(a, b)$ is an n + m + nm dimensional linear space.

$\therefore a + b, a-b, ab, a/b \in Q(a, b)$

2) Algebraic extensions and Construction in Geometry

As we studied before, constructing with ruler and compass means to get new real numbers from the given real numbers by operating algebraic operations finitely.

Here, I would like to get back to the classical Greek problems.

Definition. If F is a subfield of a field K, we say that E is a field extension of F, and one writes E / F.

Definition. The dimension of K viewed as a linear space over F is called the degree of K over F and it is denoted by $[K : F]$.

Theorem.

If we set the number u of the new figure which is constructed with ruler and compass from the old figure whose number is

$[K(u) : K] = 2^p$ (p : Positive integer)

where $K = Q(a_1, a_2, \cdots, a_n)$.

Proof. $K(u) \subset K(u_1, u_2, u_3, \cdots, u_m)$

$u_1^2 \in K$, $u_i^2 \in K(u_1, u_2, u_3, \cdots, u_{i-1})$

$\therefore [K(u_1, u_2, u_3, \cdots, u_i) : K(u_1, u_2, u_3, \cdots, u_{i-1})] = 1$ *or* 2

$[K(u) : K] = [K(u) : K(u_1)] \times [K(u_1) : K(u_1, u_2)] \times \cdots \times [K(u_1, u_2 \cdots) : K]$

$\therefore [K(u) : K] = 2^p$ (p : positive integer)

The classical Greek problems (1), (2), and (3) are explained as follows.

(1) It is impossible to trisect an angle

To trisect an angle is equal to find the value of $\cos h$ after giving an equation $a = \cos 3h$.

Using $\cos 3h = 4\cos^3 h - 3\cos h$, setting $2\cos h = u$, we find

$$u^3 - 3u - 2a = 0$$

Let $h = 20^\circ$ *then* $a = \frac{1}{2}$.

$\therefore u^3 - 3u - 1 = 0$, Q : irreducible

$\therefore [Q(u) : Q] = 3$ then u is of impossible construction.

Remark. This problem was proved by P. L. Wantzel in 1837. [8)]

(2) It is impossible to duplicate a cube

Duplication of the cube is equal to find an equation $u^3 - 2 = 0$ after giving a value of a side of a cube.

Setting $a = 1$, then $u^3 - 2 = 0$, Q : irreducible

$\therefore [Q(u) : Q] = 3$ Therefor u is of impossible construction.

(3) It is impossible to construct a square of area equal to a circle

This problem was solved in 1882 after F. Lindeman's discovery that is π not an algebraic number. [2)]

3. Radical extensions and Cyclic groups

Let the equation of degree n with coefficients, $s_1, s_2, s_3, \cdots, s_n$, and having roots, $x_1, x_2, x_3, \cdots, x_n$;

$$x^n + s_1 x^{n-1} + s_2 x^{n-2} + \cdots + s_n = 0 \quad \cdots\cdots\cdots\cdots\cdots\cdots (*)$$

Consequently, we find

$$x_1 + x_2 + x_3 + \cdots x_n = -s_1$$

$$x_1x_2 + x_1x_3 + x_1x_4 + \cdots + x_{n-1}x_n = s_2$$

$$\cdots$$

$$x_1x_2x_3 \cdots x_n = (-1)^n s_n$$

When we solve the equation, we manipulate coefficients of the equation by algebraic operations. Therefore, in order to solve the equation, we have to extend the field of rational numbers, as follows.

(1) Radical extensions

Let F be a radical number field, there is a radical tower,

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n$$

having the property that there exists prime and p_i elements such that $a_i \in F_i$, *and* $\sqrt[p_i]{a_i} \notin F_i$

$$F_{i+1} = F_i(\sqrt[p_i]{a_i})$$

Remark. Radical extensions are cyclic extensions.

Theorem. Let F be a field and let $p(x)$ be a polynomial with coefficients in F and K be a whole of the cosets for the modulus $p(x)$,

$$K = F[x] / p(x)$$

(2) The roots of $p(x)$ are the elements of K, if the coset of x be a, we find that a is a root of $p(x)$.

Proof. Let $a = x \pmod{p(x)}$

$$p(a) = p(x) \pmod{p(x)} = 0$$

$\therefore$ a is a root of $p(x)$

$\therefore$ $p(x) = (x-a)p_1(x)$ where $p_1(x)$ is a irreducible polynomial.

Remark. In fact, when $p(x) = (x-a)p_1(x)$, if x is divided by $p(x)$, we easily find that the residue is a root of $p(x)$.

$$\begin{array}{r} 1/p_1(x) \\ \hline p(x) \;)\; x \\ \quad x-a \\ \hline \qquad a \end{array}$$

$F_1 = F[x] / p_1(x)$

Let $a_1 = x \pmod{p_1(x)}$,

$p(x) = (x-a)(x-a_1)p_2(x)$ where $p_2(x)$ is an irreducible polynomial.

By repeating division similarly, we find the following theorem.

Theorem. Let F be a field, and let K be an extension of F. Let be an $p(x)$ irreducible polynomial over F. Then have a $p(x)$ factorization in K into factors of degree 1, that is

$$p(x) = (x-a)(x-a_1)(x-a_2)\cdots(x-a_n)$$

$$a,\ a_1,\ a_2,\ \cdots,\ a_n \in K$$

Definition. Let the polynomial $p(x)$ with coefficients over F has a factorization into linear factors. Then we call K splitting field of $p(x)$.

4. Normal Subgroup

1) Residue Class

Theorem. Let G be a group and let H be a subgroup of G. G is decomposed as follows.

$$G = a_1H \cup a_2H \cup a_3H \cup \cdots \cup a_nH$$

Proof. In the case of $aH \cap bH \neq \varnothing$

There is an element x such that $x \in aH \cap bH$

We can write x as follows.

$$x = ah_1 = bh_2 \ (\ h_1,\ h_2 \in H\ )$$

$$a = b\ h_2\ h_1^{-1} \ (\ h_1,\ h_2 \in H\ )$$

$$\therefore\ aH = bH$$

$$\therefore\ aH \cap bH = \varnothing \ or\ aH = bH$$

We denote this coset decomposition as follows.

$$G = a_1H + a_2H + \cdots + a_nH$$

2) Normal Subgroup

Definition. Let H be a subgroup of G.

If H satisfies the following conditions: For all we $x \in G$, have $gHg^{-1} = H$.

We say that H is a normal subgroup of G.

Remark. If G is commutative, then all of the subgroup of G is normal subgroup.

3) Quotient Groups

Theorem. If H is a normal subgroup of G, then is $\{a_1H,\ a_2H,\ a_3H,\ \cdots,\ a_nH\}$ a group.

Proof. $(gH)(g'H) = gg'\ H$

$(eH)(gH) = gH$

$\therefore$ $eH = H$ (unit element)

$(gH)(g^{-1}H) = H$

$\therefore$ $(gH)^{-1} = g^{-1}H$ (inverse element)

Definition. We call this group a quotient group and write G / H.

4) Automorphism Groups

In order to solve equations, we need an idea of automorphism groups because algebraic numbers are invariable by permutations.

Definition. Let F be a ground field and let the extension of F;

$$F \subset E \subset K$$

We call E intermediate field of F and K.

Definition.

Let s be an isomorphism of E, whole the isomorphism of E, H consists a group. We call H a fixed group of E.

$$H = G(E) = \{s \in G \mid s(E) = E\}$$

Remark. Let automorphic groups F, K be G = G(F), I = G(K) respectively.

$$G \supset H \supset I, \quad (I = \{e\})$$

$$\begin{array}{ccc} K(I) = K & \cdots\cdots\cdots\cdots & I = G(K) \\ \cup & & \cap \\ K(H) = E & \cdots\cdots\cdots\cdots & G(E) = H \\ \cup & & \cap \\ K(G) = F & \cdots\cdots\cdots\cdots & G = G(F) \end{array}$$

Theorem. Let Q be a rational number field, all the element of Q are invariable by an automorphism s.

Proof. Let n be a natural number.

$$s(n) = s(1 + 1 + 1 + \cdots + 1)$$
$$= s(1) + s(1) + s(1) + \cdots + s(1)$$
$$= 1 + 1 + 1 + \cdots + 1$$
$$= n$$
$$r = \pm \frac{n}{m} \quad (m, n : \text{natural numbers})$$
$$s(r) = s\left(\pm \frac{n}{m}\right) = \pm \frac{s(n)}{s(m)} = \pm \frac{n}{m} = r$$

Theorem. If a be an algebraic number of K, then is $s(a)$ a conjugate number of a.

Proof. Let $f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n, \quad a_1, a_2, a_3, \cdots, a_n \in K$

$$f(a) = a^n + a_1 a^{n-1} + a_2 a^{n-2} + \cdots + a_n = 0$$
$$s(f(a)) = s(a^n + a_1 a^{n-1} + a_2 a^{n-2} + \cdots + a_n)$$
$$= s(a)^n + a_1 s(a)^{n-1} + \cdots + a_n$$
$$= f(s(a)) = 0$$

$\therefore$ $s(a)$: root of $f(x)$.

5. Galois Extensions

Definition. Let ground field be F and let K be splitting extensions. If the conjugate fields of K over F coincide, we call K Galois extension G of F, and write G = Gal (E / F).

Remark.

In the extension field $K = F(a)$, let conjugate roots of a over F *be* $a = a_1, a_2, a_3, \cdots, a_n$,

$$K = F(a) = F(a_2) = F(a_3) = \cdots = F(a_n)$$

K contains all conjugate roots of a.

(1) Extend the field K as follows.

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_k = K$$

(2) Let the automorphism group be $G(F_i) = H_i$,

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_k = I = \{e\}$$
$$H_i \rhd H_{i+1}$$

Theorem（The Fundamental Theorem of Galois Theory)

Let E / F be a Galois extension with Galois group $G = Gal\ (K / F)$.

E / F: Galois extension $\Leftrightarrow$ $G \triangleright G(E)$

Remark. $Gal\ (E / F) \cong G / G\ (E)$

Proof. ($\rightarrow$) Since E is a Galois extension of F,

For all $s \in G$, $s(E) = E$

For all $s \in sGs^{-1}$,

$s = sgs^{-1} \in sG(E)s^{-1}$ where $g \in G(E)$

For all $c \in E$

$s(c) = s\ g(s^{-1}(c))$

$= s(s^{-1}(c)$ $\because$ $G(E) = E$

$= c$

$\therefore$ $s \in G(E)$

$\therefore$ $sG(E)s^{-1} \subset G(E)$

$\therefore$ $G \triangleright G\,(E)$

($\leftarrow$) Let G(E) be normal subgroup of G

For all $t \in G(E)$, $s^{-1}\ t\ s \in G(E)$

Because we are able to extend the automorphism s of E over F to the automorphism of K, ss

$s^{-1}\ t\ s = c$ where $c \in E$

$\therefore$ $t\ s\ (c) = s\ (c)$

$\therefore$ $s\ (c) \in E$

$\therefore$ $s(c) = s\ (c) \in E$

Therefore E / F is a Galois extension.

Remark. K is a Galois extension of E but it is not necessarily true that E is a Galois extension of F. Only when G(E) is a normal subgroup of G, E is a Galois extension of F.

3) Let $f\ (x)$ be a minimal polynomial of a over F, then K is a splitting field of $f\ (x)$. Because K is a separate extension field, necessary and sufficient condition for G to be solvable is the next conditions.

(1) $H_i \triangleright H_{i+1}$

(2) Order of H_i / H_{i+1} is prime.

References

1. Renè Descartes, The Geometry of Rene Descartes, translated by David Smith and Marcia L. Lathan, Dover, 1954
2. Ian Stewart, Galois Theory, Chapman and Hall, 1972
3. 安部　斉 著　　代数ことはじめ　森北出版　1993
4. 東郷　重明 著　代数入門　　サイエンス社　2001
5. 石田　信 著　　代数学入門　実教出版　1999
6. 草場　公邦 著　ガロワと方程式　朝倉書店　2004
7. 渡辺　敬一, 草場　公邦 著　代数の世界　朝倉書店　2004
8. 松村　英之　著　代数学　朝倉書店　1990