Galois theory

a draft of Lecture Notes of H.M. Khudaverdian.
Manchester, Autumn 2006 (version 16 XII 2006)

Contents

Preliminaries

0.1

Solutions to quadratic equations $x^2 + px + q = 0$ are well known (more than two thousands years...):

$$x_{1,2} = \frac{-p \pm \sqrt{p^2 - 4q}}{2}\,.$$

Every cubic equation $x^3 + ax^2 + bx + c = 0$ can be reduced to the form $x^3 + px + q = 0$ by transformation $x \to x - a/3$.

One can express roots (complex roots) of the equation

$$x^3 + px + q = 0 \tag{1}$$

through radicals using ansatz:

$$x = \sqrt[3]{u} + \sqrt[3]{v}\,.$$

Then

$$x^3 = u + v + 3x\sqrt[3]{u}\sqrt[3]{v}\,.$$

Hence comparing with (1) we see that $\sqrt[3]{u} + \sqrt[3]{v}$ is a root of the equation if

$$u + v = -q \quad \text{and } 3\sqrt[3]{u}\sqrt[3]{v} = -p$$

This is quadratic equation: u, v are roots of quadratic polynomial

$$w^2 + qw - \frac{p^3}{27}$$

and we come to famous Cardano-Tartaglia formula (Tartaglia 1535 year):

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}\,, \tag{2}$$

Remark This formula is not much use for calculations. E.g. consider polynomial $x^3{-}3x{-}18$.The simplest analysis show that it has unique real root and this root is equal to 3. On the other hand the application of Cardano-Tartaglia formula (2) gives

$$x = \sqrt[3]{9 + \sqrt{80}} + \sqrt[3]{9 - \sqrt{80}}$$

To prove that r.h.s. of the formula above is equal to 3 you have to use the fact that equation $x^3 - 3x - 18$ has the solution $x = 3$. Vicious circle???!

Another problem with formula (2): Consider the polynomial:

$$x^3 - 7x + 6 = (x - 1)(x - 2)(x + 3)$$

This polynomial has three real roots $x_1 = 1, x_2 = 2, x_3 = -3$. On the other hand applying (2) we see that

$$x = \sqrt[3]{-3 + \frac{10\sqrt{3}}{9}i} + \sqrt[3]{-3 - \frac{10\sqrt{3}}{9}i} \tag{3}$$

It is very difficult to believe that this complex expression gives real numbers $x = 1, 2, -3$. In the realm of cubic polynomials complex numbers are unavoidable. (In the case of quadratic equations if equation have real roots then they are expressed via real expressions: you do not need to use complex numbers if equation has real roots.)

These two examples convince us that Cardano–Tartaglia formula is not usually practical. But nevertheless (2) is the formula, expressing roots through radicals...

Another very useful ansatz is the following: For the equation $x^3+px+q = 0$ consider $x = \alpha x$ such that a new x obeys equation

$$x^3 - 3x = a \tag{4}$$

(Note that in the case when $p < 0$ then α is real)

Now considering ansatz $x = e^s + e^{-s}$ we see that

$$x = \begin{cases} 2\cos\left(\frac{1}{3}\arccos a\right) & \text{if }, |\frac{a}{2}| \leq 1 \\ 2\cosh\left(\frac{1}{3}\text{arccosh}a\right) & \text{if }, |\frac{a}{2}| \geq 1. \end{cases}$$

is a root of the equation above.

For fourth order equations one can also find the formula expressing roots through radicals. Considering substitution $x \to x - a/4$ we reduce quadric equation to the equation $x^4 + px^2 + qx + r = 0$. It can be rewritten in the way:

$$\left(x^2 + \frac{p}{2}\right)^2 = -qx - r + \frac{p^2}{4} \tag{5}$$

Choose u such that it obeys cubic equation:

$$\frac{q^2}{8u} = u^2 + pu + \frac{p^2}{4} - r$$

Then:

$$\left(x + \frac{p}{2} + u\right)^2 = \left(\sqrt{2u}x - \frac{q}{\sqrt{2u}}\right) \tag{6}$$

Thus we express x via radicals.

What about higher order equation?

In 1824 Abel proved that there is no formula expressing roots of polynomial equation of the order $n \geq 5$ in terms of coefficients and a finite number of arithmetical operations "+", "-", "$\times$", ":" and n-th roots. But what about a given polynomial equation of the order $n \geq 5$ Abel Theorem states that roots of the equation $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$ cannot be expressed via coefficients a, b, c, d, e, if we use only radicals and arithmetic operations. But it has the solutions expressed in radicals if coefficients a, b, c, d, e take some special values. E.g. consider the case: $a = b = c = d = 0, e = 1$, Then it is easy to see [1] that solutions of the equation $x^5 - 1 = 0$ are expressed via radicals.

Galois gives an answer on this more difficult question.

0.2 Viète Theorem

In this section we consider some links between elementary mathematics and ideas behind Galois theory. Considerations in this section are extremely informal. We give exact definitions later..

Consider polynomial

$$P(x) = x^n + a_{n-1}x^{n-1} + \dots a_0 \tag{7}$$

of the degree n with complex coefficients. We know that it has n complex roots $x_1, \dots, x_n$. It is obvious that

$$x_1 + \dots x_n = -a_{n-1}\,,$$

$$x_1x_2 + \dots x_1x_n + x_2x_3 + \dots + x_2x_n + \dots + x_{n-1}x_n = a_{n-2}\,, \tag{8}$$

$$x_1x_2x_3 + \dots x_1x_{n-1}x_n + x_2x_3x_4 + \dots + x_2x_{n-1}x_n + \dots + x_{n-2}x_{n-1}x_n = a_{n-2}\,,$$

$$\dots$$

$$x_1x_2 \dots x_{n-1}x_n = (-1)^n a_n\,. \tag{9}$$

[1] $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1 = 0)$. One root is equal to 1. To find other four roots consider substitution $z = x + \frac{1}{x}$:$x^4 + x^3 + x^2 + x + 1 = 0 \Rightarrow x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = \left(x + \frac{1}{x}\right)^2 + \left(x + \frac{1}{x}\right) - 1 = 0$ We come to quadratic equation $z^2 + z - 1 = 0\,, z = \frac{-1\pm\sqrt{5}}{2}$. x is a root of quadratic equation $x + \frac{1}{x} - z = 0$. (Note that in fact roots $x_k = e^{i\frac{2\pi k}{5}}$), (k=0,1,2,3,4) In particular $\cos 72^\circ = \frac{z_1}{2} = \frac{\sqrt{5}-1}{4}$

This is so called Viète theorem. It follows from factorization:

$$P(x) = x^n + a_{n-1}x^{n-1} + \dots a_0 = (x - x_1)\dots(x - x_n)\,. \qquad (10)$$

E.g. for quadratic polynomial $x^2 + px + q$ the Viète theorem claims that

$$x_1 + x_2 = -p \quad \text{and} \quad x_1x_2 = q\,, \qquad (11)$$

and for cubic polynomial $x^3 + ax^2 + px + q$

$$x_1 + x_2 + x_3 = -a, \quad x_1x_2 + x_2x_3 + x_3x_1 = p \quad \text{and} \quad x_1x_2x_3 = -q\,. \qquad (12)$$

More sophisticated version of Viète Theorem is:
Every symmetric polynomial $\Sigma(x_1, \dots, x_n)$ on roots $x_1, \dots, x_n$ of a given polynomial $P(x) = x^n + a_{n-1}x^{n-1} + \dots a_0$ can be expressed as polynomial on coefficients $a_{n-1}, \dots a_0$ of the polynomial $P(x)$,

The proof can be done by analysing symmetric polynomials [2]

E.g. if x_1, x_2, x_3 are roots of polynomial $x^3 + ax^2 + px + q$ then according to (12) $x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2x_1x_2 - 2x_2x_3 - 2x_3x_1 = a^2 - 2p$, $x_1^3 + x_3^2 + x_3^3 = (x_1 + x_2 + x_3)(x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_2x_3 - x_3x_1) + 3x_1x_2x_3 = (-a) \cdot (a^2 - 3p) + 3q$

[2] Make the lexicographic ordering in the space of polynomials. It is like in dictionary: x_p is higher than x_q if $p > q$. Monomial $x_1^{a_1} \dots x_n^{a_n}$ is higher than monomial $x_1^{b_1} \dots x_n^{b_n}$ if $a_1 > b_1$. If $a_1 = b_1$ we have to look at the degree of the second variable x_2: If $a_1 = b_1$ and $a_2 > b_2$ then monomial $x_1^{a_1} \dots x_n^{a_n}$ is higher than monomial $x_1^{b_1} \dots x_n^{b_n}$ and so on: monomial $x_1^{a_1} \dots x_n^{a_n}$ is higher than monomial $x_1^{b_1} \dots x_n^{b_n}$ if there exist $k = 1, 2, \dots$ such that if $a_1 = b_1, \dots a_{k-1} = b_{k-1}$ but $a_k > b_k$.

It is enough to prove the Theorem for polynomial of fixed weight. (Weight of the monomial $x_1^{a_1} \dots x_n^{a_n}$ is equal to $a_1 + \dots + a_n$. E.g the weight of the symmetric polynomial $x_1^3+x_2^3+x_1^2x_2+x_2^2x_2$is equal to 3.) Let $P(x_1, \dots, x_n)$ be symmetric polynomial of $x_1, \dots, x_n$ of the weight L:

$$P = \sum_{j_1 + \dots + j_n = L} c_{j_1 \dots j_n} x_1^{j_1} \dots j_n^{a_n}$$

Consider the highest monomial $c_{j_1 \dots j_n} x_1^{j_1} \dots x_n^{j_n}$ in the polynomial P. It is easy to see that $j_1 \geq j_2 \geq \dots \geq j_n = 0$ because this monomial is highest and P is symmetric. This monomial can be killed by the monomial proportional to the following monomial on coefficients $\pm a_{n-1} = x_1 + \dots + x_n$, $\pm a_0 = x_1 \dots x_n$:

$$a_{n-1}^{j_1 - j_2} a_{n-2}^{j_2 - j_3} \dots a_1^{j_{n-1} - j_n} a_0^{j_n}$$

Hence killing highest monomials by monomials on coefficients we express P as polynomial on coefficients

Another **Example (discriminant of cubic polynomial)** Consider expression $D = (x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$. (discriminant of cubic polynomial: it is equal to zero iff any two roots coincide) For simplicity calculate D for reduced cubic polynomial $x^3 + px + q$. Then $x_1 + x_2 + x_3 = 0$ and

$$D = \left[(x_1 + x_2)^2 - 4x_1x_2\right] \left[(x_2 + x_3)^2 - 4x_2x_3\right] \left[(x_3 + x_1)^2 - 4x_3x_1\right] = \tag{13}$$

$$\left[x_3^2 - 4x_1x_2\right] \left[x_1^2 - 4x_2x_3\right] \left[x_2^2 - 4x_3x_1\right] =$$

$$-63x_1^2x_2^2x_3^2 - 4(x_1^3x_2^3 + x_2^3x_3^3 + x_3^3x_1^3) + 16x_1x_2x_3(x_1^3 + x_2^3 + x_3^3) =$$

$$-63q^2 - 4\left((-px_1 - q)(-px_2 - q) - \dots\right) - 16q\left((-px_1 - q) - \dots\right) =$$

$$D = -27q^2 - 4p^3\,. \tag{14}$$

We see that discriminant D appears up to a factor in Cardano-Tartaglia formula (2): $\sqrt{\frac{p^3}{27} + \frac{q^2}{4}} = \sqrt{\frac{27q^2+4p^3}{108}} = \frac{\sqrt{-D}}{6\sqrt{3}}$

Now consider more properly the properties of symmetric polynomials. The polynomial $\Sigma(t_1, \dots, t_n)$ (or rational function $R(t_1, \dots, t_n) = \frac{P(t_1,\dots,t_n)}{Q(t_1,\dots,t_n)}$) is called symmetric if it is invariant under all permutations of $(t_1, \dots, t_n) \to (t_{\sigma_1}, \dots, , t_{\sigma_n})$ of variables. $((1, \dots, n) \to (\sigma_1, \dots, \sigma_n)$ is a permutation)

Viète Theoreme can be formulated in slightly different way:

The polynomial (rational function) which remains invariant under action of the group S_n of permutations is polynomial (rational function) of coefficients.

Example Let x_1, x_2, x_3 be roots of cubic equation $f = x^3+ax^2+bx+c = 0$ with rational coefficients. Consider the group S_3 of permutations. It contains 6 elements:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, s = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, s^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \tag{15}$$

$$\sigma_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \sigma_{13} = s{\circ}\sigma_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \sigma_{23} = \sigma_{12}{\circ}s = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \tag{16}$$

It acts on roots if x_1, x_2, x_3 of cubic polynomial $f = x^3 + ax^2 + bx + c$ and on functions of roots:

$$e \circ \Sigma(x_1, x_2, x_3) = \Sigma(x_1, x_2, x_3)\,, \quad s \circ \Sigma(x_1, x_2, x_3) = \Sigma(x_2, x_3, x_1)\,, \tag{17}$$

$$s^2 \circ \Sigma(x_1, x_2, x_3) = \Sigma(x_3, x_1, x_2)\,, \quad \sigma_{12} \circ \Sigma(x_1, x_2, x_3) = \Sigma(x_2, x_1, x_3)\,, \quad (18)$$

$$\sigma_{13} \circ \Sigma(x_1, x_2, x_3) = \Sigma(x_3, x_2, x_1)\,, \quad \sigma_{23} \circ \Sigma(x_1, x_2, x_3) = \Sigma(x_1, x_3, x_2)\,, \quad (19)$$

Consider an arbitrary polynomial $\Sigma(x_1, x_2, x_3)$ on roots. (E.g. $\Sigma(x_1, x_2, x_3) = x_1^7 x_2^5 x_3^2 + x_1^9 x_2^4 x_3$)

Act on this polynomial by the group S_3:

$$\Sigma_{\text{symm}} = \Sigma + s \circ \Sigma + s^2 \circ \Sigma + \sigma_{12} \circ \Sigma + \sigma_{13} \circ \Sigma + \sigma_{23} \circ \Sigma$$

i.e.

$$\Sigma_{\text{symm}}(x_1, x_2, x_3) = \Sigma(x_1, x_2, x_3) + \Sigma(x_2, x_3, x_1) + \cdots + \Sigma(x_1, x_3, x_2) \quad (20)$$

Then the polynomial $\Sigma_{\text{symm}}(x_1, x_2, x_3)$ is symmetric polynomial:

$$\forall g_i \in S_3 \qquad g_i \circ \Sigma_{\text{symm}} = \Sigma_{\text{symm}}$$

Hence the value of polynomial Σ_{symm} on the roots is a rational number. (Prove it!)

Example E.g. Let $\Sigma(t_1, t_2, t_3) = t_1 + \frac{t_2}{t_3}$. Then

$$\Sigma_{\text{symm}}(x_1, x_2, x_3) = x_1 + \frac{x_2}{x_3} + x_2 + \frac{x_3}{x_1} + x_3 + \frac{x_1}{x_2} + x_2 + \frac{x_1}{x_3} + x_1 + \frac{x_3}{x_2} + x_3 + \frac{x_2}{x_1} =$$

If x_1, x_2, x_3 are roots of cubic polynomial $x^3 + ax^2 + bx + c$ then it is equal to

$$2(x_1 + x_2 + x_3) + \frac{x_1 + x_2}{x_3} + \frac{x_2 + x_3}{x_1} + \frac{x_1 + x_3}{x_2} = -2a - \frac{a + x_3}{x_3} - \frac{a + x_1}{x_1} - \frac{a + x_2}{x_2} =$$

$$-2a - 3 - a\left(\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}\right) = -2a - 3 + \frac{ab}{c}$$

We see that in spite of the fact that we cannot solve (do not want to solve) the equation we can easily express the symmetric combinations of roots via coefficients of polynomial.

0.3 Trying to generalize Viète Theorem. Toy example of Galois Theory

Now try to analyze polynomial of roots which **are not invariant** under all permutations.

In general case polynomial $\Sigma(x_1, \ldots, x_n)$ (where $x_1, \ldots, x_n$ are n roots of polynomial equation) takes $n!$ different values under the action elements of permutation group S_n. If polynomial $\Sigma(x_1, \ldots, x_n)$ is symmetric polynomial as above then it takes exactly one value. Consider intermediate case, where polynomial is not symmetric (i.e. is not invariant under all group S_n) but it is invariant under the action of subgroup $H \subseteq S_n$ [3]. We cannot apply in this case Viète Theorem. But still one can calculate the values of this polynomial on roots without straightforward calculaltion of the roots.

Demonstrate the main idea on the following example:

Example Consider the polynomial:

$$w(x_1, x_2, x_3) = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 \,. \tag{22}$$

This polynomial is not symmetric polynomial: $\sigma_{12} \circ w \neq w$. But it is still invariant under the action of subgroup $H = (e, s, s^2) \subseteq S_3$ of cyclic permutations:

$$s \circ w(x_1, x_2, x_3) = w(x_2, x_3, x_1) = x_2^2 x_3 + x_3^2 x_1 + x_1^2 x_2 = w(x_1, x_2, x_3)$$

Under the action of all group S_3 it takes two values ($|S_3| = 6$, $|H| = 3$, $6 : 3 = 2$)

$$w = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 \,, \quad \text{and} \quad w' = \sigma_{12} \circ w = x_2^2 x_1 + x_1^2 x_3 + x_3^2 x_2$$

. Consider quadratic polynomial

$$\mathcal{P}(z) = (z - w)(z - w') = z^2 - (w + w')z + ww'$$

It is evident that $w + w'$ and ww' are invariant under action of the group S_3 of all permutations and hence according to Viète Theorem they can be expressed rationally through a, b, c, coefficients of the cubic polynomial f! For example $\sigma_{12}(w + w') = w' + w$. We come to very important conclusion:

The expression $w(x_1.x_2.x_3) = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1$ for roots of the cubic equation is a root of a quadratic equation with rational coefficients. We can calculate it by solving the equation of lower degree.

[3] i.e. it takes at most m different values where m is an index of subgroup H in the group S_n:

$$m = \frac{|S_n|}{|H|} = \frac{n!}{|H|} \tag{21}$$

We did this conclusion without solving the cubic equation: we just examine the symmetry property of the polynomial (22).

These considerations lead to the following statement which can be considered as a generalization of Viète Theorem

Proposition

Let $x_1, x_2, \dots, x_n$ are roots of polynomial $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1 x + a_0 = 0$. Let $\Sigma(x_1, \dots, x_n)$ be a polynomial on roots $x_1, \dots, x_n$ with coefficients which are polynomials on coefficients $a_1, \dots, a_{n-1}$.

1. If the polynomial $\Sigma(x_1, \dots, x_n)$ takes only one value under action of permutation group S_n Σ is polynomial on coefficients $a_1, \dots, a_{n-1}$ (just standard Viète Theorem:).

2. If the polynomial $\Sigma(x_1, \dots, x_n)$ defined above takes two values under the action of group S_n then it is a root of quadratic equation (with coefficients which are polynomials of $a_1, \dots, a_{n-1}$)

This statement can be considered as a toy example in Galois Theory.

Proof of Proposition Consider subgroup H of permutations which preserve $\Sigma(x_1, \dots, x_n)$. One can prove that subgroup H has index 2 ($|H| = \frac{|S_n|}{2}| = \frac{n!}{2}$) Let $g \in S_n, g \notin H$. If $H = \{h_1, h_2, h_3, \dots, h_k\}$, then $S_n = \{h_1, h_2, h_3 \dots, h_k, gh_1, gh_2, gh_3, \dots, gh_k\}$ Consider $\Sigma' = g \circ \Sigma$. Then

of roots. Hence according to the Viète Theorem u, v are polynomials on $a_1, \dots, a_{n-1}$. Respectively Σ, Σ' are roots of quadratic equation $z^2 - uz + v = 0$ ∎

1 Ring of polynomials

In this Section we consider the ring of polynomials over field and we see that this ring has features close to the features of ring of integers. In particularly for this ring there exists an analogue of Fundamental Theorem of Arithmetics

1.1 Recollection of rings

Definition A ring is a set R equipped with two binary operations $" + ", " \times "$ such that $\{R, +\}$ is abelian group under addition, multiplication is associative $(ab)c = a(bc)$ and the following relations hold (distribution laws):

$$a \times (b + c) = a \times b + a \times c,\ (b + c) \times a = b \times a + c \times a$$

,

Definition An integral domain $(R,+,\times)$ is a ring with the following properties:

- Multiplication $\times$ is commutative
- There exists an element e such that for every $a \in R$, $e \times a = a \times e = a$
- If $ab = 0$ then $a = 0$, or $b = 0$

Examples $\mathbf{Z},\mathbf{Q}$ $\mathbf{R}$, $\mathbf{C}$, $Mat[p \times p]$ with standard multiplicatioon and addition are rings and these rings are integral domains.

The linear space of vectors with standard addition law and vector product $\times$ is ring where multiplication is anticommutative ($a \times b = -b \times a$), has not element e and product of two orthogonal vectors is equal to zero.

The space $C([0,1])$ of continuous functions on $[0,1]$ is ring but it is not integral domain: Consider functions f, g such that $f \equiv 0$ for $x < 3/4$ and $g \equiv 0$ for $x > 1/4$ Then $fg = 0$ but $f \neq 0$ and $g \neq 0$

Another example: $\mathbf{Z}/n\mathbf{Z}$-ring of residuals modulo n. It contains elements $\{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n}\}$, $\bar{a} + \bar{b} = \bar{c}$, where $c = a + b$ modulo n and $\bar{a} \times \bar{b} = \bar{d}$, where $d = ab$ modulo n.

Definition A ring $(R, +\times)$ is a *field* if it $R - \{0\}$ is abelian group with respect to multiplication $\times$.

E.g. integral domain is a field if every non-zero element has inverse.

Examples. $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ are fields. $\mathbf{Z}$ is not a field, Space $Mat[p \times p]$ of $p \times p$ matrices is not a field too.

Another important example: Let $(R,+,\times)$ be an integral domain. Then one can consider its field of fractions: pairs f/g with $g \neq 0$ and indentification $f/g = f'/g'$ if $fg' = f'g$.

In this way one come from $\mathbf{Z}$ to $\mathbf{Q}$.

Another very important example:

Proposition A ring $\mathbf{Z}/n\mathbf{Z}$ is a field iff n is a prime.

Characteristic of field

Let $(K, +\times)$ be any field. Consider the elements

$$a_n = \underbrace{1 + 1 + \cdots + 1}_{n-times} \tag{23}$$

If for all n $a_n \neq 0$ then all a_n are different. Hence this field possesses $\mathbf{Z}$ and $\mathbf{Q}$. Suppose n is a minimal number such that $a_n = 0$ $(n > 0)$. Then evidently n is a prime. Hence the field possesses a field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

We come to

Proposition The prime subfield of every field (intersection of all subfields) is $\mathbf{Q}$ or $\mathbf{F}_p$

This motivates

Definition. We say that a field K has a *characteristic* 0 if its prime subfield is $\mathbf{Q}$. We say that a field K has a *characteristic* p if its prime subfield is $\mathbf{F}_p$.

Geometric interpretaion of the ring $\mathbf{Z}/N\mathbf{Z}$. This ring can be interpreted in terms of regular N-gon on the plane. Namely consider n $\{A_0, A_1, \dots, A_{N-1}\}$ points $\{A_0, A_1, \dots, A_{N-1}\}$ on the complex plane which are vertices of the regular n-gon:

$$A_0 = 1, A_1 = \varepsilon_N, A_2 = \varepsilon_N^2, A_3 = \varepsilon_N^3 \dots, A_N = \varepsilon_N^{N-1}, \text{ where } \varepsilon = e^{\frac{2\pi i}{N}} \tag{24}$$

and define addition and multiplication as follows

$$A_p \widetilde{+} A_q = \varepsilon_N^{k+q} = A_{p+q \text{ (modulo } N)}, \; A_p \widetilde{*} A_q = \varepsilon_N^{pq} = A_{pq \text{ (modulo } N)}$$

It is easy to see that we come to the structure of the ring $\mathbf{Z}/N\mathbf{Z}$. E.g. if $N = 5$ we have hexagon with the vertices

$$A_0 = 1, A_1 = e^{\frac{2\pi i}{6}} = e^{\frac{\pi i}{3}}, A_2 = e^{\frac{2\pi i}{3}}, A_3 = -1, A_4 = e^{\frac{-2\pi i}{3}}, A_5 = e^{\frac{-\pi i}{3}}$$

$A_2 \widetilde{+} A_3 = A_5, \; A_2 \widetilde{*} A_3 = A_0,$

1.2 Ring of polynomials over field or integral domain

Let $\mathbf{K}$ be a ring. Consider the set of polynomials over $\mathbf{K}$, i.e. polynomials

$$a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0 \tag{25}$$

with coefficients $(a_n, a_{n-1}, \dots, a_1, a_0)$ from ring $\mathbf{K}$.

One can naturally define the operations " + " and " × " in the set of polynomials. It is easy to see that the set of polynomials becomes a ring under these operations. We denote this ring by $\mathbf{K}[t]$. One can easy prove

Proposition A ring $\mathbf{K}[t]$ is an integral domain if the ring K is an integral domain

An arbitrary field is integral domain. In what follows we will mainly consider polynomials with coefficients in a field.

Remark One can consider polynomial (25) as function on $\mathbf{K}$ with values in $\mathbf{K}$ or as formal expression defined by coefficients $(a_n, a_{n-1}, \dots, a_1, a_0)$. Here we stand on the second point of view considering polynomials as formal expressions (25). These two approaches can be essentially different. E.g. if $\mathbf{K}$ is finite field then one can construct two polynomials $f = a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0$ and $g = b_m t^m + m_{m-1} t^{m-1} + \dots + b_1 t + b_0$ such that they coincide as functions from $\mathbf{K}$ to $\mathbf{K}$ $(\forall t \in K \ f(t) = g(t))$ but do not coincide as formal polynomials (i.e. they have different coefficients.) E.g. let $\mathbf{K} = F_3 = \mathbf{Z}/3\mathbf{Z}$. Then polynomials $f = t^{2003}$ and $g = f + t^3 - t$ coincide at all $t = \{\bar{0}, \bar{1}, \bar{2}\}$. It can be easily generalized. Let p be prime then in the field $\mathbf{K} = F_p = \mathbf{Z}/p\mathbf{Z}$ $= \{\bar{0}, \bar{1}, \bar{2}, \dots, p \bar{-} 1\}$ a polynomial

$$h_p(t) = t(t - \bar{1})(t - \bar{2}) \dots (t - p \bar{-} 1) = t^p - t \tag{26}$$

takes zero values at all $t \in F_p$. For an arbitrary polynomial $f \in F_p[t]$ $f(t) \equiv f(t) + t^p - t(t)$.

The situation is different for an infinite field:

Proposition Let two polynomials $f(t) = a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0$ and $g(t) = b_m t^m + m_{m-1} t^{m-1} + \dots + b_1 t + b_0$ coincide in infinite number of distinct points (distinct elements of the field K). Then these polynomials coincide as formal polynomials,i.e.

$$b_0 = a_0, b_1 = a_1 \dots, b_k = a_k, \dots$$

Exercise Prove this Proposition. (Hint: Consider the difference of two polynomials. Note that polynomial $at^n + bt^{n-1} + \dots$ has no more that n roots if $a \neq 0$. Compare with (26).)

Definition We say that the degree of polynomial $f \in \mathbf{K}[t]$ is equal to m if $f = a_m t^m + \dots + a_0$ with $a_m \neq 0$. The degree of constant non-zero polynomial (non-zero scalar from K) are equal to zero by definition. For every polynomial $f \in \mathbf{K}[t]$ we denote by ∂f the degree of this polynomial. It is convenient to assign to the polynomial 0 the degree equal to $-\infty$ (See the exercise below).

Exercise Show that for polynomials $f, g \in \mathbf{K}[t]$

$$\partial(f + g) \leq \partial f + \partial g \,, \partial(fg) = \partial f + \partial g \,. \tag{27}$$

Exercise Prove that the set of units (set of invertible elements) in $\mathbf{Q}[t]$ is just $\mathbf{Q} - 0$.

Later we use the notion of *monic polynomial.* A polynomial $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$ with coefficients from the integral domain is called monic polynomial if the highest coefficient a_n is equal to 1.

Remark The set of monic polynomials of degree n is not a linear space, It is affine space associated with $n-1$-dimensional vector space.

1.3 Highest common factor.

In the same way as in the ring of integers every polynomial in the ring of polynomials can be divided by another provided that a remainder term is allowed. (As it was mentioned above we consider a ring $K[t]$ where K is a field)

Proposition Let $f, g \in \mathbf{K}[t]$ and $g \neq 0$. Then there exist unique polynomials h, r such that

$$f = hg + r\,, \quad \text{with} \quad \partial r < \partial g\,. \tag{28}$$

Remark In the field of integers instead (28) for arbitrary integers p, q we have

$$p = hq + r\,, \quad \text{with} \quad |r| < |q|\,. \tag{29}$$

The degree of polynomial in the ring of polynomials plays the role of the usual norm in the ring of integers[4].

The existence algorithm for (28)is evident. The uniqueness follows from the (27): If $f = hg + r = h'g + r'$ then

$$(h - h')g = r - r', .$$

Indeed suppose $h - h' \neq 0$. Then the degree of polynomial in l.h.s. is not less than degree of polynomial g. On the other hand the degree of polynomial in r.h.s. is less that degree of polynomial g. Contradiction. Hence $h = h', r = r'$.

For two polynomials f, g one can consider their highest common factor

Definition A highest common factor (h.c.f.(f, g)) of polynomials f, g is a

[4] Note that in the ring of integers, the remainder is not fixed uniquely by the condition above: $37 = 5\times 7+2 = 6\times 7+(-5)$ The standard norm norm in integers is an archimedian norm, the norm defined by degree of polynomials is non-archimedian norm.

polynomial d_0 such that it divides f, g and if polynomial d divides f and g then it divides d_0 also.

Here an indefinite article "a" stands in the appropriate place: highest common factor of two polynomials is defined uniquely up to multiplication by a constant (non-zero element of the field K) [5]

First prove uniqueness. If d_0 and $\tilde{d_0}$ are highest common factors of polynomials f, g then by definition $d_0|\tilde{d_0}$ and vice versa $\tilde{d_0}|d_0$. Hence it follows from (28) and (27) that $\tilde{d_0} = kd_0$, where $k \in \mathbf{K}$.

The existence follows from Euclidean algorithm.

Let $f = r_0$, $g = r_1$ then according (28) apply Euclidean algorithm. We have the ladder of divisions with decreasing degrees of remainders:

$$\begin{array}{cccccc} r_0 & = h_1 r_1 & + r_2 & , & \partial r_2 < \partial r_1 \\ r_1 & = h_2 r_2 & + r_3 & , & \partial r_3 < \partial r_2 \\ \dots & \dots & \dots & & \dots \\ r_{n-1} & = h_n r_n & + r_{n+1} & , & \partial r_{n+1} < \partial r_n \\ r_n & = h_{n+1} r_{n+1} & +0 & , & r_{n+2} = 0\,, \partial r_{n+2} = -\infty \end{array} \tag{30}$$

Climbing up on this ladder it is easy to see that r_{n+1} is highest common divisor.

The following technical lemma is very useful:

Lemma If polynomials f, g are coprime then there exist polynomials a, b such that

$$af + bg = 1 \tag{31}$$

Of course the same statement is right in the field of integers:

Lemma′ If integers p, q are coprime then there exist integers a, b such that

$$ap + bq = 1 \tag{32}$$

Example 1 $f = x^2$, $g = x - 1$, f, g are obviously coprime polynomials and $f - (x + 1)g = 1$, $a = 1, b = 1 - x$

Example 2 $p = 45$, $q = 7$, p, q are coprime. Obviously

$$13q - 2p = 1 \tag{33}$$

Example 3

[5] The group of unities of the ring of polynomials $K[t]$ (invertible elements of this ring) is the initial field K. The highest common factor is defined up to the unity.

$p = 225$, $q = 157$, p, q are coprime. It is very easy to check but not obvious to find that

$$43q - 30p = 1 \tag{34}$$

First two examples are very easy. But how to guess an answer in the third one [6]?

A way to find a, b obeying (31) (respectively (32) is to apply Euclidean algorithm (30) for polynomials [7] f, g. Demonstrate it in the case if algorithm (30) has only five steps:

$$f = r_0, g = r_1 \quad \begin{array}{llllll} r_0 & = h_1 r_1 & + r_2 & , & \partial r_2 < \partial r_1 \\ r_1 & = h_2 r_2 & + r_3 & , & \partial r_3 < \partial r_2 \\ r_2 & = h_3 r_3 & + r_4 & , & \partial r_4 < \partial r_3 \\ r_3 & = h_4 r_4 & + r_5 & , & \partial r_5 < \partial r_4 \\ r_4 & = h_5 r_5 & & , & \partial r_6 = -\infty \end{array} \tag{35}$$

In the last equation the highest common divisor r_5 is equal to one (or constant) because polynomials are coprime.

Look on the last steps of the ladder. For $f' = r_3, g' = r_4$ the last but one step gives a solution to (31):

$$r_3 - h_4 r_4 = r_5 = 1\,, f' - h_4 g' = 1$$

Using the upper step of the ladder: $r_2 = h_3 r_3 + r_4$ we express r_4 via r_2, r_3:

$$r_3 - h_4(r_2 - h_3 r_3) = 1$$

We come to the relation (31) for for $f' = r_2, g' = r_3$. Now using the step $r_1 = h_2 r_2 + r_3$ we express r_3 via r_1, r_2 and come to the relation (31) for for $f' = r_1, g' = r_2$. And so on till end...

Of course the same can be done for ring of integers.

Example Let $f = t^3 - 2$, $g = t^2 + 3t + 5$. Then dividing $t^3 - 2$ by $t^2 + 3t + 5$ and then dividing $(t^2 + 3t + 5)$ by the remainder we come to

$$\mathbf{t^3 - 2} = (t - 3)(\mathbf{t^2 + 3t + 5}) + (4t + 13)\,, \tag{36}$$

[6] Note that any solution of (31) (or correspondingly of (32) for ring of integers) produce all solutions: if a pair (a_0, b_0) is a solution of (31) then an arbitrary solution is given by the formula $a = a_0 + Rg, b = b_0 + Rf$ where R is an arbitrary polynomial. (For the ring of integers: if (a_0, b_0) obey is a solution of (31) then an arbitrary solution is given by the formula $a = a_0 + Rq, b = b_0 + Rp$ where R is an arbitrary integer.)

[7] Of course often it can be more effective to find solution to equation (31) by straightforward considerations.

$$(\mathbf{t^2}+\mathbf{3t}+\mathbf{5}) = \left(\frac{t}{4}-\frac{1}{16}\right)(\mathbf{4t}+\mathbf{13}) + \frac{93}{16}\,, \tag{37}$$

$$r_0 = \mathbf{t^3}-\mathbf{2}, \quad r_1 = (\mathbf{t^2}+\mathbf{3t}+\mathbf{5}), \quad , r_2 = \mathbf{4t}+\mathbf{13}$$

The relation (37) means that for functions $f' = (\mathbf{t^2}+\mathbf{3t}+\mathbf{5})$, $g' = (\mathbf{4t}+\mathbf{13})$

$$f' - \left(\frac{t}{4}-\frac{1}{16}\right)g' = \frac{93}{16}$$

Now using (36) express g' via $f = (\mathbf{t^3}-\mathbf{2})$ and $g = (\mathbf{t^2}+\mathbf{3t}+\mathbf{5})$ we come to the

$$(\mathbf{t^2}+\mathbf{3t}+\mathbf{5}) - \left(\frac{t}{4}-\frac{1}{16}\right)\left[\mathbf{t^3}-\mathbf{2}-(t-3(\mathbf{t^2}+\mathbf{3t}+\mathbf{5}))\right] = \frac{93}{16}$$

Opening brackets we come to

$$(4t^2-13t+19)(\mathbf{t^2}+\mathbf{3t}+\mathbf{5}) - (4t-1)(\mathbf{t^3}-\mathbf{2}) = 93$$

1.4 Continuous fractions and Euclidean algorithm

Technically it is easy and beautiful to calculate a solution of the equations (31) and (32) using continuous fractions.

Demonstrate this on the ring of integers (For ring of polynomials it is almost the same)

E.g. consider numbers $p = 225, q = 157$ from the example 3:

$$\mathbf{225} = 1\times 157+68\,, \quad \Leftrightarrow \frac{225}{157} = 1+\frac{68}{157}\,; \mathbf{157} = 2\times\mathbf{68}+21\,, \quad \Leftrightarrow \frac{225}{157} = 1+\frac{1}{2+\frac{21}{68}}$$

$$\mathbf{68} = 3\times\mathbf{21}+5\,, \quad \Leftrightarrow \frac{225}{157} = 1+\frac{1}{2+\frac{1}{3+\frac{5}{21}}}\,; \mathbf{21} = 4\times\mathbf{5}+1\,, \quad \Leftrightarrow \frac{225}{157} = 1+\frac{1}{2+\frac{1}{3+\frac{1}{4+\frac{1}{5}}}}$$

Now take the last but one approximation of the fraction

$$x_0 = \frac{225}{157} = 1+\frac{1}{2+\frac{1}{3+\frac{1}{4+\frac{1}{5}}}} \tag{38}$$

i.e. remove its last "deepest" part:

$$x_1 = 1+\frac{1}{2+\frac{1}{3+\frac{1}{4}}}$$

Then

$$x_1 = 1 + \frac{1}{2 + \frac{1}{3+\frac{1}{4}}} = 1 + \frac{1}{2 + \frac{4}{13}} == 1 + \frac{13}{30} = \frac{43}{30}$$

and

$$x_1 - x_0 = \frac{43}{30} - \frac{225}{157} = \frac{43 \times 157 - 30 \times 225}{157 \times 30} = \frac{1}{157 \times 30}$$

We come to solution to the equation (34) [8].

Continuous fractions give us the following : Write continuous fraction for a fraction $\frac{f}{g}$ then take its last but one approximation,i.e. remove its "deepest"part, and return to the usual fraction. We come to the fraction $\frac{a}{b}$ such that $ag - bf = \pm 1$.

E.g. $f = x^2 + x - 1, g = x^2$: We have

$$x_0 = \frac{f}{g} = \frac{x^2 + x - 1}{x - 1} = 1 + \frac{x-1}{x^2} = 1 + \frac{1}{\frac{x^2}{x-1}} = 1 + \frac{1}{x + 1 + \frac{1}{x-1}}$$

The first approximation will be

$$x_1 = 1 + \frac{1}{x+1} = \frac{x+2}{x+1}$$

We see that

$$(x+2)\mathbf{x^2} - (x+1)(\mathbf{x^2 + x - 1}) = 1$$

1.5 Factorisation of polynomials

The Fundamental Theorem of Arithmetic states that there exists a unique decomposition of every integer on prime numbers (up to the order of multipliers). This Theorem follows from:

Lemma If p is a prime integer such that $p|ab$ for two integers a, b then $p|a$ or $p|b$. The proof of this lemma is based on the lemma (32) (analogue of (31) for the ring of integers) for integers: Let $ab = mp$ and p does not divide a. Then a, p are coprime. If by (32) $ax + py = 1$ then $abx + pby = b$. p divides ab and pb. Hence it divides b also.

In the ring $\mathbf{K}[t]$ of polynomials with coefficients in the field $\mathbf{K}$ the role of prime numbers are played by irreducible polynomials.

[8] If $\frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \frac{P_3}{Q_3}, \ldots, \frac{P_n}{Q_n}, \frac{P_{n+1}}{Q_{n+1}}, \ldots$ is the sequence of continuous fractions approximating a given number then for every k

$$\frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}} = \frac{\pm 1}{Q_k Q_{k+1}} \tag{39}$$

Definition The polynomial $p(t) \in \mathbf{K}[t]$ is called reducible if $p = fg$ where the degrees of polynomials f and g are less than the degree of the polynomial p.Otherwise the polynomial is called reducible.

(Compare with definition of composite and prime integers)

For example the polynomial $t^2 + t + 1$ is irreducible in $\mathbf{Q}[t], \mathbf{R}[t]$ and it is reducible in $\mathbf{C}[t]$.

Irreducible polynomials play the role of prime numbers in the ring of polynomials.

Lemma If p is irreducible polynomial in $\mathbf{K}[t]$, and $p|fg$ for two polynomials $f, g \in \mathbf{K}[t]$, then $p|f$ or $p|g$. The proof is the same as for integers: Let $fg = hp$ and p does not divide f. Then polynomials f, p are coprime. If by (31) $fx + py = 1$ then $fgx + pgy = g$. p divides fg and pg. Hence it divides g also.

From this lemma follows Theorem:

Theorem Every polynomial $F \in \mathbf{K}[t]$ can be decomposed uniquely by irreducible polynomials (up to a constant factor and ordering of multipliers)

Proof Suppose $F = f_1 f_2 \cdot \dots \cdot f_n = g_1 g_2 \cdot \dots \cdot g_n$ where polynomials $(f_1, \dots, f_n, g_1, \dots, g_m)$ are irreducible polynomials of degree greater than 1 (i.e. not constants). Consider polynomial f_1. It follows from lemma that f_1 divides at least one of polynomials $g_1, \dots, g_m$. Without loss of generality suppose that f_1 divides g_1. Both these polynomials are irreducible and they are not constants. Hence $f_1 = c_1 g_1$ where $c_1 \in K$ is a constant. Divide F by f_1 and consider f_2. Thus we will prove that after reordering of polynomials $g_1, \dots, g_m$ we come to $f_1 = c_1 g_1, f_2 = c_2 g_2, \dots, f_n = c_n g_n$.

1.6 Tests for irreducibility

Gauss Lemma If polynomial f with integer coefficients is irreducible over $\mathbf{Z}$ then it is irreducible over $\mathbf{Q}$.

This is very useful Lemma. Irreducibility over $\mathbf{Z}$ is much easier to check that irreducibility over $\mathbf{Q}$. E.g if $f = t^3 + at^2 + bt + c$ is a polynomial with integer coefficients then irreducibility over $\mathbf{Z}$ means the *absence of the integer roots*. This can be checked easily because integer root divides c.

Note that the absence of integer roots is sufficient but not necessary condition for irreducibility of monic polynomial if the degree of polynomial is higher than 3: the polynomial $x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$ is reducible over $\mathbf{Z}$ in spite of the fact that it has no even real roots!

Proof of the lemma

Let a polynomial $f \in \mathbf{Z}[t]$ be reducible over $\mathbf{Q}$: $f = gh$, where

$$f = A_n t^n + A_{n-1} t^{n-1} + \cdots + A_1 t + A_0 \,, \quad A_n \neq 0 \,, A_i \in \mathbf{Z}$$

$$g = \alpha_n t^n + \alpha_{n-1} t^{n-1} + \cdots + \alpha_1 t + \alpha_0 \,, \quad \alpha_n \neq 0 \,, \alpha_i \in \mathbf{Q}$$

$$h = \beta_m t^m + \beta_{m-1} t^{m-1} + \cdots + \beta_1 t + \beta_0 \,, \quad \alpha_n \neq 0 \,, \beta_i \in \mathbf{Q}$$

Prove that it is reducible over $\mathbf{Z}$ too, i.e. one can choose coefficients α_i, β_j integers.

Choose N such that multiplying by N we can come to polynomials g', h' with integer coefficients:

$$f' = Nf = g'h', \tag{40}$$

where

$$g', h' \in \mathbf{Z}[t] \quad g' = a_n t^n + \cdots + a_0 \,, \quad h' = b_m t^n + \cdots + b_0 \,, a_i, b_j \in \mathbf{Z} \tag{41}$$

E.g. we can take N equal to the product of all denominators of all fractions $\{\alpha_n, \ldots, \alpha_0, \beta_m, \ldots, \alpha_0\}$.

Consider *minimal* (positive integer) N such that (40) is obeyed. Prove that it is equal to 1, i.e. polynomial f itself is reducible over $\mathbf{Z}$. Suppose that $N \neq 1$ and it contains prime factor p. It means that all coefficients of f' are divisible on p. If all coefficients of g' or all coefficients of h' are divisible on p then one can chose $g' \mapsto \frac{g'}{p}$ or $h' \mapsto \frac{h'}{p}$ and reduce the number N. But the number N is chosen already to be the minimal. Hence suppose that not all coefficients of g and not all coefficients of h are divisible on p. Let r be the smallest number such that a_r is not divisible on p and s be the smallest number such that b_s is not divisible on p. Comparing coefficient at t^{r+s} in the left hand side and right and side of the (40) we see that this coefficient is equal to

$$\underbrace{K}_{\text{divisible on } p} = \sum_{i+j=r+s} a_i b_j = \underbrace{a_r b_s}_{\text{not divisible on } p} +$$

$$\underbrace{\sum_{i<r,\, j>s, i+j=r+s} a_i b_j}_{\text{divisible on } p} + \underbrace{\sum_{i>r,\, j<s, i+j=r+s} a_i b_j}_{\text{divisible on } p}$$

Contradiction. ■

There are different ways to check irreducibility over **Z**. In particular very practical Test is

Eisenstein Test. Let f be a polynomial with integer coefficients, $f = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$ and p be a prime number such that the following conditions are obeyed:

1) p does not divide the higher coefficient a_n,

2) p divides all other coefficients

3) p^2 does not divide the coefficient a_0

Then polynomial f is irreducible over **Z**. Hence according Gauss lemma it is irreducible over **Q**.

Proof: Suppose for a contradiction that $f = gh$ where $g = b_r t^r + b_{r-1} t^{r-1} + \cdots + b_1 t + b_0$, $h = c_s t^s + a_{s-1} t^{s-1} + \cdots + a_1 t + a_0$. Then $a_0 = b_0 c_0$. p divides a_0 and p^2 does not divide a_0. W.L.O.G. suppose that p does not divide b_0 and p divides c_0. Note that p does not divide the highest coefficient c_s. Let k be a minimal number such that p does not divide c_k. Then $a_k = b_0 c_k + b_1 c_{k-1} + \dots$ is not divisible on p. Contradiction.

Examples

Example. Consider polynomials

$$f(t) = \frac{t^7 - 1}{t - 1} = 1 + t + t^2 + t^3 + t^4 + t^5 + t^6 \tag{42}$$

This polynomial is irreducible. To see it consider $t = u + 1$ and apply Eisenstein test for polynomial $f(1 + u)$ and for $p = 7$. One can prove in the similar way that a polynomial $f(t) = \frac{t^p - 1}{t - 1}$ is irreducible over **Q** for an arbitrary prime p.

$$g(t) = \frac{t^6 - 1}{t - 1} = 1 + t + t^2 + t^3 + t^4 + t^5 \tag{43}$$

over **Q**. This polynomial is reducible: $\frac{t^6 - 1}{t - 1} = 1 + t + t^2 + t^3 + t^5 = \frac{(t^3 - 1)(t^3 + 1)}{t - 1}$ $= (t^2 + t + 1)(t^3 + 1)$.

Emphasize that the Eisenstein criterion is a sufficient but not necessary condition for a polynomial being irreducible.

2 Field extension

We say that $L : K$ is a field extension if K is a subfield of L, or if K is embedded in L by a field monomorphism.

If X is subset in the field L then subfield in L generated by X is intersection of all subfields of L which contain X.

If $L : K$ is field extension denote by $K(X)$ subfield of L generated by $K \cup X$.

Examples

1. Consider in a field $\mathbf{C}$ of complex numbers subfield $\mathbf{R}$ of real numbers. $\mathbf{R}(i) : \mathbf{R}$ is nothing but $\mathbf{C} : \mathbf{R}$. Subfield $\mathbf{R}(i) = \mathbf{C}$.

2. Consider in a field $\mathbf{R}$ of real numbers subfield $\mathbf{Q}$ of rational numbers. $\mathbf{Q}(\sqrt{2}) : \mathbf{Q}$ is extension of rationals by $\sqrt{2}$. $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2}, a, b \in \mathbf{Q}\}$. It is a subfield in $\mathbf{R}$ which does not coincide with $\mathbf{R}$

We say that extension $L : K$ is isomorphic to extension $\tilde{L} : \tilde{K}$ if there exist isomorphisms $\psi\colon K \leftrightarrow \tilde{K}$, $\varphi\colon L \leftrightarrow \tilde{L}$ such that $\varphi\big|_K = \psi$ and $\tilde{\iota}\psi = \varphi\iota$, where $\iota, \tilde{\iota}$ are embedding monomorphims of K and $\tilde{K}$ in L and $\tilde{L}$ respectively.m

2.1 Simple extension

The extension $L : K$ is called simple if there exists $\alpha \in L$ such that $L = K(\alpha)$. E.g. extensions $\mathbf{Q}(i) : \mathbf{Q}$, $\mathbf{Q}(\sqrt{2}) : \mathbf{Q}$ is a simple extension.

Another example: extension $\mathbf{Q}(i, \sqrt{2}) : \mathbf{Q}$ is defined by two generators, but it is a simple extension. To see it consider the complex number

$$\theta = i + \sqrt{2} \tag{44}$$

It is evident that $\mathbf{Q}(\theta) \subseteq \mathbf{Q}(i, \sqrt{2})$ because $\theta \in \mathbf{Q}(i, \sqrt{2})$. Prove that $\mathbf{Q}(i\sqrt{2}) \subseteq \mathbf{Q}(\theta)$. We see that

$$\frac{1}{\theta} = \frac{\sqrt{2} - i}{3}$$

Hence

$$2\sqrt{2} = \theta + \frac{3}{\theta} \text{ and } \quad 2i = \theta - \frac{3}{\theta} \quad \text{i.e.} \quad \sqrt{2} \in \mathbf{Q}(\theta)\,, i \in \mathbf{Q}(\theta)\,, \mathbf{Q}(i\sqrt{2}) \subseteq \mathbf{Q}(\theta)\,. \tag{45}$$

Exercise Find a polynomial $p(x) \in \mathbf{Q}[x]$ such that $p(\theta) = 0$.

Remark Later we will see that this is true for a large class of extensions (See Theorem in the end of this Section about primitive element.)

Definition Simple extension $K(\alpha) : K$ is called simple algebraic extension if α is algebraic over K. Otherwise simple extension is called a transcendent extension.

Reminder If $L : K$ is an arbitrary field extension then a number $\alpha \in L$ is called algebraic over K if it is a root of non-trivial (non-zero) polynomial with coefficients in K. Otherwise it is called transcendent over K. The complex number is called an algebraic number if it is a root of non-trivial polynomial (or monic polynomial) over $\mathbf{Q}$. Otherwise it is called transcendental number.

Remark The polynomial is non-trivial if its degree is greater or equal to 0. The polynomial is trivial if all its coefficients are equal to zero, i.e. its degree is equal to $-\infty$. Monic polynomial is non-trivial. If a number α is a root of non-trivial polynomial $p(t) = a_n t^n + \cdots + a_0$ with $a_n \neq 0$ then it is a root of monic polynomial $\frac{p(t)}{a_n}$)

Now we classify simple extensions. Consider first two basic examples:

Example 1 Consider set of fractions $\left\{\frac{P(t)}{\mathbf{Q}(t)}\right\}$, where P, Q are arbitrary polynomials such that $Q \neq 0$. Two fractions $\frac{P}{\mathbf{Q}}$, $\frac{P'}{\mathbf{Q}'}$ are equal iff $PQ' \equiv P'Q$. One can naturally define addition and multiplication in this set. We come to the field $K(t)$ which is field of fractions of integer domain; in this case integer domain is the ring of polynomials $K[t]$.

All elements of the field $K(t)$ are generated by elements of initial field K and indeterminate t. This is simple extension $K(t) : K$ because indeterminate t is not algebraic over K: (Suppose t is algebraic and $P(t) \equiv 0$. Then P is zero polynomial.)

Before considering the next example formulate very important lemma:

Lemma *Let $p = p(t)$ be an irreducible polynomial over the field K. Let $I_p = (p)$ be an ideal generated by the polynomial p in the ring $K[t]$ of all polynomials over K (It is the set of all polynomials divisible on p: $I_p = (p) = \{f \colon f \in K[t], f = ph\}$. Then the quotient ring $K[t]/(p)$ is a field.*

Proof One can easy to define $+$ and $\times$ in the factor ring $K[t]/(p)$. To prove that a ring $K[t]/(p)$ is a field one has to prove that every equivalence class $[f]$ ($[f] = [f']$ if $f - f' = pg$) has inverse if $f \neq 0$. Without loss of generality suppose that f is coprime with p. (If no, then $f = hp + f'$ where

$[f'] = [f]$ and f' is coprime with p). Use now the technical lemma (31): there exist polynomials a, b such that $af + bp = 1$. Hence

$$[a][f] = [1] \quad \square \tag{46}$$

Now we are ready to consider the following example:

Example 2 let p be an irreducible non-trivial polynomial over K. Consider according the lemma above the field $K[t]\big/(p)$ This field is an extension of the field K by the element $\theta = [p]$.

E.g. if $p = t^2 - 2 \in \mathbf{Q}[t]$ then $\mathbf{Q}\big/(p)$ is isomorphic to $\mathbf{Q}(\sqrt{2})$

These two examples in fact exhaust all the cases of simple extensions:

Theorem 1 Every transcendental simple extension $K(\alpha) : K$ is isomorphic to the extension $K(t) : K$ where $K(t)$ is a field of fractions $\frac{P(t)}{Q(t)}$ of polynomials over K with indeterminate t. (Please, pay attention that ring of polynomials is denoted by $K[t]$ and the field of fractions by $K(t)$.)

Proof. Let α be an arbitrary transcendental (non-algebraic) number over K. Hence for any non-zero polynomial Q, $Q(\alpha) \neq 0$ and a number $\frac{P(\alpha)}{Q(\alpha)}$is well defined. There is one-one correspondence between all fractions $\frac{P(t)}{Q(t)}$ $(Q(t) \not\equiv 0)$ and elements $\frac{P(\alpha)}{Q(\alpha)}$. This is required isomorphism. For example consider an extension $Q(\pi) : Q$. Then the map $\frac{P(t)}{Q(t)} \to \frac{P(\pi)}{Q(\pi)}$ defines isomorphism of extensions. because transcendent number π cannot be a root of non-trivial polynomial over rationals.

Before formulating the next Theorem we introduce the notion of *minimum polynomial*. Let θ be an algebraic over K, i.e. there exists a non-trivial polynomial over K such that θ is its root $(K(\theta) : K$ is an algebraic extension).

In the set of all non-trivial polynomials over K which have θ as a root consider a monic polynomial $p \in K[t]$ of the *smallest degree* such that $p(\theta) = 0$. The polynomial p is called the *minimum polynomial* of θ over K.

If $p = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0, g = t^n + b_{n-1}t^{n-1} + \cdots + b_1 t + b_0$ are two *different* minimum polynomials then considering a polynomial $p - g = (a_{n-1} - b_{n-1})t^{n-1} + \cdots + (a_1 - b_1)t + (a_0 - b_0)$ one comes to monic polynomial of smaller degree. If polynomial p is reducible: $p = fg$ then θ is a root of one of polynomials f or g of smaller degree. *Hence minimum polynomial of algebraic number θ is defined uniquely and it is irreducible polynomial.*

Theorem 2

Simple algebraic extensions are produced by the irreducible polynomials.

Namely, let $K(\theta) : K$ be an algebraic extension and $p \in K[t]$ its minimum polynomial. Then the extension $K(\theta) : K$ is isomorphic to the quotient of the ring $K[t]$ by the ideal generated by the irreducible polynomial p:

$$K(\theta) : K \text{ is isomorphic to } \ K[t]/(p)$$

Two simple algebraic extensions $K(\theta_1) : K$, $K(\theta_2) : K$ are isomorphic if θ_1, θ_2 are roots of the same minimum polynomial.

Roots of irreducible polynomial are on an equal footing.

Remark Note that it is not TRUE that different irreducible polynomials in general produce different extensions. E.g. polynomials t^2-2 and t^2-2t-1 produce the same extension.

Example Consider the following four extensions of field of rationals:
a) $\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}$
b) $\mathbf{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}}) : \mathbf{Q}$
c) $\mathbf{Q}[t]/(t^3-2) : \mathbf{Q}$
d) $\mathbf{Q}(\sqrt[3]{7}) : \mathbf{Q}$

Extensions $a), b), c)$ are isomorphic, because $\sqrt[3]{2}$, $\sqrt[3]{2}e^{\frac{2\pi i}{3}}$ are roots of the same polynomial t^3-2 and this polynomial is irreducible over $\mathbf{Q}$ according to Eisenstein Test.

The extensions $\mathbf{Q}(\sqrt[3]{7}) : \mathbf{Q}$, $\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}$ are not isomorphic: To prove it suppose that σ is an isomorphism required. Then $\sigma(\sqrt[3]{7})^3 = \sigma(7) = 7$. On the other hand the equation $x^3 = 7$ has not solution in the field $\sqrt[3]{2}$. *Contradiction*

Counterexample; If $p = fg$ is reducible polynomial over $\mathbf{Q}[t]$ then $[f], [g] \neq 0$ in $K[t]/(p)$ but $[f] \cdot [g] = [p] = 0$. Hence $K[t]/(p)$ is not a field. moreover it is not an integral domain.

Example Let α be a root of cubic polynomial $x^3+x-1=0$. One can easily prove that this polynomial is irreducible. It is easy to see that this polynomial has only one real root $x_1 = \alpha$ and two conjugate complex roots $x_2 = \beta + i\gamma, x_3 = \beta - i\gamma$, because derivative $f' = 3x^2+1$ is positive function. All fields $\mathbf{Q}(x_1), \mathbf{Q}(x_2), \mathbf{Q}(x_3)$ are isomorphic to the field $\mathbf{Q}[x]/(x^3+x-1)$. The elements of the field $\mathbf{Q}[x]/(x^3+x-1)$ can be considered as polynomials $\{a+bx+cx^2\}$, where operations have to be factorized by ideal generated by the polynomial x^3+x-1. E,g.

$$(x^2+x)(x^2-x) \approx x - 2x^2\,, \tag{47}$$

because

$$[x^2+x][x^2-x]=[x^4-x^2]=[x\cdot x^3-x^2]=[x(1-x)-x^2]=[x-2x^2]$$

and

$$\frac{1}{x}\approx x^2+1 \tag{48}$$

These are just relations for roots for the polynomial x^3+x-1:

$$(\alpha^2+\alpha)(\alpha^2-\alpha)=\alpha-2\alpha^2\,,\qquad \frac{1}{\alpha}=\alpha^2+1$$

Using methods of the subsection "Highest common factor" one can express an arbitrary fraction as polynomial.

2.2 Degree of extension

If $L:K$ is a field extension it is worth considering L as a vector space over field K. In other words forget about multiplication of arbitrary elements in L. Consider in L operation addition and substraction for all elements but restrict multiplication to the case where one of the multipliers belongs to the subfield K (coefficients field). Thus we consider L as a vector space over K.

We come to very important invariant: *degree of an extension which is equal to the dimension of L considered as vector space over field K*:

$$[L:K]=deg(L:K)=\mathrm{dim}L_K \tag{49}$$

Theorem Let $K(\alpha):K$ be a simple extension. Then $[K(\alpha):K]=\infty$ if α is transcendental over K. If α is algebraic over K then $[K(\alpha):K]=n$, where n is a degree of minimum polynomial of α over K.

Proof. Consider "vectors" $\mathbf{e}_1=1$, $\mathbf{e}_2=[t]$, $\mathbf{e}_3=[t^2]$,...,$\mathbf{e}_n=[t^{n-1}]$. It follows from definition of minimum polynomial that these vectors consist a basis. ■

This is very workable theorem. E.g. to prove that degree of extension $\mathbf{Q}(\sqrt[7]{2}):\mathbf{Q}$ is equal to 7 we prove that polynomial x^7-2 is irreducible (one can do it using Eisenstein Test) hence this polynomial is minimum polynomial and due to Theorem degree of the extension is equal to 7.

Let K,M,L be fields such that $K\subseteq M\subseteq L$. One says that $K\subseteq M\subseteq L$ is a *Tower of field extensions.*

Theorem 2(Tower Law) If $K \subseteq M \subseteq L$ is a tower of field extensions then

$$[L : K] = [L : M] \cdot [M : K] \tag{50}$$

The proof is evident from definition. Let $\{\mathbf{e}\}_\mathbf{i}$ be a basis of L considered as a vector space over M (i.e. every element of L can be uniquely expressed as $\sum x^i \mathbf{e}_i$, where coefficients $x^i \in M$). Respectively let $\{\mathbf{f}\}_a$ be a basis of M considered as a vector space over K (i.e. every element of M can be uniquely expressed as $\sum a^i \mathbf{e}_i$, where coefficients $a^i \in K$). Then it can be easily proved that elements $\{\mathbf{e}_i \mathbf{f}_a\}$ consist a basis of L considered as a vector space over K. This proves (50).

Exercise 1 Prove that there is not any intermediate field in $\mathbf{Q}(\sqrt[p]{7}) : \mathbf{Q})$ which does not coincide with $\mathbf{Q}$ or $\mathbf{Q}(\sqrt[p]{7})$ if p is a prime number.

Solution follows immediately from Tower law.

Exercise 2. Prove that polynomial $f = x^4 + 6x + 2$ has no root in the field $\mathbf{Q}(\sqrt[5]{2})$.

Solution follows from Tower law: prove that polynomial f is irreducible. Hence degree of extension $\mathbf{Q}(\alpha) : \mathbf{Q}$ is equal to 4, where α is a root of f. On the other hand $[\mathbf{Q}(\sqrt[5]{2}) : \mathbf{Q}] = 5$

2.3 Algebraic extension

Extension $L : K$ is called algebraic if every element of L is algebraic over K.

Simple algebraic extension is finite extension by Theorem from previous subsection.

Algebraic extension can be generated by finite number of elements, but in general it is not the case (E.g. the algebraic closure of rationals (see later))

Theorem The field extension $L : K$ is finite iff this extension is algebraic finitely generated extension, i.e. $L : K$ is algebraic and there exist finitely many elements $\alpha_1, \ldots, \alpha_n$ such that $L = L(\alpha_1, \ldots, \alpha_k)$.

Proof:

Let $[L : K] < \infty$. Suppose $[L : K] = n$ and $\{e_1, \ldots, e_n\}$ be a basis of L considered as a linear space over K. Then $L = K(e_1, \ldots, e_n)$. Prove that every element $\alpha \in L$ (and in particularly elements e_i) is algebraic over K. Consider the set of elements $\{1, \alpha, \ldots, \alpha^n\}$. This set contains $n+1$ elements. The dimension of L considered as vector space over K is equal to n. Hence "vectors" $\{1, \alpha, \ldots, \alpha^n\}$ have to be linear dependent (considered as vectors in vector space L over K). Hence there exists a sequence $\{\gamma_1, \ldots, \gamma_n\}$ of coefficients belonging to K such that not all coefficients are equal to zero and $\gamma_1+\gamma_2\alpha+\gamma_3\alpha^2+\cdots+\gamma_{n+1}\alpha^n=0$. We see that α is a root of non-trivial polynomial. (If γ_r be the highest non-zero coefficient: $\gamma_r\neq 0$ and $\gamma_i=0$ for $i>r$ then α is a root of non-trivial polynomial $\gamma_r t^r+\cdots+\gamma_1 t+\gamma_0$)

To prove the inverse implication for the extension $K(\alpha_1,\ldots,\alpha_n)$ with $\{\alpha_1,\ldots,\alpha_n\}$ algebraic over K consider the "tower" of field extensions

$$K\subseteq K(\alpha_1)\subseteq K(\alpha_1,\alpha_2)\subseteq\cdots\subseteq K(\alpha_1,\ldots,\alpha_n)=L$$

Every extension in this tower is trivial or simple algebraic. Hence from the Tower Law it follows that $[L:K]<\infty$:

$$[L:K]=[K(\alpha_1,\ldots,\alpha_n):K(\alpha_1,\ldots,\alpha_{n-1})]\cdot[K(\alpha_1,\ldots,\alpha_{n-1}):K(\alpha_1,\ldots,\alpha_{n-2})]\cdot$$

$$\cdots\cdot[K(\alpha_1,\alpha_2):K(\alpha_1)]\cdot[K(\alpha_1:K]<\infty\,,$$

because degree of every extension $K(\alpha_1,\ldots,\alpha_r):K(\alpha_1,\ldots,\alpha_{r-1})]$ is finite. It is just the degree of algebraic number α_r over field $K(\alpha_1,\ldots,\alpha_{r-1})]$.

Use this Theorem to study the set of algebraic numbers, i.e. complex numbers which are roots of polynomials with rational coefficients.

Corollary The set of all algebraic numbers is a field.

Proof. Denote this set by $\mathbf{A}$: $\mathbf{Q}\subset\mathbf{A}\subset\mathbf{C}$.

One has to prove that for $\alpha,\beta\in\mathbf{A}$, $\alpha+\beta$, $\alpha\beta$ and $\frac{\alpha}{\beta}$, $(\beta\neq 0)$ belong to $\mathbf{A}$ also. The extensions $\mathbf{Q}(\alpha):\mathbf{Q}$ and $\mathbf{Q}(\alpha,\beta):\mathbf{Q}(\alpha)$ are finite because α and β are algebraic. From Tower Law it follows that field extension $\mathbf{Q}(\alpha,\beta):\mathbf{Q}$ is finite too. Hence by Theorem all elements of $\mathbf{Q}(\alpha,\beta)$ and in particular $\alpha+\beta$, $\alpha\beta$ and $\frac{\alpha}{\beta}$, $(\beta\neq 0)$ are algebraic. ■

The degree of extension $\mathbf{A}:\mathbf{Q}$ is equal to infinity. Indeed consider for arbitrary N a polynomial t^N-2. This polynomial is irreducible according to Eisenstein test (Apply Eisenstein test for $p=2$). Hence $[\mathbf{Q}(\alpha_N):\mathbf{Q}]=N$, where $\alpha_N=\sqrt[N]{2}$ is a root of polynomial t^N-2. $\mathbf{Q}(\alpha)$ is a subfield of $\mathbf{A}$. It proves that $\forall N\quad[\mathbf{A}:\mathbf{Q}]\geq\mathbf{N}$, hence $[\mathbf{A}:\mathbf{Q}]=\infty$.

The following exercise describes very important property of the field of algebraic numbers:

Exercise Prove that *the field of algebraic numbers is algebraically closed.* In other words we have to prove that every polynomial $p=A_0+A_1t+\cdots+A_nt^n$ with coefficients in algebraic numbers ($A_k\in\mathbf{A}$) has a root which is algebraic number too.

Solution follows immediately from Theorem above: *Let $p = A_0 + A_1 t + \cdots + A_n t^n$ where complex numbers A_i are algebraic. Let complex number θ be a root of this polynomial. Then extension $\mathbf{Q}(A_0, \ldots, A_n, \theta) : \mathbf{Q}(A_0, \ldots, A_n)$ is algebraic, hence it is finite. The extension $\mathbf{Q}(A_0, \ldots, A_n) : \mathbf{Q}$ is finite too, because all $A_0, \ldots, A_n$ are algebraic. Hence by Tower law extension $\mathbf{Q}(A_0, \ldots, A_n, \theta) : \mathbf{Q}$ is finite. Hence θ is algebraic over $\mathbf{Q}$* ■

This solution proves the existence of polynomial with rational coefficients.

One can give explicit construction of this polynomial:

explicit construction of polynomial for θ: Let algebraic number A_k $(k = 1, 2, \ldots, n)$ are roots of some polynomials $F_k \in \mathbf{Q}[x]$. Let $\{A^{i_k}\}$ is all set of roots of polynomial F_k. Then take polynomial $p = A_0 + A_1 t + \cdots + A_n x^n$ and put instead coefficient A_1 an arbitrary roots of polynomial F_1, put instead coefficients A_2 an arbitrary roots of polynomial F_2, put instead coefficient A_3 an arbitrary roots of polynomial F_3 and so on. Consider a polynomial:

$$\mathcal{P} = \prod_{i_0, i_2, i_3, \ldots, i_n} \left(A_0^{i_0} + A_1^{i_1} t + \cdots + A_n^{i_n} x^n \right) \tag{51}$$

where product goes over all roots of polynomials F_k. All coefficients of this polynomial are symmetric functions on roots. Hence they are rational. On the other hand θ is a root fo this polynomial because it is a root of polynomial p. We proved that θ is algebraic. Moreover we constructed polynomial over rationales such that θ is its root. ■

Remark One can consider analogously the set of algebraic numbers over arbitrary field K and prove that this set is a field and this field is algebraically closed over K.

2.4 Constructions by ruler and compasses I. Obstacles.

The notion of degrees of extension allows us to formulate very simple but powerful results which prove non-existence for solutions of very classic problems of constructing by ruler and compasses.

Note that by ruler and compasses we can "perform" operations " $+$ ", " $-$ ", " $\times$ ", " $:$ " and "$\sqrt{\ }$", i.e. solve linear and quadratic equations.

Namely take an arbitrary segment on the plane as a segment of unit length. Consider coordinate system attached to an arbitrary point (constructing two perpendicular lines). We come to Argand plane. One can see that every complex number $z = a + ib$ such that a, b are rationals or square roots of rationals can be constructed. Indeed if a, b are integers then to construct $a = n$ one have to take unit segment n times. To construct $a = m : n$ one has to construct an arbitrary angle $\angle ABC$ with vertex at the point B, then construct segments $BM = q$ and $MN = p$ on the ray BA and segment $BP = 1$ on the ray BC. Then construct line which passes through the point

N and is parallel to the line MP. Denote by Q the intersection of this line with ray BC. We have: $BM : MN = BP : PQ$. Hence $PQ = p : q$. Now show how to construct $\sqrt{n}$. Construct segment AKB (all three points on the one line) such that $AK = n, KB = 1$. Construct a middle point O of this segment ($AO = \frac{n+1}{2}$) and then construct the circle with centre at the point O and diameter $Ab = n + 1$. Construct segment KD such that KD is perpendicular to AB and the point D is on the circle. It is easy to see that

$$KD = \sqrt{AK \cdot KB} = \sqrt{n}$$

because $\angle DAb = 90^\circ$.

Example Divide a circle on five equal arcs, i.e. construct regular pentagon. It is suffice to construct an angle 72°. Use the fact that $\cos 72^\circ = \frac{\sqrt{5}-1}{4}$ (see Homework 1)

Any algorithm of constructing by ruler and compasses contains the following steps:

1) Take an arbitrary point (One can always assume that it is a point with rational coordinates)

2) Draw the line which passes through given two points.

3) Draw the circle with centre in the given point and a given radius.

4) Take a point which is an intersection of two lines (solution of linear equation)

5) Take a point which is an intersection of line and circle (solution of quadratic equation)

6) Take a point which is an intersection of two circles (solution of quadratic equation)

These considerations lead to the following

Theorem If a complex number α is constructible, i.e. it can be constructed by the ruler and compasses, then α is an algebraic number and degree of extension $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ is power of 2, $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^r$.

Proof of the Theorem. Let a number α is constructible. Then there exists an algorithm containing finite number of steps such that applying this algorithm we come to the number α.

It means that step by step (see above) we construct a sequence of numbers $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \ldots, \alpha_{n-2}, \alpha_{n-1}, \alpha_n\}$ such that

α_1 is a root of linear or quadratic polynomial with rational coefficients.

α_2 is a root of linear or quadratic polynomial with coefficients from the field $\mathbf{Q}(\alpha_1)$.
α_3 is a root of linear or quadratic polynomial with coefficients from the field $\mathbf{Q}(\alpha_1, \alpha_2)$.
α_4 is a root of linear or quadratic polynomial with coefficients from the field $\mathbf{Q}(\alpha_1, \alpha_2, \alpha_3)$.
. . . .
α_{n-1} is a root of linear or quadratic polynomial with coefficients from the field $\mathbf{Q}(\alpha_1, \dots, \alpha_{n-2})$.
α_n is a root of linear or quadratic polynomial with coefficients from the field $\mathbf{Q}(\alpha_1, \dots, \alpha_{n-1})$.

Consider tower of extensions

$$\mathbf{Q} \subseteq \mathbf{Q}(\alpha_1) \subseteq \mathbf{Q}(\alpha_1, \alpha_2) \subseteq \cdots \subseteq \mathbf{Q}(\alpha_1, \dots, \alpha_n) \tag{52}$$

We see that the degree of every extension in this tower is equal to one or two. Hence degree of extension $\mathbf{Q}(\alpha_1, \dots, \alpha_n) : \mathbf{Q}$ is equal to power of 2. Moreover if β be an arbitrary element in $\mathbf{Q}(\alpha_1, \dots, \alpha_n)$ then considering tower $\mathbf{Q} \subseteq \mathbf{Q}(\beta) \subseteq \mathbf{Q}(\alpha_1, \dots, \alpha_n)$ we come to conclusion that degree of the extension $\mathbf{Q}(\beta) : \mathbf{Q}$ is an exponent of 2.

The Theorem states necessary condition for a number α be constructive by ruler and compasses.

A question arises: is a condition that $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^r$ is sufficient? The answer is: "No" This condition is not sufficient.

Later we will show that the necessary and sufficient condition of constructibility is an existence of the tower (52) where all the extensions have degree ≤ 2. But nevertheless this Theorem gives very effective proof of non-existence of constructions.

Example It is impossible by ruler and compasses to trisect the angle $\angle ABC = 60^\circ$

Proof Suppose that it is possible. Thus a number $\alpha = \cos 20^\circ$ is constructible. But degree of extension $\mathbf{Q}(\alpha) : \mathbf{Q}$ is equal to three. Contradiction.

Example Given a segment $AB = a$ it is impossible by ruler and compasses to construct to construct a segment $CD = b$ such that $b^2 = \pi a^2$.

Proof. Suppose it is possible. Thus a number π is constructible. But π is a transcendent number and degree of extension $[\mathbf{Q}(\pi) : \mathbf{Q}]$ is equal to infinity. Contradiction.

2.5 Splitting field

Definition The field $\Sigma(f)$ is called a splitting field for a polynomial $f \in K[t]$ over K if $K \subseteq \Sigma$ and

1) f splits in $\Sigma(f)$, i.e. f has his all roots in $\Sigma(f)$ ($f = a(t-\alpha_1)\dots(t-\alpha_n)$)

2) The field $\Sigma(f)$ cannot be "decreased", i.e. if f splits over N such that $K \subseteq N \subseteq \Sigma(f)$ then $N = \Sigma(f)$.

The second condition is equivalent to the fact that $\Sigma = K(\alpha_1, \dots, \alpha_n)$

For example $\mathbf{Q}(e^{\frac{2i\pi}{5}})$ is a splitting field of polynomial $f = t^5 - 1$. Indeed it contains all the roots $x_0 = 1$, $x_1 = \varepsilon$, $x_2 = \varepsilon^2$, $x_3 = \varepsilon^3$, $x_4 = \varepsilon^4$, where $\varepsilon = e^{\frac{2\pi i}{5}}$ of this polynomial. On the other hand if f splits in $N \subseteq \Sigma(f)$, then $\varepsilon \in N$. Hence $\mathbf{Q}(\varepsilon) \subseteq N$. Hence $N = \mathbf{Q}(\varepsilon)$.

Another example: Splitting field of the polynomial $t^{12} - 1$ over $\mathbf{Q}$. Roots of this polynomial are numbers $\{e^{\frac{2\pi ik}{12}}\} = \{e^{\frac{\pi ik}{6}}\}$, $k = 0, 1, 2, \dots, 11$. One can prove that $\Sigma(f) = \mathbf{Q}(e^{\frac{i\pi}{6}}) = \mathbf{Q}(i, \sqrt{3})$, because $e^{\frac{i\pi}{6}} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$.

$\mathbf{Q}(\sqrt[3]{2})$ is not splitting field for polynomial $t^3 - 2$. It contains only one root of this polynomial. The splitting field $\Sigma(t^3 - 2) = \mathbf{Q}(\sqrt[3]{2}.i\sqrt{3})$.

Note that every polynomial over $\mathbf{Q}$ splits over $\mathbf{C}$. But $\mathbf{C}$ is very "large" to be a splitting field for polynomial. For every polynomial $f \in \mathbf{Q}[t]$ $\mathbf{C}$ contains a splitting field $\Sigma(f) = \mathbf{Q}(\alpha_1, \dots \alpha_n)$ where $\alpha_1, \dots \alpha_n$ are complex roots of the polynomial.

Example Calculate splitting field of polynomial $x^6 - 1$.

Solution: $x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$. it is easy to see that all roots are in the field $\mathbf{Q}(i\sqrt{3})$. Hence $\Sigma(x^6 - 1) = \mathbf{Q}(x_1, x_2, x_3, x_4, x_5, x_6) = \mathbf{Q}(i\sqrt{3})$.

Does splitting field always exists? At what extent is it unique?

Theorem For every polynomial $f \in K[t]$ there exists a splitting field. It is unique up to isomorphism.

Prove first the existence.

If $\partial f = 1$ then $\Sigma(f) = K$.

Suppose that the existence of splitting field is proved already for arbitrary field K and for arbitrary polynomial of degree $\leq k$. . Consider polynomial f of degree $k + 1$. Consider its arbitrary irreducible factor p: $f = pg$, where $p \in K[t]$ is irreducible over K.

The degree of p is less or equal to $k+1$. Adjoin the root α of the polynomial p to the field K, i.e. consider the field [9]

$$K(\alpha) = K[t]/(p(t)) = \{\text{the field of equivalence classses of polynomials:}\}$$

$$[h] = [h'] \quad \text{iff} \quad p|h-h'\,, \quad \text{i.e.} h-h' = p\cdot g\,. \tag{53}$$

Now we have that polynomial p and polynomial f has at least one root in the field $K(\alpha)$ (53).

Hence irreducible factor of polynomial f in this field is less or equal to k:

$$f = (t-\alpha)f' = (t-\alpha)\cdot\frac{f(t)}{t-\alpha}$$

Hence by inductive hypothesis there exists a splitting field $\Sigma(f')$ for a polynomial f' considered as polynomial over field $K(\alpha)$. This will be a splitting field over a field K too.

The uniqueness of splitting field (up to an isomorphism) follows from

Lemma Let ι be an isomorphism of fields K and K', $f\in K[t]$, $\Sigma(f)$ be a splitting field for polynomial f and T be a field such that polynomial $f' = \iota(f)$ splits over T (i.e. T contains a splitting field).

Then there exist a monomorphism $\hat{\iota}$ of field $\Sigma(f)$ into a field T such that $\hat{\iota}\big|_K = \iota$:

$$\begin{tikzcd}
\Sigma(f) \arrow[r, "\hat{i}"] & T \\
K \arrow[u] \arrow[r, leftrightarrow, "i"] & K' \arrow[u]
\end{tikzcd} \tag{54}$$

Corollary If $\Sigma(f)$ is a splitting field for polynomial $f\in K[t]$, ι is isomorphism of fields K and K' and $\Sigma'(f')$ is a splitting field for polynomial $f' = i(f)\in K[t]$ then $\Sigma(f)$ is isomorphic to $\Sigma(f)$.

Before going to very important notion of *normal extension* it is instructive to analyze in detail splitting field for cubic polynomial with rational coefficients.

2.6 Splitting field for cubic polynomial with rational coefficients.

Let $f = x^3 + ax^2 + px + c$ be cubic polynomial with rational coefficients.

[9] In other words the field $K(\alpha) = K[t]/(p(t))$ can be viewed as a field of polynomials of degree less or equal to the $r-1$ (where r is a degree of polynomial p. The root α can be viewed as equivalence class of polynomial t. $\alpha = [t]$.(See (47))

There are two cases

I) f is irreducible (over $\mathbf{Q}$)
II) f is reducible (over $\mathbf{Q}$).

First consider trivial case II. Polynomial $f = x^3 + ax^2 + px + c = (x - r)g$ has one rational root. Here $g = x^2 + px + q, r \in Q$ There are two subcases:

IIa) f is reducible and g is irreducible (over $\mathbf{Q}$)
IIb) f is reducible and g is reducible(over $\mathbf{Q}$).

Case IIb: $f = (x - r_1)(x - r_2)(x - r_3)$ all roots are rational and splitting field $\Sigma(f)$ is equal to $\mathbf{Q}$ itself.
In the case IIb) the degree of splitting field (the degree of field extension $\Sigma(f) : \mathbf{Q}$) is equal to 1.
Case IIa: $f = (x - r)(x^2 + px + q) = (x - r_1)(x - \alpha_1)(x - \alpha_2)$ one root is rational two other roots belong to quadratic extension ($\alpha_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p}{2}^2 - q}$).
Splitting field $\Sigma(f)$ is equal to $\mathbf{Q}\left(\sqrt{\frac{p}{2}^2 - q}\right)$,
In the case IIa) the degree of splitting field (the degree of field extension $\Sigma(f) : \mathbf{Q}$) is equal to 2.

Now return to most interesting case I when polynomial is irreducible over $\mathbf{Q}$. In this case all three roots x_1, x_2, x_3 of the polynomial are not rational numbers. It is easy to see that or all three roots are real or one root is real and other two roots are complex conjugated.

All fields extensions $\mathbf{Q}(x_1) : \mathbf{Q}, \mathbf{Q}(x_2) : \mathbf{Q}, \mathbf{Q}(x_3) : \mathbf{Q}$ are isomorphic but in general they are different fields. E.g. for polynomial $f = x^3 - 2$, $\mathbf{Q}(x_1)$ is subfield of $\mathbf{R}$, $\mathbf{Q}(x_2)$, $\mathbf{Q}(x_3)$ are not subfields of $\mathbf{R}$.

Without loss of generality consider $\mathbf{Q}(x_1)$. There are two possibilities: x_2 **belongs** to $\mathbf{Q}(x_1)$ or x_2 **does not belong** to $\mathbf{Q}(x_1)$.

Note that x_2, x_3 are roots of quadratic equation with coefficients over $\mathbf{Q}(x_1)$. Hence x_3 belongs to $\mathbf{Q}(x_1)$ if and only if x_2 belongs to $\mathbf{Q}(x_1)$. We come to the following two subcases:

Ia) f is irreducible. $x_2, x_3 \in \mathbf{Q}(x_1)$, i.e. all roots are rationally expressed via x_1. Splitting field $\Sigma(f)$ is just $\mathbf{Q}(x_1) = \mathbf{Q}(x_2) = \mathbf{Q}(x_3)$.
The degree of splitting field (the degree of field extension $\Sigma(f) : \mathbf{Q}$) is equal to 3.

Ib) f is irreducible. $x_2, x_3 \notin \mathbf{Q}(x_1)$, i.e. roots x_2, x_3 are **not** rationally expressed via x_1. Splitting field $\Sigma(f) = \mathbf{Q}(x_1, x_2, x_3) \neq \mathbf{Q}(x_1)$.

$\mathbf{Q}(x_1) \neq \mathbf{Q}(x_2) \neq \mathbf{Q}(x_3)$ in spite of the fact that these fields are isomorphic.
The degree of splitting field (the degree of field extension $\Sigma(f) : \mathbf{Q}$) is equal to $6 = 3 \times 2$.

The example for the case Ia is the "famous" polynomial $x^3 - 3x - 1$. It has roots $x_1 = 2\cos 20°$, $x_2 = 2\cos 140° = -2\cos 40°$ $x_3 = 2\cos 240° = -2\cos 80°$. It is easy to see (using formula $\cos 2\varphi = 2\cos^2\varphi - 1$) that

$$x_2^2 = 2 - x_1^2, \qquad x_3^2 = 2 - x_2^2$$

are related with each other by rational transformation

An example for the case Ib) is the polynomial $x^3 - 2$.

How to distinguish between these two subcases when irreducible polynomial has all three roots rational expressable via each other or not? The answer is following:
discriminant $D = d^2 = [(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)]^2$ of irreducible cubic polynomial is square of rational if and only if $\mathbf{Q}(x_1) = \mathbf{Q}(x_2) = \mathbf{Q}(x_3)$.

E.g. for irreducible cubic polynomial $x^3 - 3x - 1$ $D = -4p^3 - 27q^2 = 81 = 9^2$, for irreducible polynomial $x^3 - 2$ $D = -4p^3 - 27q^2 = -108$. The fact that discriminant of irreducible polynomial is square of rational if $\mathbf{Q}(x_1) = \mathbf{Q}(x_2) = \mathbf{Q}(x_3)$ follows immediately from the Tower low. Inverse implication follows from Galois Fundamental Theorem: see in details the subsection **Galois group for cubic polynomial** in section 3. (Alternative "elementary" proof of inverse implication see in the Appendix A)

Note also that if square root of Discriminant is rational and cubic polynomial is not reducible then at least one root is rational, hence due to Vèta Theorem all roots are rational.

2.7 Normal extension

Definition The field extension $L : K$ is called normal extension if every irreducible polynomial $f \in K[t]$ which has at least one zero in L splits in L.

In other words extension $L : K$ is normal if for arbitrary irreducible polynomial $f \in K[t]$ the following condition holds:

If this polynomial has at least one root in L then it has all its roots in L:

One out, all out

Examples

1. The extension $\mathbf{Q}(\sqrt{5}) : \mathbf{Q}$ is a normal extension. Prove it: Let p be irreducible polynomial which contains one root x_1 in this field. The degree of the extension $\mathbf{Q}(\sqrt{5}) : \mathbf{Q}$ is equal to 2. Hence the degree of the polynomial p is equal 1 or 2. If it is "1" nothing to prove. If it is "2" then $p = t^2 + bt + c$ the second root of the polynomial have to belong to the field because $x_1 x_2 = c, x_1 + x_2 = -p$.

Note that we can prove analogously that every extension of degree 2 has to be normal.

2. Extension $\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}$ is not normal extension. It contains one and only one root of polynomial $t^3 - 2$. (Other roots are not real numbers.)

Theorem A finite extension $N : K$ is normal extension if and only if N is a splitting field for some polynomial with coefficients in K.

Proof of the Theorem

First prove that N is splitting field for a polynomial.

Let $N : K$ be a finite normal extension. Then by the theorem on finite extensions (see subsection Algebraic extension) N is finitely generated algebraical extension: $N = K(\alpha_1, \ldots, a_n)$ where all elements of N including $\alpha_1, \ldots a_n$ are algebraic over K.

Consider polynomials $g_1, g_2, \ldots, g_n$ such that g_1 is the minimum polynomial over K of the element α_1, g_2 is the minimum polynomial over K of the element α_2, g_3 is the minimum polynomial over K of the element α_3... g_n is the minimum polynomial over K of the element α_n.

Consider polynomial $F = g_1 \cdot g_2 \cdot \ldots \cdot g_n$. N is a normal extension, hence all polynomials $\{g_1, g_2, \ldots, g_n\}$ *have all their roots in* N because they have at least one root in N ($g_k(\alpha_k) = 0$). Hence polynomial F splits over N. On other hand if F splits over N' such that $K \subseteq N' \subseteq N$ then $\alpha_k \in N$;, hence $N' = N$. This proves that N is splitting field for polynomial F.

Now we give the sketch of proof of inverse implication [10].

The proof of the fact that for arbitrary polynomial $f \in K[t]$ the extension $\Sigma(f) : K$ is a normal extension is founded on the following. Let g be polynomial irreducible over K

[10] This is not necessary for exam.

with a root $\alpha \in \Sigma(f)$. Consider isomorphic fields $K(\alpha)$, $K(\beta)$ and construct step by step splitting fields $\Sigma(f)$, $\Sigma'(f)$ over $K(\alpha)$ and $K(\beta)$ respectively. The roots $\{x_1, x_2, \dots, x_n\}$ of polynomial f will be adjoined to the field $K(\alpha)$ and the roots of the same polynomial but in the different order $\{x_{i_1}, x_{i_2}, \dots, x_{i_n}\}$ will be adjoined to the field $K(\beta)$. Hence if α is rationally expressed via roots of f, i.e. α belongs to the splitting field then β is rationally expressed via roots also, i.e. β belongs to splitting field too.

We want to emphasize the fact that Theorem states that splitting field of a given polynomial contains all roots or no roots of arbitrary polynomial. For example let x_1, x_2, x_3 be roots of cubic polynomial $f \in \mathbf{Q}[x]$, $\theta = x_1 - x_2$ and R be minimum polynomial of θ. Polynomial R has N roots $\theta = \theta_1, \theta_2, \dots, \theta_N$. (In general $N = \partial R$ could be equal 1 (if all roots of f are rational), 2 (if only one root of f is rational), 3 (e.g. for equation $x^3 - 3x - 1$) and 6 (e.g. for $f = x^3 - 2$) (see previous subsection)

The Theorem states that not only θ but all other roots of R belong to $\Sigma(f)$ too.

This Theorem is very important in applications.

Example 1 Consider extension $\mathbf{Q}(\varepsilon) : \mathbf{Q}$ where $\varepsilon = e^{\frac{2\pi i}{p}}$ where p is arbitrary prime number. The easiest way to see that this extension is normal it is to use Theorem. $\mathbf{Q}(\varepsilon)$ is a splitting field of polynomial $t^p - 1$. (Roots of the polynomial $t^p - 1$ are $\{1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \dots, \varepsilon^{p-1}\}$) Hence it follows form Theorem that an extension $\mathbf{Q}(\varepsilon) : \mathbf{Q}$ is normal extension.

Example 2 We considered above extension $\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}$ which was not normal extension. On the other hand an extension $\mathbf{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbf{Q}$ is normal extension. One can easy check that this extension is a splitting field of the polynomial $t^3 - 2$. (Show it!)

2.8 Separable polynomials

Definition The polynomial is called separable if it has no multiple zeros in the splitting field.
The element $\theta \in L$ is called separable over subfield K if minimum polynomial of θ is separable over K.
An algebraic extension $L : K$ is called separable if every element in L is separable over K.

Consider arbitrary irreducible polynomial $p = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ over field K. Suppose that *it is not separable.* Consider its derivative, polynomial $Dp = nt^{n-1} + (n-1)a_{n-1}t^{n-2} + \cdots + a_1$. Polynomials p, Dp have trivial highest common factor because p is irreducible and degree of Dp is less that degree of p. Hence $Dp \equiv 0$. This is possible only if characteristic of the field K is not equal to 0. We come to

Theorem Every irreducible polynomial over field of characteristic 0 is separable.

Note that if L is separable over K then L is separable over arbitrary intermediate subfield M because minimum polynomial of every element over M divides minimum polynomial of this element over K.

2.9 Theorem on primitive element

In this subsection we consider finite separable extension, i.e. extensions by separable elements. These extensions are in fact simple extensions.

Theorem If $L : K$ is finite separable extension of the field K then it is simple extension, i.e. there exists θ such that $L = K(\theta)$

An element θ is called *primitive element* of the extension.

The Theorem follows from Lemma

Lemma If $K(\alpha, \beta)$ is algebraic extension and β is separable then there exists $\theta \in K(\alpha, \beta)$ such that $K(\theta) = K(\alpha, \beta)$

Indeed if $L : K$ is finite extension then $L = K(\beta_1, \dots, \beta_n)$ where all β_i are algebraic over K. Applying lemma to the tower of extensions $K \subseteq K(\beta_1, \beta_2) \subseteq \dots \subseteq L$ we come to a primite of the extension $L : K$.

If K is field of characteristic 0 then it follows from the Theorem of the previous subsection the following working case of the Theorem:

Theorem′ Every finite extension of the field of characteristic 0 is simple algebraic extension.

We give here the proof of the lemma in the case if K is infinite field. (E.g. for field of characteristic zero) Let f, g be minimum polynomials of α, β respectively. Consider a field such that $K \subseteq K(\alpha, \beta) \subset \Sigma$ where all roots of polynomials f, g are present. (E.g. $\Sigma = \Sigma(gf)$). Let $\{\alpha_i\}$, $\{\beta_k\}$ be roots of polynomials f, g Suppose that $\alpha = \alpha_1, \beta = \beta_1$.

Now consider

$$\theta = \alpha + c\beta \,, \tag{55}$$

where c is an arbitrary coefficient from field K which obey the following condition:

$$c \neq \frac{\alpha_1 - \alpha_i}{\beta_m - \beta_1} \,, m \neq 1 \,, \quad \text{and} \, i \text{ is arbitrary} \tag{56}$$

We can do it because g is separable polynomial $\beta_m \neq \beta_i$ if $m \neq i$ and K is infinite field. Hence one can always choose c obeying condition above. Note also that in particularly $c \neq 0$)

Consider polynomials $g(x)$, $\tilde{f}(x) = f(\theta - cx)$. These polynomials are polynomials over the field $K(\theta)$. It is easy to see using (56) that these polynomials have one and only one general root $\beta = \beta_1$. Hence their highest common divisor is equal to $(x - \beta_1)$. On the other hand general common divisor is polynomial in $K(\theta)[t]$. Hence $\beta \in K(\theta)$ and obviously $\alpha = \theta + c\beta \in K(\theta)$. Hence $K(\alpha, \beta) \subseteq K(\theta)$. On the other hand according to (55) $K(\theta) \subseteq K(\alpha, \beta)$. Hence $K(\alpha, \beta) = K(\theta)$. ■

Consider two examples.

Example 1 Find primitive element of field extension $\mathbf{Q}(i, \sqrt{2}) : \mathbf{Q}$. We did it by "bare hands" (see subsection "Simple extensions") and proved that i and $\sqrt{2}$ are rational functions of $\theta = \sqrt{2} + i$ (see (45)), i.e. $\mathbf{Q}(i + \sqrt{2}) = \mathbf{Q}(i, \sqrt{2})$. Repeat these calculations using technique which was used above in the proof of the lemma above. Consider polynomials $g = x^2 + 1, f = x^2 - 2$. $\Sigma(fg) = \mathbf{Q}(\sqrt{2}, i)$. It is easy to see that polynomials $g = x^2 + 1$ and $\tilde{f} = f(\theta - x) = (\sqrt{2} + i - x)^2 - 2$ have one and only one general root. It is $x = i$. Hence $x = i$ has to be the root of $\tilde{f} - g$ ($x - i$ is common divisor of $\tilde{f}$, g). $\tilde{f} - g = (\theta - x)^2 - 2 - x^2 - 1 = \theta^2 - 2\theta x - 3$. Hence $x = i = \frac{3-\theta^2}{2\theta}$. It is easy to see that we come to (45).

Another more serious example

Example 2 Consider polynomial $f = x^3 - 2$ over $\mathbf{Q}$. Its splitting field

$$\Sigma(x^3 - 2) = \mathbf{Q}(x_1, x_2, x_3)\,, \quad x_1 = \sqrt[3]{2}\,, x_2 = \sqrt[3]{2}e^{\frac{2\pi i}{3}}\,, x_3 = \sqrt[3]{2}e^{\frac{-2\pi i}{3}}\,. \tag{57}$$

$$x_1 = \sqrt[3]{2}\,, x_{2,3} = \sqrt[3]{2}e^{\frac{\pm 2\pi i}{3}} = \sqrt[3]{2}\left(-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right)\,,$$

$$\Sigma(x^3 - 2) = \mathbf{Q}(x_1, x_2, x_3) = \mathbf{Q}(\sqrt[3]{2}, i\sqrt{3})\,.$$

($\mathbf{Q}(x_1, x_2, x_3) = \mathbf{Q}(\sqrt[3]{2}, i\sqrt{3})$ because roots can be rationally expressed via $\sqrt[3]{2}, i\sqrt{3}$ and on the other hand number $\sqrt[3]{2}, i\sqrt{3}$ can be rationally expressed via roots: $\sqrt[3]{2} = x_1, i\sqrt{3} = \frac{x_2+x_3}{x_1}$)

Find primitive element of this extension, i.e. θ such that $\mathbf{Q}(\theta) = \Sigma(x^3 - 2) = \mathbf{Q}(\sqrt[3]{2}, i\sqrt{3})$.

$$\theta = x_2 - x_3 = i\sqrt{3}\sqrt[3]{2}\,.$$

One can easy to prove that it is primitive: $\theta^2 = -3\sqrt[3]{4} = -\frac{6}{\sqrt[3]{2}}$. Hence $\sqrt[3]{2} = -\frac{6}{\theta^2}$ and $i\sqrt{3} = -\frac{\theta^3}{6}$, i.e.

$$x_1 = -\frac{6}{\theta^2},\ x_{2,3} = -\frac{6}{\theta^2}\left(-\frac{1}{2} \pm \frac{\theta^3}{12}\right) = \frac{3}{\theta^2} \pm \frac{\theta}{2} \tag{58}$$

We have $\theta^6 = -108$, i.e. θ is a root of the polynomial $t^6 + 108 = 0$. It is easy to see that this is the minimum polynomial of θ, i.e. degree of the extension is equal to 6. Indeed consider two towers: $\mathbf{Q} \subseteq \mathbf{Q}(i\sqrt{3}) \subseteq \mathbf{Q}(\theta)$ and $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{2}) \subseteq \mathbf{Q}(\theta)$. From the first tower it follows that 2 divides $[\mathbf{Q}(\theta) : \mathbf{Q}]$. From the second Tower it follows that 3 divides $[\mathbf{Q}(\theta) : \mathbf{Q}]$. Hence 6 divides $[\mathbf{Q}(\theta) : \mathbf{Q}]$. On the other hand θ is a root of polynomial $t^6 + 108$. Hence $[\mathbf{Q}(\theta) : \mathbf{Q}] = 6$ and $t^6 + 108$ is its minimum polynomial.

One can see that θ is primitive this mimicking the proof of the lemma using relations (55), (56), i.e. using general method: *Polynomials* $x^3 - 2, (\theta + x)^2 - 2$ *have one and only one general root. This is* x_3: $x_3^3 - 2 = 0$, $(\theta + x_3)^3 - 2 = x_2^3 - 2 = 0$ (Compare with previous section). Hence their highest common divisor is equal to $x - x_3 = x - \sqrt[3]{2}e^{\frac{-2\pi i}{3}}$. On the other hand it belongs to the field $\mathbf{Q}(\theta)$: it is $x - f(\theta)$, where $f(\theta)$ is element in $\mathbf{Q}(\theta)$. Thus x_2 and x_3 belong to $\mathbf{Q}(\theta)$ also.

Calculate explicitly $f(\theta)$ by calculating highest common divisor. Applying Euclidian algorithm (see (30), (35)) we will see that highest common divisor is $x + \frac{\theta}{2} - \frac{3}{\theta^2}$. Hence

$$x + \frac{\theta}{2} - \frac{3}{\theta^2} = x - x_3\,, \tag{59}$$

$$x_3 = \frac{3}{\theta^2} - \frac{\theta}{2}\,. \tag{60}$$

Now it is easy to express $x_2 = \theta + x_3$ and $x_1 = -x_2 - x_3$ in terms of θ:

$$x_1 = \frac{\theta^4}{18}\,, x_{2,3} = \frac{\theta}{2} \pm \frac{3}{\theta^2} = \frac{\theta}{2} \pm \frac{\theta^4}{36}\,, \tag{61}$$

because $\theta^6 = -108$. (Compare with (58)) We express roots x_1, x_2, x_3 as rational functions of primitive element θ.

3 Galois group. Galois correspondence between intermediate groups and subgroups of Galois group. Fundamental Theorem of Galois Theory

Let $L : K$ be a field extension. A group of automorphisms of field L which are identical on K is called Galois group of field extension. We denote this group by $\Gamma(L : K)$.

Remark In the case $K = \mathbf{Q}$ every automorphism is automatically $\mathbf{Q}$-aitomorphism. So in this case Galois group $L : \mathbf{Q}$ is nothing but group of all automorphisms of L.

Very simple examples:

Exercise 1 Calculate Galois group of $\mathbf{C} : \mathbf{R}$. Answer: $\{\mathbf{id}, \sigma\}$, where $\sigma(a+bi) = a-bi$, $a, b \in R$, i.e. $\sigma(z) = \bar{z}$ is complex conjugation for complex numbers z.

Indeed it is easy to check that $\{\mathbf{id}, \sigma\}$ is a group of $\mathbf{R}$-automorphism: $\sigma^2 = \mathbf{id}$ and:

$$\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2,\ \overline{(az_1 + bz_2)} = a\bar{z}_1 + b\bar{z}_2, \text{for every } a, b \in \mathbf{R} \tag{62}$$

On the other hand if φ is an arbitrary $\mathbf{R}$-automorphism, i.e. automorphism which is identical on $\mathbf{R}$ and $\varphi(i) = x$, then $\varphi(i^2) = \varphi(-1) = -1$. $x^2 = -1$. Hence $\varphi(i) = x = \pm i$ and $\varphi(a+bi) = a \pm bi$. Thus φ is equal to $\mathbf{id}$ or to σ. We proved that Galois group $\Gamma(\mathbf{C} : \mathbf{R}) = \{\mathbf{id}, \sigma\}$ possesses two elements: identical transformation and complex conjugation.

Exercise 2 Calculate Galois group of $\mathbf{Q}(\sqrt{2}) : \mathbf{Q}$

(answer: $\{\mathbf{id}, \sigma\}$, where $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$, $a, b \in \mathbf{Q}$) This can be proved in the similar way as above (Do it!)

Exercise 3 Calculate Galois group of $\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}$

(answer: $\{\mathbf{id}\}$, because an equation $x^3 - 2 = 0$ has unique root in $\mathbf{R}$: If $\sigma(x) = y$, then $x = y$ because $y^3 - 2 = \sigma(x^3 - 2) = 0$)

Exercise 3 Calculate Galois group of $\mathbf{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}}) : \mathbf{Q}$

(answer: $\{\mathbf{id}\}$, because an extension $\mathbf{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}}) : \mathbf{Q}$ is isomorphic to the extension $\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}$ considered in the previous example.

Exercise* 4. Calculate Galois group of $\mathbf{R} : \mathbf{Q}$.

Surprisingly the answer is $\{\mathbf{id}\}$: in the other words there is no any automorphisms of $\mathbf{R}$ except an identical one!

3.1 Galois group of polynomials

Let $f \in K[t]$ be polynomial over field K and $L = \Sigma(f)$ be its splitting field. Then $L : K$ will be a **normal** field extension. (See the Theorem in subsection "Normal extension").

Let $\{x_1, \dots, x_n\}$ be roots of the polynomial f. Consider Galois group of field extension $\Sigma(f) : K$. Sometimes we call Galois group $\Gamma(\Sigma(f) : K)$ as a Galois group of polynomial f and we denote it shortly by $\Gamma(f)$.

In the case if f is polynomial with rational coefficients, $f \in \mathbf{Q}[t]$ then Galois group of polynomial $\Gamma(f)$ is Galois group of field extension $\Sigma(f) : \mathbf{Q}$. It is just group of automorphisms of splitting field $\Sigma(f)$, because as it was mentioned above every automorphism is $\mathbf{Q}$-automorphism. and $L = \Sigma(f)$ its splitting field.

Now a simple but important statement

There is one-one correspondence between elements of Galois group and subgroup of group of permutations of roots of polynomial.

Let $f \in K[t]$ be a polynomial, and $x_1, x_2, \dots, x_n$ be roots of this polynomial in splitting field $\Sigma(f)$. Consider a group S_n of permutations of all roots. It is evident that $|S_n| = n!$. It is easy to see that every Galois automorphism defines permutation of the roots. Indeed let $f = t^n + a_{n-1}t^{n-1} + \dots + a_1 t + a_0$ be a polynomial over K and $\sigma \in \Gamma(f)$, be Galois automorphism of $\Sigma(f)$, i.e. σ is automorphism of $\Sigma(f)$ which is identical on K. Consider an arbitrary root x_i of polynomial f. Suppose $\sigma(x_i) = y$. Prove that y is a root of f too (may be the same may be another), i.e. $y = x_j$. Indeed for every root x_i of the polynomial f

$$0 = f(x_i) = x_i^n + a_{n-1}x_i^{n-1} + \dots + a_1 x_i + a_0 \,. \tag{63}$$

Apply K- automorphism σ to the left hand side and right hand side of this expression. We come to

$$\begin{aligned} 0 = \sigma(f(x_i)) &= \sigma(x_i^n + a_{n-1}x_i^{n-1} + \dots + a_1 x_i + a_0) \\ &= y^n + a_{n-1}y^{n-1} + \dots + a_1 y + a_0 = 0 \,. \end{aligned} \tag{64}$$

Hence y is also a root of the polynomial f.

(The same is the special case of polynomials with coefficients in $\mathbf{Q}$ every automorphism of splitting field $\Sigma(f)$ over $\mathbf{Q}$ does not change rational coefficients of polynomials. Hence it transforms a root to a root.)

On the other hand if g is Galois transformation of the splitting field $\Sigma(f)$ which is identical on roots: $g(x_i) = x_i$, then this transformation is identical on whole splitting field since every element of splitting field is rational function of elements of field K and roots $x_1, \ldots, x_n$

We see that **There is monomorphism of Galois group in the group of permutations of roots**

We can identify

Galois group of polynomial with a subgroup of group of permutations of roots,

i.e. every Galois automorphism of $\Sigma(f)$permutes roots of the polynomial f. E.g. the Galois group $\Gamma(f)$ of a polynomial f over $\mathbf{Q}$ is the Galois group of the extension $\Sigma : \mathbf{Q}$, where Σ is a splitting field of f over $\mathbf{Q}$. One can take Σ as the subfield of $\mathbf{C}$ generated by the roots of the polynomial f. Every $\mathbf{Q}$-isomorphism (in fact every automorphism, because every automorphism is automatically $\mathbf{Q}$-automorphism) does not change f and transforms zero of f into a zero of f. Distinct elements of $\Gamma(f)$ induce distinct permutations. Hence there is a group monomorphism of $\Gamma(f)$ into the group of all permutations of the zeros of f.

It is natural to ask a question: Is it right that every permutation of roots is necessarily generated by some Galois transformation. NO!!!

Consider examples.

Example (naive example) Consider polynomial $f = x^3 - 3x - 18$ It is reducible cubic polynomial, It has roots $x_1 = 3, x_{2,3} = \frac{3 \pm i\sqrt{15}}{2}$. It is evident that a splitting field is equal to $\mathbf{Q}(i\sqrt{15})$ and Galois automorphism is generated by transformation $i\sqrt{15} \to -i\sqrt{15}$ (Every number $z \in \Sigma(f = x^3 - 3x - 18) = \mathbf{Q}(i\sqrt{15})$, $z = p + iq\sqrt{15} \to p - iq\sqrt{15}$). Hence Galois automorphism permutes roots x_2, x_3. But Galois automorphism *cannot move the root* $x_1 = 3$ because Galois automorphism is identical on rational numbers.

Example Consider polynomial $f = x^4 - 5x^2 + 6$. It is easy to see that $f = (x^2 - 2)(x^2 - 3)$. Hence roots are equal to $x_{1,2} = \pm\sqrt{2}$, $x_{3,4} = \pm\sqrt{3}$. Hence $\Sigma(f) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. Group of permutations of roots has $4! = 24$ elements but Galois group possesses 4 elements: $\{1, \tau, \sigma, \tau\sigma\}$, where $\tau(\sqrt{2}) = -\sqrt{2}, \tau(\sqrt{3}) = \sqrt{3}$, $\sigma(\sqrt{2}) = \sqrt{2}, \sigma(\sqrt{3}) = -\sqrt{3}$. (See in details in (149)and 3-rd example in the subsection 3.8)

More interesting example:

Example Consider "glorious" polynomial $x^3 - 3x - 1$. Its roots are $x_1 = 2\cos 20°, x_2 = -2\cos 40°, x_2 = -2\cos 80°$. Here the situation is more interesting: All roots are irrational, because polynomial $x^3 - 3x - 1$ is irreducible. But if Galois transformation transforms x_1 to x_2 then x_2 **has to be transformed** to x_3. Indeed $\cos 40^\circ = 2\cos^2 20^\circ - 1, \cos 80^\circ = 2\cos^2 40^\circ - 1$. Hence

$$x_2 = 2 - x_1^2. \ if \quad \sigma(x_1) = x_2, \quad \text{then} \tag{65}$$

$$\sigma(x_2) = \sigma(2 - x_1^2) = 2 - \sigma(x_1)\sigma(x_1) = 2 - x_2^2 = x_3^2. \tag{66}$$

More formally $\mathbf{Q}(x_1) = \mathbf{Q}(x_2) = \mathbf{Q}(x_3)$. Every root is primitive element of field extension. Hence roots are rationally expressed via each other. Galois group is cyclic group containing three elements: $\mathbf{id}, \sigma, \sigma^2$, where $\sigma(x_1) = x_2, \sigma(x_2) = x_3, \sigma(x_3) = x_1$. [11]

Example Polynomial $x^p - 1$.

First consider the case if p is prime. Splitting field of this polynomial is $\mathbf{Q}(\varepsilon)$ where $\varepsilon = e^{\frac{2\pi i}{p}}$ All roots of polynomial are $\{1, \varepsilon, \varepsilon^2, \varepsilon^3, \ldots, \varepsilon^{p-1}\}$. Galois automorphisms σ_k $(k = 1, 2, 3, \ldots)$ are defined by condition

$$\sigma_k(\varepsilon) = \varepsilon^k, (k = 1, 2, \ldots, p - 1) \tag{67}$$

Indeed this condition defines transformation of every root. Galois group contains $p - 1$ elements $\sigma_1, \ldots, \sigma_{p-1}$. It is just the degree of the extension $\Sigma(x^p - 1) : \mathbf{Q}$. ($x^p - 1 = (x - 1)\frac{x^p - 1}{x - 1}$. Polynomial $\frac{x^p-1}{x-1} = 1 + x + x^2 + x^3 + \cdots + x^{p-1}$ is irreducible polynomial of degree $p-1$) For equation $x^p - 1$ Galois group is subgroup of $p - 1$ elements in the group of permutations. (Group of all permutations of roots contains $p!$ elements.)

You ask a question: where you used a fact that p is prime? In the case if p is not prime then the automorphism (67) is not well-defined. E.g. for $p = 6$ roots are $1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5$ where $\varepsilon = e^{\frac{i\pi}{3}}$. It is easy to see that not all automorphisms $\sigma_3(\varepsilon) = \varepsilon^3$ are well defined. Indeed $\varepsilon^3 = -1 \in \mathbf{Q} \Rightarrow \varepsilon \in \mathbf{Q}$. Contradiction. There is no automorphism which maps first root $e^{\frac{i\pi}{3}}$ to the third.

Later we will see that order of Galois group is just the degree of splitting field ($|\Gamma(f)| = [\Sigma(f) : \mathbf{Q}]$). In the case if p is not prime then degree of splitting field is not equal to $p - 1$. E.g. $[\Sigma(x^6 - 1) : \mathbf{Q}] = 2$, $[\Sigma(x^8 - 1) : \mathbf{Q}] = 4$ because all roots are powers of $e^{\frac{\pi i}{4}}$. (See more detail about $[\Sigma(x^N - 1) : \mathbf{Q}]$ in Appendix...)

[11] May be you are sick and tired by this polynomial. Is there another cubic polynomial which behaves in the similar way. Of course! Consider for example minimum polynomial of cos $\frac{2\pi}{7}$ (See your coursework!)

For the case $p = 5$ Galois group is cyclic group with four elements (see for the details the next subsection). In fact this is true for every prime p: Galois group of polynomial $t^p - 1$ is cyclic group $\{1, \tau, \tau^2, \dots, \tau^{p-2}\}$ of the order $p - 1$. E.g. consider $p = 7, 11$

a) $p = 7$. $\Gamma(t^7 - 1) = \Gamma(\mathbf{Q}(\varepsilon) : \mathbf{Q})$ where $\varepsilon = e^{\frac{2\pi i}{7}}$

$$\Gamma(t^7 - 1) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$$

where

$$\sigma_k(\varepsilon) = \varepsilon^k (k = 1, 2, 3, 4, 5, 6)$$

with multiplication law:

$$\sigma_p \sigma_q = \sigma_n, n = pq \pmod 7$$

because $\varepsilon^7 = 1$ and

$$\sigma_p \sigma_q(\varepsilon) = \sigma_q(\varepsilon^p) = (\sigma_q(\varepsilon))^p = (\varepsilon^q)^p = \varepsilon^{pq}$$

Consider $\tau = \sigma_3$. One can see that it is generator:

$$1 = \sigma_1, \tau = \sigma_3, \tau^2 = (\sigma_3)^2 = \sigma_2, \tau^3 = (\sigma_3)^3 = \sigma_6, \tau^4 = (\sigma_3)^4 = \sigma_4, \tau^5 = (\sigma_3)^5 = \sigma_5 \tag{68}$$

We see that Galois group is cyclic group $\{1, \tau, \tau^2, \tau^3, \tau^4, \tau^5\}$ with $\tau(\varepsilon) = \varepsilon^3$.

b) $p = 11$. $\Gamma(t^{11} - 1) = \Gamma(\mathbf{Q}(\varepsilon) : \mathbf{Q})$ where $\varepsilon = e^{\frac{2\pi i}{11}}$

$$\Gamma(t^{11} - 1) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \dots, \sigma_{11}\}$$

where

$$\sigma_k(\varepsilon) = \varepsilon^k, (k = 1, 2, 3, \dots, 10)$$

with multiplication law:

$$\sigma_p \sigma_q = \sigma_n, n = pq (\mod 11)$$

because $\varepsilon^{11} = 1$ and

Consider $\tau = \sigma_2$: $\tau(\varepsilon) = \varepsilon^2$. Then

$$1 = \sigma_1, \tau = \sigma_2, \tau^2 = (\sigma_2)^2 = \sigma_4, \tau^3 = (\sigma_2)^3 = \sigma_8, \tau^4 = (\sigma_2)^4 = \sigma_5, \tau^5 = (\sigma_2)^5 = \sigma_{10}$$

$$\tau^6 = (\sigma_2)^6 = \sigma_9, \tau^7 = (\sigma_2)^7 = \sigma_7, \tau^8 = (\sigma_2)^8 = \sigma_3, \tau^9 = (\sigma_2)^7 = \sigma_6, \tau_1 0 = 1$$

We see that Galois group is cyclic group $\{1, \tau, \tau^2, \tau^3, \tau^4, \tau^5, \dots, \tau^9\}$ with $\tau(\varepsilon) = \varepsilon^2$

3.2 Galois group for polynomial $x^5 - 1 = 0$. Why we need to study intermediate fields

Return to the example of solution of the equation $x^5 - 1 = 0$. We already know that solutions of this equation form pentagon on the complex plane:

$$x_0 = 1, x_1 = \varepsilon, x_2 = \varepsilon^2, x_3 = \varepsilon^3 = \frac{1}{\varepsilon^2}, x_2 = \varepsilon^4 = \frac{1}{\varepsilon}, \tag{69}$$

where

$$\varepsilon = e^{\frac{2\pi i}{5}} = \cos 72^\circ + i \sin 72^\circ \tag{70}$$

We calculate Galois group of this polynomial and answer the following question: Is it possible to solve this equation in radicals? Our best wish is to solve this equation in quadratic radicals. This is equivalent to the fact that regular pentagon can be constructed with ruler and compasses. (The fact of constructing regular pentagon is well-known 2000 years. Later we elaborate a method to understand how to deal with a problem of constructing regular $N - gon$ with a ruler and compasses.)

The splitting field is $\Sigma(x^5 - 1) = \mathbf{Q}(e^{\frac{2\pi i}{5}}) : \mathbf{Q}$. The Galois group contains four elements:

$$\sigma_k \colon \sigma_k(\varepsilon) = \varepsilon^k, \quad k = 1, 2, 3, 4 \tag{71}$$

Here σ_1 is identity. Every σ_k defines some permutation in S_5. Denote $\sigma_2 = \tau$ where τ is a permutation of roots $\{\varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4\}$ induced by $\varepsilon \to \varepsilon^2$:

$$\tau^2 = \sigma_4, \tau^3 = \sigma_3, \tau^4 = \sigma_1 = \mathbf{id} \tag{72}$$

$$\tau = \begin{pmatrix} \varepsilon & \varepsilon^2 & \varepsilon^3 & \varepsilon^4 \\ \varepsilon^2 & \varepsilon^4 & \varepsilon & \varepsilon^3 \end{pmatrix} \tag{73}$$

and correspondingly:

$$\tau^2 = \begin{pmatrix} \varepsilon & \varepsilon^2 & \varepsilon^3 & \varepsilon^4 \\ \varepsilon^4 & \varepsilon^3 & \varepsilon^2 & \varepsilon \end{pmatrix}, \tau^3 = \begin{pmatrix} \varepsilon & \varepsilon^2 & \varepsilon^3 & \varepsilon^4 \\ \varepsilon^3 & \varepsilon & \varepsilon^4 & \varepsilon^2 \end{pmatrix} \tag{74}$$

Galois group $\Gamma(\mathbf{Q}(\varepsilon) : \mathbf{Q})$ is a cyclic group $\{1, \tau, \tau^2, \tau^3\}$. This group contains only one proper subgroup, (i.e. subgroup which does not coincide with all group and the group formed with one identity element). It is subgroup $H = \{1, \tau^2\}$.

Consider arbitrary element $\alpha \in \mathbf{Q}$:

$$\alpha = a + b\varepsilon + c\varepsilon^2 + d\varepsilon^3 + e\varepsilon^4$$

It is easy to see that $\tau^2(\alpha) = \alpha$ if and only if $b = e, c = d$ because $\tau^2(\varepsilon) = \varepsilon^4$, $\tau^2(\varepsilon^2) = \varepsilon^3$, $\tau^2(\varepsilon^3) = \varepsilon^2$, $\tau^2(\varepsilon^4) = \varepsilon$, i.e. element a remains fixed under transformation of subgroup H if it is equal to $\alpha = a + b(\varepsilon + \varepsilon^4) + c(\varepsilon^2 + \varepsilon^3)$. Note that $(\varepsilon^2 + \varepsilon^3) = (\varepsilon + \varepsilon^4)^2 - 2$. Hence we come to conclusion:

The elements of the field $\mathbf{Q}(\varepsilon)$ which remain fixed under action of Galois subgroup H form intermediate subfield

$$M = \mathbf{Q}(\varepsilon + \varepsilon^4) = \mathbf{Q}\left(\varepsilon + \frac{1}{\varepsilon}\right) = \mathbf{Q}(\sin 18^\circ) \tag{75}$$

(In the next subsection we will study it more properly and will denote it by $H^\dagger$)

Now solve the equation $\frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1 = 0$ in radicals.

Consider ansatz:

$$z = x + \frac{1}{x} \tag{76}$$

Then $\frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1 = x^2\left(x^2 + \frac{1}{x^2} + x + \frac{1}{x} + 1\right)$ and

$$x^2 + \frac{1}{x^2} + x + \frac{1}{x} + 1 = \left(x + \frac{1}{x}\right)^2 + \left(x + \frac{1}{x}\right) - 1 \Rightarrow z^2 + z - 1 = 0\,. \tag{77}$$

We come to quadratic equation. Its solution is $z_{1,2} = \frac{-1\pm\sqrt{5}}{2}$, $(z_1 = 2\cos 72^\circ, z_2 = 2\cos 144^\circ$

Then we solve another quadratic equation produced by (76):

$$z = x + \frac{1}{x} \Rightarrow x^2 - zx + 1 = 0,\; x_{1,2} = \frac{z \pm \sqrt{z^2-4}}{2} \tag{78}$$

Coefficients of this equation are not rational numbers (z is not rational). But we already calculated it. You see that sequence of equations (77) and (78) give as solution of equation $x^5 - 1 = 0$ in radicals. Moreover we see that we use only quadratic radicals [12].

Now express these "pedestrians considerations" on the formal language:

[12] in other words it means that we can construct these numbers by ruler and compasses

The fact that we can solve the equation $x^5 - 1 = 0$ in two steps solving quadratic equations just corresponds to the fact that intermediate field $M = \mathbf{Q}(\varepsilon + \varepsilon^4)$ in (75) has degree 2. Thus by Tower law $[\mathbf{Q}(\varepsilon) : M] = 2$. It means that elements of M (and in particularly $\varepsilon + \frac{1}{\varepsilon} = 2\sin 18^\circ$ is a root of quadratic equation with rational coefficients) and elements of $\mathbf{Q}(\varepsilon)$ (in particularly ε itself) is a root of quadratic equation with coefficients in M.

It is just expressed by equations (76) and (77).

We see that the fact that the $\mathbf{Q}(\varepsilon) : \mathbf{Q}$ extension of degree 4 possesses intermediate field M which is quadratic extension is crucial for solving equation $x^5 - 1$ in quadratic radicals.

We really need to study intermediate fields. And they are related with subgroups...

3.3 Correspondence between intermediate fields and subgroups of Galois group.

We define here maps * and,$\dagger$ between the set $\mathcal{F}$ of intermediate fields of a field extension $L : K$ and the set $\mathcal{G}$ of subgroups of Galois group $\Gamma(L : K)$.

If M is intermediate field: $K \subseteq M \subseteq L$ then subgroup M^* is equal to $\Gamma(L : M)$. M^* is subgroup of all automorphisms from Γ which are identical not only on the field K but on the field M too.

If H is subgroup of $\Gamma = \Gamma(L : K)$ then $H^\dagger$ is subfield of elements which remain fixed under an action of automorphisms from subgroup H. This subfield contains the field K.

Consider examples:

1. First of all trivial examples. Let $\Gamma = \Gamma(L : K)$. Then it is evident that $L^* = \mathbf{id}$ contains only identical transformation, $K^* = \Gamma$ by definition. It is easy to see that to trivial subgroup corresponds all field L: $\{e\}^* = L$. On the other hand consider subfield $\Gamma^\dagger$. $K \subset \Gamma^\dagger$ by definition. But in general case $K \neq \Gamma^\dagger$. E.g. consider a "bad" example: $K = \mathbf{Q}, L = \mathbf{Q}(\sqrt[3]{2})$. Then Galois group Γ contains only identical transformation because the field $\mathbf{Q}(\sqrt[3]{2})$ contains only one root of polynomial $x^3 - 2$. Then $\Gamma^\dagger = L$. (The reason why this example is "bad" it is that this extension is not normal.)

The following properties of maps $^*,^\dagger$ can be easily checked:

1) If subfield $M_1 \subseteq M_2$, then $M_2^* \leq M_1^*$ and If subgroup $H_1 \leq H_2$, (H_1, H_2 aqre subgroups of Galois groups) then $H_2^* \subseteq H_1^*$

One can say that maps $^*,^\dagger$ are **inversing the order**

Now return again to the example of polynomial $x^p - 1$, where p is prime. In the end of the subsection "Galois group of polynomial" we obtained that that Galois group contains exactly $p-1$ automorphims $\sigma_1, \dots, \sigma_{p-1}$ (see (67)).

Consider cases, $p = 5, p = 7$

Example($p = 5$) This example was considered indeed in the previous subsection by bare hands. We can repeat it again: The Galois group (71) contains only one proper subgroup H and $H^\dagger = M$ is just intermediate field which is quadratic extension. In the next subsection we will learn that *there are no any other intermediate subfields because there is one-one correspondence between subgroups and subfields for finite normal extensions.*

Example ($p = 7$). In this case Galois group $\Gamma = \{1, \tau, \tau^2, \tau^3, \tau^4, \tau^5\}$ contains four subgroups: $H_1 = \Gamma$, $H_2 = \{1, \tau^2, \tau^4\}$, $H_3 = \{1, \tau^3\}$, $H_6 = \{1\}$.

$H_1^\dagger = \mathbf{Q}$—only rational numbers remain fixed under action of all transformations.

$H_6^\dagger$ is evidently all the field $\mathbf{Q}(e^{\frac{2\pi i}{7}})$. What about $H_2^\dagger, H_3^\dagger$. Note that $\tau^3(\varepsilon) = \varepsilon^6 = \frac{1}{\varepsilon}$ (see calculations in (68)) Hence $\varepsilon + \frac{1}{\varepsilon} = 2\cos\frac{2\pi i}{7}$ belongs to H_3. one can show that $H_3^\dagger = \mathbf{Q}(\cos\frac{2\pi}{7})$.

3.4 Fundamental Theorem of Galois Theory. Formulation

Let $L : K$ be *finite, normal, separable* extension. Then

1) Order of Galois group is equal to degree of the field extension:

$$|\Gamma(L : K)| = [L : K]\,. \tag{79}$$

2) The maps $*, \dagger$ are mutual inverse and establish an order reversing one-one correspondence between the set $\mathcal{F}$ of intermediate fields of extension $L : K$ and the set $\mathcal{G}$ of subgroups of the Galois group $\Gamma(L : K)$:

$$M_1 \subseteq M_2 \Rightarrow M_1^* \geq M_2^*\,, \tag{80}$$

$$H_1 \geq H_2 \Rightarrow H_1^\dagger \subseteq H_2^\dagger \tag{81}$$

$$\dagger \circ * = \mathbf{id}\,,\ \text{i.e.}\,, (M^*)^\dagger = M \text{ for arbitrary intermediate field} \tag{82}$$

$$* \circ \dagger = \mathbf{id}\,,\ \text{i.e.}\,, (H^\dagger)^* = H \text{ for arbitrary subgroup } H \text{ of Galois group} \tag{83}$$

3) For every intermediate field M the degree of extension $L : M$ is equal to the order of subgroup M^*. Respectively degree of extension $M : K$ is equal

to the index of subgroup M^* in Galois group $\Gamma(L:K)$:

$$[L:M] = |M^*|\,, \tag{84}$$

$$[M:K] = \frac{|\Gamma(L:K)|}{|M^*|} \tag{85}$$

4) An intermediate field is normal extension of K if and only if M^* is normal subgroup [13] in the Galois group $\Gamma(L:K)$. Note that finite extension is normal extension iff it is spliting field for polynomial. Hence we can reformulate this point as:

$$\text{intermediate field } M \text{ is a splitting field for a polynomial over } K \Leftrightarrow \tag{86}$$

$$\Leftrightarrow M^* \text{ is a normal subgroup in } \Gamma \tag{87}$$

5) In the case if intermediate field M is normal extension of K then Galois group of field extension $M:K$ is isomorphic to quotient group $\Gamma(L:K)/M^*$

We give the proof of this theorem in the next subsection. Then we will consider examples. Now only some comments:

Comments to the condition of Theorem: Note that condition that extension is normal, finite means that it is generated by polynomial. (See the subsection "Normal extension")

1) Comment to the 1-st statement:

This statement is only about the order of the group.

We consider later a construction of all Galois automorphisms via roots of so called resolution polynomial and prove that number of these automorphisms (i.e. order of Galois group) is equal to the degree of resolvent polynomial, i.e. degree of field extension. (See the next subsection "Calculation of Galois group using primitive elements")

The condition to be normal extension is essential: Indeed consider extension $\mathbf{Q}(\sqrt[3]{2}):Q$. Its degree is equal 3 but Galois group contains only one element.

[13] subgroup $H \leq G$ is normal if $\forall h \in H$, $\forall g \in G$, $g^{-1}hg \in H$. In other words H coincide with all conjugate subgroups gHg^-1 and one can consider natural group structure on factor space G/H: the operation $[g_1] \circ [g_2] = [g_1 \circ g_2]$, where $[g]$ is equivalence class is well-defined.

The condition that extension is finite is essential too[14].

The condition of separability is essential too, but we do not discuss it here.

2) Comment to the 3-st statement:

Note that it is true even if extension $M : K$ is not normal extension: if subgroup M^* is not normal, then quotient space Γ/M^* is not in general a group, but still its order is related with degree of extension by (84).

3) Comment to the 4-st statement: May be it is main point of Galois correspondence [15].

Suppose we have to solve polynomial equation. We cannot do it straightforwardly. Instead we calculate Galois group of polynomial. Then we find normal subgroup H in Galois group and corresponding intermediate field $M = H^\dagger$. The condition that $M : K$ is normal extension means that M is a splitting field for another polynomial (of less degree). In other words a combination of roots obey the polynomial equation of less degree. Thus we come to substitution which allows us to solve polynomial equation of less degree. E.g. in (75) to solve equation $1 + x + x^2 + x^3 + x^4 = 0$ we solve equation $z^2 - z - 1$. Roots of former equation define intermediate field $\mathbf{Q}(\varepsilon + \frac{1}{\varepsilon})$. (See also example 5) in subsection "Examples,examples,examples...")

3.5 Proof of Galois Fundamental Theorem

Use Theorem on primitive element. Let θ be a primitive element of extension $L : K$ and R be a minimum polynomial of θ: R has N roots $\{\theta_1, \dots, \theta_N\}$ $(\theta = \theta_1)$, where N is degree of R. Fields $K(\theta_i)$ are isomorphic (see Theorem 2 in subsection 2.1) on the other hand $L = K(\theta_1)$ and L is *normal extension.* Hence all fields $K(\theta_i)$ coincide.

$$L = K(\theta_1) = K(\theta_2) = \cdots = K(\theta_n) \tag{88}$$

Hence all isomorphisms $K(\theta_i) \leftrightarrow K(\theta_j)$ are automorphisms.

[14] Consider a striking counterexample: Extension $\mathbf{R} : \mathbf{Q}$ is infinite-dimensional and its Galois group contains only one element. It sounds very strange: adding new elements we expand Galois group, but we add non-countable number of elements to $\mathbf{Q}$ and mysteriously come to normal infinite extension with trivial Galois group

[15] Note that notion of normal group arisen just as a group corresponding to the normal extension.

In particularly one can consider automorphisms $\{\tau_1, \tau_2, \dots, \tau_N\}$ defined by condition

$$\tau_j(\theta_1) = \theta_j \tag{89}$$

These automorphisms belong to Galois group.

On the other hand If τ is automorphism of L which leaves intact elements of K (i.e. τ belongs to Galois group of automorphisms) then it transforms a root of polynomial R to another root of this polynomial. Hence we come to the conclusion that Galois automorphisms are automorphisms $\{\tau_1, \tau_2, \dots, \tau_N\}$ defined by (89).

We proved the formula (79) of Fundamental Theorem. Moreover we described explicitly by (89) Galois automorphisms in terms of roots of resolvent polynomial.

Before proving (80)—(83) we formulate and prove the following

Lemma 1 If M is intermediate field for field extension $L : K$ then

a) $L : M$ is finite if $L : K$ is finite

b) $L : M$ is normal extension if $L : K$ is normal extension

c) $L : M$ is separable extension if $L : K$ is separable extension.

The a) is evident because $[L : M] = [L : K]/[M : K]$.

Prove b). Let α be a root of polynomial $h = t^m + A_{m-1}t^{m-1} + \dots + A_1 t + A_0$ such that h is irreducible polynomial over M ($A_n \in M$) and $\alpha \in L$. h is the minimum polynomial of α over M. Prove that all roots of h belong to L. Consider minimum polynomial f of α over K $f = t^n + a_{n-1}t^{m-1} + \dots + a_1 t + a_0$. It is evident that h divides f. Hence all roots of h are roots of f. But roots of f belong to L because a is a root of f and $L : K$ is a normal extension ■.

In the same way we can prove c). If h is a minimum polynomial of $a \in L$ over M then it divides the minimum polynomial f of a over K. f has no repeated roots. Hence h has no repeated roots too ■.

Lemma 2 Let element $a \in L$ remains fixed under all Galois automorphisms. Then it belongs to the main field K. In other words Lemma states that not only $K^* = \Gamma(L : K)$ (by definition) but $\Gamma^\dagger = K$, i.e. $K^{*\dagger} = K$ and $\Gamma^{\dagger *} = \Gamma$.

Remark Compare this lemma with Viète Theorem from the subsection 0!

Proof of the Lemma. Consider minimum polynomial of a over K. Suppose degree of this polynomial is not equal to one. Hence it has more than one roots $\{a_1, a_2, \dots\}$ ($a = a_1$). Considering automorphisms of the field K induced by $a = \alpha_1 \to a_2$ we come to Galois automorphism which changes a.

Contradiction. Hence degree of minimum polynomial of a is equal to one. Thus $a \in K$ ■.

Now return to the proof of Galois Fundamental Theorem.

Formulae (80),(81) follow from definition of maps $\dagger, *$. From Lemma 1 follows that for arbitrary intermediate field M, the extension $L : M$ is separable,finite and normal. Hence from Lemma 2 it follows that $\Gamma(L : M)^\dagger = M$. On the other hand $\Gamma(L : M) = M^*$. Hence $M^{*\dagger} = M$. The relation (82) is proved.

Consider now arbitrary subgroup H. Let $M = H^\dagger$ and $\tilde{H} = M^* = H^{\dagger *}$. Prove that $H = \tilde{H}$. First by definition $H \leq \tilde{H}$. These groups both are finite. So it sufficient to prove that $|H| = |\tilde{H}|$

It follow from Lemma 1 and (79) that

$$[L : H^\dagger] = |\tilde{H}| \,. \tag{90}$$

On the other hand consider polynomial which is equal to the product of linear polynomials $(x - \tau((\theta))$ where θ is a primitive element of extension $L : K$ and τ is Galois automorphism belonging to the subgroup H

$$\mathcal{R}(t) = \prod_{\tau \in H} (x - \tau((\theta)) \tag{91}$$

All coefficients of this polynomial are fixed under the action of group H. Hence they belong to $M = H^\dagger$. We see that polynomial $\mathcal{R}(t)$ is a polynomial of degree $|H|$ over M and primitive element θ is its root. Hence *minimum polynomial of* θ *over* M *has degree less or equal to* $|H|$:

$$[L : M] \leq |H| \Leftarrow |\tilde{H}| \leq |H| \,. \tag{92}$$

We have that $|H| \leq |\tilde{H}|$. Hence it follows from (90) and (92) that $|H| = |\tilde{H}|$. ■

Now prove (86).

Suppose $H \leq \Gamma$ is a normal subgroup in Γ. Prove that $M = H^\dagger$ is a normal extension of K.

Let g be irreducible polynomial over K and its root α belongs to M. $L : K$ is a normal extension, so all roots of this polynomial belong to L. Prove that all roots of this polynomial belong to M, i.e. $M : K$ is a normal extension. Let $\beta \in L$ be another root of this polynomial. Consider Galois automorphism $\tau\Gamma(L : K)$ such that $\tau(\alpha) = \beta$. Then for arbitrary $h \in H$

$\tau^{-1} \circ h \circ \tau \in H$ because H is a normal subgroup in Γ. Hence $(\tau^{-1} \circ h \circ \tau)\alpha = \alpha$, because $\alpha \in M = H^\dagger$. On the other hand

$$\alpha = \tau^{-1} \circ h \circ \tau(\alpha) = \tau^{-1} \circ h(\beta) \,. \Rightarrow h(\beta) = \beta \tag{93}$$

Hence $\beta \in M$ ■.

Now prove that M^* is a normal subgroup in Γ if $M : K$ is a normal extension.

Consider arbitrary $h \in H = M^*$, $g \in \Gamma$. We have to prove that transformation $g^{-1}hg$ does not move elements of M. Consider arbitrary $\alpha \in M$. Let f be its minimum polynomial over K and $\beta = g(\alpha)$. β is a root of f too. (Galois transformation transforms roots to roots). Hence $\beta \in M$ because $M : K$ is a normal extension. Now apply Galois transformation $g^{-1}hg$ to α: $g^{-1}hg(\alpha) = g^{-1}h(\beta) = g^{-1}(\beta)$ because H does not move elements of M and $\beta \in M$. Hence $g^{-1}hg(\alpha) = g^{-1}(\beta) = \alpha$, ■

It remains to prove the statement 5 of Galois fundamental Theorem.

First of all note that under Galois transformation every element in L transforms to conjugate (i.e. to another root of the same irreducible polynomial).

Hence Galois automorphism maps M onto M if M is normal extension, i.e. Galois automorphism do not move M taking as whole.

Let $H = M^*$ be Galois group of $L : M$. Consider factor group Γ/H and Galois group of extension $M : K$. Let $[g]$ be an arbitrary element in the factor group Γ/H (equivalence class in Γ w.r.t. subgroup H). Consider arbitrary representative $g \in [g]$ and Galois transformation of M by g. Note that if $g' = g \circ h$ is another representative of the same equivalence class then it defines the same action on M because $h|_H = \mathbf{id}$. Thus we define homomorphism of Γ/H in Galois group of extension $M : K$. prove that it is isomorphism. If $[g]$ defines identity automorphism on M then $g \in H$ and $[g] = \mathbf{id}$ in Γ/H. Hence our homomorphism is monomorphism. On the other hand let τ be arbitrary automorphism of M (identical on K) ($\tau \in \Gamma(M : K)$). Its prolongation $\tilde{\tau}$ on L defines an element in $\Gamma(L : K)$. Hence our monomorphism is epimorphism.

3.6 Galois group for cubic polynomial, discriminant and complex roots

Consider arbitrary cubic polynomial with rational coefficients. It has three complex roots. It is easy to see that or all three roots are real or one root is real and two other roots are complex conjugated.

Consider group S_3 of all permutations of roots (see subsection 0):

$$I = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}, s = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}, s^2 = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix}, \qquad (94)$$

$$\sigma_{12} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}, \sigma_{13} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix}, \sigma_{23} = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix}, \qquad (95)$$

Galois group is a subgroup of the group of permutations:

Group S_3 contains 6 subgroups: trivial subgroup $\{1\}$, three subgroups of permutations $\{1, \sigma_{12}\}$, $\{1, \sigma_{23}\}$, $\{1, \sigma_{13}\}$ cyclic subgroup $\{1, s, s^2\}$ and whole group itself $\{1, s, s^2, \sigma_{12}, \sigma_{13}, \sigma_{23}\}$. Consider all the cases.

Reducible case. If cubic polynomial $f = t^3 + at + bt + c$, $a, b, c, \in \mathbf{Q}$ is reducible over $\mathbf{Q}$ then it has at least one rational root [16]. Denote it by x_1. Dividing a polynomial f on $t - x_1$, $x_1 \in \mathbf{Q}$ we come to quadratic polynomial which have two rational roots or two irrational roots. So we have two subcases: *f has three rational roots,* or *f is reducible and splitting field is quadratic extension..* If all roots are rational (e.g. polynomial $t^3 - t = t(t-1)(t+1)$) then Galois group contains only identical transformation. It is just the case IIb in the subsection "Splitting field for cubic polynomials". If *f is reducible and splitting field is quadratic extension.*, i.e. one root is rational and two roots are not rational (E.g. $f = t^3 - t = t(t^2 - 2)$) then Galois group contains two elements. It is $\{I, \sigma_{23}\}$ (if $x_1 \in \mathbf{Q}$ and $x_2, x_3 \notin \mathbf{Q}$). It is just the case IIa in the subsection "Splitting field for cubic polynomials".

Now consider the most interesting *Irreducible case*: when $f(t) = t^3 + at^2 + bt + c$ is irreducible cubic polynomial, (a, b, c, are rational coefficients).

Let x_1, x_2, x_3 be roots of this polynomial. All these roots are algebraic irrationals and they are different because irreducible polynomial over rationales is separable (Or simply because in other case the polynomial f has a common root with derivative f'. This contradicts to irreducibility.).

For every root x_1, x_2, x_3 degree of isomorphic extensions $\mathbf{Q}(x_1) : \mathbf{Q}$ or $\mathbf{Q}(x_2) : \mathbf{Q}$ or $\mathbf{Q}(x_3) : \mathbf{Q}$ is equal to three because f is irreducible polynomial. Do these extensions coincide? Or in other words: "Do roots x_2, x_3 belong to the extension $\mathbf{Q}(x_1)$?". Or in other words is extension $\mathbf{Q}(x_1)$ normal extension?

[16] Note again that If degree of polynomial is greater than 3 then reducibility over $\mathbf{Q}$ does not mean an existence of the rational root

Roots x_2, x_3 are roots of quadratic polynomial with coefficients in the field $\mathbf{Q}(x_1)$. Indeed according to Viète Theorem$x_2 + x_3 = a - x_1$, $x_2 x_3 = \frac{-c}{x_1}$ Here a, b, c are coefficients of the cubic polynomial. If x_2 belongs to the extension $\mathbf{Q}(x_1)$ then x_3 belongs too and degree of the splitting field will be 3. According to Fundamental Theorem of Galois Theory Galois group of polynomial contains 3 elements. This is cyclic subgroup $\{1, s, s^2\}$. It is exactly the case of "glorious" polynomial $t^3 - 3t - 1$ (see e.g. (65))

If x_2 does not belong to the extension $\mathbf{Q}(x_1)$ then extension $\mathbf{Q}(x_1) : \mathbf{Q}$ *is not normal*, degree of the extension $\Sigma(f) = \mathbf{Q}(x_1, x_2, x_3) : \mathbf{Q}(x_1)$ is equal to 2. Hence degree of the splitting field over rationales is equal to 6. Galois group contains 6 elements. It is just the group of all permutations as in the example of polynomial $t^3 - 2$ (See the subsection above)

So we see that for irreducible polynomial or degree of extension $\Sigma(f) : \mathbf{Q}$ is equal to 6 and Galois group is group of all permutations (95), (94) or degree of extension $\Sigma(f) : \mathbf{Q}$ is equal to 3 and Galois group is cyclic subgroup (94). How to distinguish between these two cases for irreducible polynomial?

Recall notion of discriminant $D = (x_1 - x_2)^2 (x_2 - x_3)^3 (x_3 - x_1)^2$. For irreducible polynomial discriminant is not equal to zero, because roots are distinct. Remember that D is rational according to Viète Theorem. (In the beginning of the course we calcualted discriminant for cubic polynomial $x^3 + px + q$ (see (14))). Consider square root of discriminant

$$d = \sqrt{D} = \pm(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \qquad (96)$$

Consider now the tower of extensions:

$$\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{D}) \subset \Sigma(f) = \mathbf{Q}(x_1, x_2, x_3)$$

Simple but very important remark: Remember that D is rational according to Viète Theorem. Hence square root of discriminant is a root of quadratic polynomial with rational coefficients. Suppose that degree of the extension $\Sigma : \mathbf{Q}$ is equal to three. Then by Tower Law degree of the extension $\mathbf{Q}(\sqrt{D}) : \mathbf{Q}$ *cannot be equal to 2* and it is equal to 1, i.e. $\mathbf{Q}(\sqrt{D}) = \mathbf{Q}$. Hence $\sqrt{D}$ is rational. Now suppose that $\sqrt{D}$ is rational. Note that transpositions $\sigma_{12}, \sigma_{13}, \sigma_{13}$ (see (95)) change a sign of square root of discriminant $(x_1 - x_2)(x_2 - x_3)(x - x_1) \to -(x_1 - x_2)(x_2 - x_3)(x - x_1)$ ($D \neq 0$ because roots are distinct). Hence transpositions **do not belong to Galois group**, because Galois transformations do not change rationals. Galois group contains only cyclic permutations $\{1, s, s^2\}$ defined by (94). Cyclic transformations preserve $(x_1 - x_2)(x_2 - x_3)(x - x_1)$. We proved that if degree of splitting field is equal to 3 then square root of discriminant is rational and we proved that if discriminant is rational then Galois group is cyclic group containing three elements $\{1, s, s^2\}$. On the other hand according to Galois Fundamental Theorem the condition that Galois group is cyclic implies that degree of splitting field is equal to three. We come to

Theorem If $f = t^3 + at + bt + c, a, b, c, \in Q$ is irreducible cubic polynomial over rationales then following conditions are equivalent:

a) Splitting field of this polynomial has degree 3 over rationales

b) square root of discriminant is rational number

c) Galois group is cyclic

Remark If square root of discriminant of cubic polynomial is rational and polynomial is reducible then all roots have to be rational. This follows from Vièta Theorem.

(We proved that a)⇒b)⇒c)⇒a))

Note that implication $a) \to b)$ is proved without using Galois Theory. One can prove $b) \to a)$ without Galois Theory also (noting that roots x_2, x_3 of cubic polynomial can be rationally expressed via root x_1 and discriminant (see Appendix A).

It follows from this Theorem that Galois group of irreducible polynomial is group of all permutations of roots iff square root of discriminant is not rational.

Example Consider polynomial $t^3 - 3t - 1$. We know already that its Galois group is cyclic. Check that discriminant is rational: According (14)

$$D = (x_1 - x_2)^2 (x_2 - x_3)^2 (x_3 - x_1)^2 = -27q^2 - 4p^3 = -27 + 108 = 81, \ \sqrt{81} = 9$$

We see that square root of discriminant is rational.

Example $t^3 - 2$. Check that discriminant is not rational:

$$D = (x_1 - x_2)^2 (x_2 - x_3)^2 (x_3 - x_1)^2 = -27q^2 - 4p^3 = -108, \ \sqrt{-108} = \notin \mathbf{Q}$$

Galois group contains 6 elements as we know it already.

Complex roots and Galois group

Cubic polynomial $f = t^3 + t^2 + bt + c$ with rational coefficients has one real root and two complex roots or three real roots. Indeed $f \to -\infty$ if $t \to -\infty$

and $f \to \infty$ if $t \to \infty$. Hence there exists at least one real root. If $x = a + bi$ is a complex root then conjugated number $\bar{x} = a - bi$ is a root too

If irreducible cubic polynomial has only one real root and two complex roots which are not real, then splitting field has degree 6 over rationales. This follows from the fact that discriminant is negative. Indeed if $x_1 = \lambda \in \mathbf{R}$ and $x_{2,3} = a \pm bi$ then

$$D = (x_1 - x_2)^2(x_2 - x_3)^3(x_3 - x_1)^2 = (\lambda - a - bi)^2(2bi)^2(a - bi - \lambda)^2 < 0$$

Hence $\sqrt{D} \notin \mathbf{Q}$. According to Theorem above the degree of the splitting field is equal to 6 and Galois group possesses 6 elements. But one can prove it in a different way: Consider conjugation automorphism $z \to \bar{z}$, $a \pm bi \to a - bi$. The field of all real numbers remains fixed under this automorphism.

Now consider restriction of this automorphism on splitting field $\Sigma(f) = \mathbf{Q}(x_1, x_2, x_3)$ of cubic polynomial with rational coefficients. It is Galois transformations. If all roots are real then this is *identical transformation* of the splitting field. But if all rooots are not real, i.e. two roots are complex conjugate and one root is real then conjugation automorphism is transposition of the second and third root. Hence Galois group possesses transposition. Hence it possesses all permutation, because polynomial is irreducible and $|\Gamma| = 3, 6$. Hence its order is equal to 6 and degree of extension is equal to 6.

Note that subgroup containing two elements (identity and conjugation automorphism) *is not normal subgroup in the group of all permutations.* Hence by Galois Fundamental Theorem splitting field $\Sigma(f)$ does not possess any normal extension of degree 3.

3.7 Examples, and exercises

In this subsection we consider some exercises-examples and give a sketch of their solutions.

1. *Find Galois group for cubic polynomial $t^3 + pt + 1$ where p is a given integer.*

2. *Irreducible cubic polynomial with rational coefficients has a complex root. Prove that its splitting field does not contain a number $\alpha = \cos 20°$.*

3. *Find Galois group of quadratic polynomial $x^4 - 5x^2 + 6$*

4. *Find Galois group of the polynomial $x^4 + 4$*

5. *What can you say about Galois group of the polynomial $x^N - 1$? About Galois group of the field extension* $\mathbf{Q}(\cos \frac{2\pi}{N})$ (Try to do detailed analysis of the cases $N = 7, 17, 19$)

1) First note that polynomial $t^3 + pt + 1$, $p \in \mathbf{Z}$ is reducible iff one of its roots is equal ± 1. Hence $t^3 + pt + 1$ is irreducible iff an integer $p \neq 2$ or $p \neq 0$. If $p = 2$ then $t^3 + pt + 1 = (t+1)(t^2 - t + 1)$. $\Gamma(f) = \Gamma(t^2 - t + 1)$ contains two elements. If an integer $p \neq 2, 0$ then Galois group is cyclic iff $\sqrt{D} = \sqrt{-27 - 4p^3} \in Q$ (see subsection 3.6).

2) If the irreducible polynomial f has complex root then its Galois group is group of all permutations: $|\Gamma(f)| = 6$ (see in detail subsection 3.6). Field $\mathbf{Q}(\cos 20^\circ)$ is normal field because it is splitting field for the polynomial $t^3 - 3t - 1$. Suppose it is a subfield of $\Sigma(f)$. Consider Tower of extensions: $\mathbf{Q} \subset \mathbf{Q}(\cos 20^\circ) \subset \Sigma(f)$. Consider Galois group of the extension $\Sigma(f) : \mathbf{Q}(\cos 20^\circ)$. According Galois Fundamental Theorem The Galois group of the extension $\Sigma(f) : \mathbf{Q}(\cos 20^\circ)$ contains $[\Sigma(f) : \mathbf{Q}(\cos 20^\circ)] = 6 : 3 = 2$ elements and it is has to be normal group. Subgroup containing two elements it is identity and transposition. This subgroup is not normal subgroup in the group of all permutations. Contradiction.

3. Polynomial is product of two irreducible quadratic polynomials $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$. Galois transformation maps root of irreducible quadratic polynomial to another (or to the same) root of this polynomial $\sqrt{3} \mapsto \pm\sqrt{3}$, $\sqrt{2} \mapsto \pm\sqrt{2}$. Degree of the splitting field is equal to 4 (to see it use tower law). Any element of splitting field $\Sigma(f) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ can be expressed in the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$. Galois group contains four elements: $\{1, \tau_1, \tau_2, \tau_1 \circ \tau_2\}$ where τ_1 changes $\sqrt{2}$ but it does not change $\sqrt{3}$; τ_2 changes $\sqrt{3}$ and it does not change $\sqrt{2}$: $\tau_1(\sqrt{2}) = -\sqrt{2}, \tau_1(\sqrt{3}) = \sqrt{3}$, $\tau_2(\sqrt{2}) = \sqrt{2}, \tau_2(\sqrt{3}) = -\sqrt{3}$, $\tau_1 \circ \tau_2(\sqrt{2}) = -\sqrt{2}, \tau_1 \circ \tau_2(\sqrt{3}) = -\sqrt{3}$. The action on arbitrary element is given by the formulae:

$$\begin{gathered}
\tau_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\
\tau_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\
\tau_1 \circ \tau_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}
\end{gathered}$$

Group is abelian but *not-cyclic*. It is direct product of two groups.

4) This polynomial is very famous (Marie-Sophie Germain polynomial.) It is not evident but this polynomial is decomposable over rationals: $x^4 + 4 = (x^2 + 2)^2 - 4x^2 = (x^2 + 2x + 2)(x^2 - 2x + 2)$ Splitting field is just $\mathbf{Q}(i)$, roots are $\pm(1 \pm i)$. Galois group contains two elements. $\{1, \sigma\}$: $\sigma(i) = -i$.

5. Splitting field of polynomial $x^N - 1$. First, two words for arbitrary N. Spliting field of this polynomial is $\mathbf{Q}(\varepsilon_N)$ where $\varepsilon_N = e^{\frac{2\pi i}{N}}$. It has N roots $x_k = \varepsilon_n^k$ $(k = 0, 1, 2, \dots, N)$.

Extension $\Sigma(x^N - 1) = \mathbf{Q}(\varepsilon_N)$ is normal extension. What can we say about its degree? Let $P_N(x)$ be minimum polynomial of ε_N This polynomial divides polynomial x^{N-1}. Denote by $\varphi(N)$ the degree of the polynomial P_N. $x^N - 1 = (x-1)(1 + x + x^2 + \dots + x^{N-1})$. Hence P_N divides polynomial $1 + x + x^2 + \dots + x^{N-1} = \frac{x^N - 1}{x-1}$. We know that in the case where $N = p$ is prime number then by Eisentein polynomial $1 + x + x^2 + \dots + x^{N-1} = \frac{x^N - 1}{x-1}$ is irreducible. Hence $P_N = 1 + x + x^2 + \dots + x^{N-1}$ and $\varphi(N) = N - 1$ if N is prime. In general case $\varphi(N)$ less than or equal to $N - 1$ [17].

Consider e.g. a case $N = 2p$ where p is a prime number. Then

$$x^N - 1 = x^{2p} - 1 = (x^p - 1)(x^p + 1) =$$

$$(x-1)(x+1)(x^{p-1} + x^{p-2} + \dots + x + 1)(x^{p-1} - x^{p-2} + \dots + x^2 - x + 1)$$

One can see using Eisenstein Test that polynomial $1 - x + x^2 - x^3 + \dots + x^{p-1} = \frac{x^p + 1}{x+1}$ is irreducible ($x \to -x$ it transforms to $\frac{x^p - 1}{x-1}$). Hence $P_N = x^{p-1} - x^{p-2} + \dots - x + 1$ and $\varphi(2p) = p - 1$ for $N = 2p$ with p prime.

For example

$$P_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1, \ \varphi(14) = 6$$

Below we consider in detail examples of $N = 7, 19, 17$. But before two words about a number $\alpha_N = \cos\frac{2\pi}{N}$ in general case and for arbitrary prime p. Let P_N be minimum polynomial of $\varepsilon_N = e^{\frac{2\pi i}{N}}$. Consider the tower:

$$\mathbf{Q} \subseteq \mathbf{Q}(\alpha_N) \subset \mathbf{Q}(\varepsilon_N)$$

Degree of the extension $\mathbf{Q}(\varepsilon_N) : \mathbf{Q}(\alpha_N)$ is equal to 2 because ε is a root of quadratic polynomial over $\mathbf{Q}(\alpha_N)$ and this polynomial is irreducible (Why?). Hence degree of the extension $\mathbf{Q}(\alpha_N) : \mathbf{Q}$ is equal to $\varphi(N) : 2$, where $\varphi(N)$ is degree of the extension $\mathbf{Q}(\varepsilon_N) : \mathbf{Q}$. Galois group of the polynomial $x^N - 1$ is abelian, hence all subgroups are normal. It follows from Fundamental

[17] One can show that $\varphi(N)$ is number of integers k such that $1 \leq k \leq N$ and which are coprime with N, i.e. number of invertible elements in the ring $\mathbf{Z}/n\mathbf{Z}$. Galois group of $x^N - 1$ is just multiplication group of the ring $\mathbf{Z}/n\mathbf{Z}$

Theorem of the Galois Theory that extension $\mathbf{Q}(\alpha_N)$ is normal extension. If $N = p$ is prime number (greater that 2) then degree of the normal extension $\mathbf{Q}(\alpha_N) : \mathbf{Q}$ is equal to $\frac{p-1}{2}$. Hence minimum polynomial of α_N has degree $\frac{p-1}{2}$. It possesses all its roots in the normal extension $\mathbf{Q}(\alpha_N)$. In particular this implies that all roots of minimum polynomial are real because $\mathbf{Q}(\alpha_N) \subset \mathbf{R}$.

For example if $N = 7$ then degree of extension $\mathbf{Q}(\alpha_7) : \mathbf{Q}$ is equal to 3, this extension is normal and $\mathbf{Q}(\alpha_7)$ belongs to $\mathbf{R}$. The minimum polynomial of α_7 has degree 3 its all roots are in the normal extension $\mathbf{Q}(\alpha_7)$ and they are real.

For this case we can calculate everything by bare hands: E.g. for $N = 7$: ε_7 is a root of the polynomial $1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ We have:

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = 0 \Rightarrow$$

$$\left(\frac{1}{x^3} + x^3\right) + \left(\frac{1}{x^2} + x^2\right) + \left(\frac{1}{x} + x\right) + 1 =$$

$$\left(\frac{1}{x} + x\right)^3 - 3\left(\frac{1}{x} + x\right) + \left(\frac{1}{x} + x\right)^2 - 2 + \left(\frac{1}{x} + x\right) + 1 = 0$$

for $x = \varepsilon_7$. Hence polynomial $z^3 - 2z + z^2 - 1$ ($z = x + \frac{1}{x}$) is a minimum polynomial for the number $2\cos\frac{2\pi}{7}$ (Compare these calculations with calculations in subsection 3.2. for polynomial $x^5 - 1$). This polynomial has three real roots. It can be checked straightforwardly: other roots of this polynomial are $\varepsilon^2 + \varepsilon^{-2} = 2\cos\frac{4\pi}{7}$ and $\varepsilon^3 + \varepsilon^{-3} = 2\cos\frac{6\pi}{7}$. Alternatively it was proved above using Galois Theory.

One can perform similar straightforward calculations for arbitrary $N = p$ prime number. Then $P_N = 1 + x + x^2 + \cdots + x^{p-1}$. Dividing polynomial P_N on $x^{\frac{p-1}{2}}$ we come to:

$$\left(x^{\frac{p-1}{2}} + x^{\frac{1-p}{2}}\right) + \left(x^{\frac{p-3}{2}} + x^{\frac{3-p}{2}}\right) + \cdots = 0 \,\text{for}\ x = \varepsilon_N$$

Hence using relation $\varepsilon_N^k + \varepsilon_N^{-k} = 2\cos\frac{2\pi k}{N}$ we see that

$$s_{\frac{p-1}{2}} + s_{\frac{p-3}{2}} + \cdots = 0$$

where we denote by

$$s_k = \varepsilon_N^k + \varepsilon_N^{-k} = 2\cos\frac{2\pi k}{n}$$

It is easy to see that s_k are polynomials on $s_1 = \alpha_N$:

$$s_2 = \varepsilon_N^2 + \varepsilon_N^{-2} = (\varepsilon_N + \varepsilon_N)^2 - 2 = s_1^2 - 2,$$

$$s_3 = \varepsilon_N^3 + \varepsilon_N^{-3} = (\varepsilon_N + \varepsilon_N)^3 - 3\,(\varepsilon_N + \varepsilon_N) = s_1^3 - 3s_1,$$

$$s_4 = \varepsilon_N^4 + \varepsilon_N^{-4} = (\varepsilon_N + \varepsilon_N)^4 - 4\,(\varepsilon_N + \varepsilon_N)^3 + 12\,(\varepsilon_N + \varepsilon_N) - 6 = s_1^4 - 4s_1^3 + 12s_1 - 6,$$

Hence we come to polynomial of degree $\frac{p-1}{2}$ such that $2\alpha_N$ is its root. On the other hand degree of the extension $\mathbf{Q}(\alpha_N) : \mathbf{Q}$ is equal to $\frac{p-1}{2}$. Hence we come to minimum polynomial of the number $2\alpha_N$. One can see that roots of this polynomial are $\{2\cos\frac{2\pi k}{p-1}\}$ $(k = 1, 2, \ldots, \frac{p-1}{2})$

Splitting field of polynomial $x^7 - 1$

Its splitting field $\Sigma(x^7 - 1) = \mathbf{Q}(\varepsilon_7)$, $(\varepsilon_7 = e^{\frac{2\pi i}{7}})$. We know that $[\mathbf{Q}(\varepsilon_7) : \mathbf{Q}] = 6$, because 7 is prime number and polynomial $\frac{x^7-1}{x-1}$ is irreducible.

According to Fundamental Theorem of Galois Theory (the first point) the Galois group contains 6 transformations ($|\Gamma(f)| = [\Sigma(f) : \mathbf{Q}]$). These transformations are uniquely defined by the transformation of one of roots,say ε, because splitting field is just simple extension defined by one of the roots: $\mathbf{Q}(\varepsilon) = \mathbf{Q}(\varepsilon^2) = \cdots = \mathbf{Q}(\varepsilon^6) = \Sigma(x^7 - 1)$. Transformations $\varepsilon \mapsto \varepsilon^k$, $k = 1, 2, 3, 4, 5, 6$, define Galois transformations of the splitting field. Write their action on all roots:

identical transformation

$$1)\quad \varepsilon \mapsto \varepsilon, \varepsilon^2 \mapsto \varepsilon^2, \varepsilon^3 \mapsto \varepsilon^3, \varepsilon^4 \mapsto \varepsilon^4, \varepsilon^5 \mapsto \varepsilon^5, \varepsilon^6 \mapsto \varepsilon^6 \tag{97}$$

and the following transformations

$$2)\quad \varepsilon \mapsto \varepsilon^2, \varepsilon^2 \mapsto \varepsilon^4, \varepsilon^3 \mapsto \varepsilon^6, \varepsilon^4 \mapsto \varepsilon, \varepsilon^5 \mapsto \varepsilon^3, \varepsilon^6 \mapsto \varepsilon^5 \tag{98}$$

$$3)\quad \varepsilon \mapsto \varepsilon^3, \varepsilon^2 \mapsto \varepsilon^6, \varepsilon^3 \mapsto \varepsilon^2, \varepsilon^4 \mapsto \varepsilon^5, \varepsilon^5 \mapsto \varepsilon, \varepsilon^6 \mapsto \varepsilon^4 \tag{99}$$

$$4)\quad \varepsilon \mapsto \varepsilon^4, \varepsilon^2 \mapsto \varepsilon, \varepsilon^3 \mapsto \varepsilon^5, \varepsilon^4 \mapsto \varepsilon^2, \varepsilon^5 \mapsto \varepsilon^6, \varepsilon^6 \mapsto \varepsilon^3 \tag{100}$$

$$5)\quad \varepsilon \mapsto \varepsilon^5, \varepsilon^2 \mapsto \varepsilon^3, \varepsilon^3 \mapsto \varepsilon, \varepsilon^4 \mapsto \varepsilon^6, \varepsilon^5 \mapsto \varepsilon^4, \varepsilon^6 \mapsto \varepsilon^2 \tag{101}$$

$$6)\quad \varepsilon \mapsto \varepsilon^6, \varepsilon^2 \mapsto \varepsilon^5, \varepsilon^3 \mapsto \varepsilon^4, \varepsilon^4 \mapsto \varepsilon^3, \varepsilon^5 \mapsto \varepsilon^2, \varepsilon^6 \mapsto \varepsilon \tag{102}$$

One can see that it is cyclic group. Denote by

$$\tau\colon \varepsilon \mapsto \varepsilon^3 \tag{103}$$

Then we see that

$$\Sigma(x^7 - 1) = \{1, \tau, \tau^2, \tau^3, \tau^4, \tau^5\}, \tau^6 = 1 \tag{104}$$

where we denote by 1 the identity transformation. ($\tau^2\colon \varepsilon \mapsto \varepsilon^2$, $\tau^3\colon \varepsilon \mapsto \varepsilon^6$, $\tau^4\colon \varepsilon \mapsto \varepsilon^4$, $\tau^5\colon \varepsilon \mapsto \varepsilon^5$) This group contain four subgroups

$$H_1 = \{1, \tau, \tau^2, \tau^3, \tau^4, \tau^5\}, H_2 = \{1, \tau^2, \tau^4\}, H_3 = \{1, \tau^3\}, H_6 = \{1\} \qquad (105)$$

(we denote by subindex the index of the subgroup)

The corresponding subfields are:

$$H_1^\dagger = \mathbf{Q}, \quad H_2^\dagger = \mathbf{Q}(\theta_2), H_3^\dagger = \mathbf{Q}(\theta_3), \quad H_6^\dagger = \mathbf{Q}(\varepsilon) \qquad (106)$$

In details

$H_1^\dagger$ it is subfield of elements which are remained fixed under all transformations from the Galois group $\Gamma = H_1$. It is $\mathbf{Q}$.

$H_2^\dagger$ it is subfield of elements which are remained fixed under all transformations from the subgroup H_2. The element $\theta_2 = \varepsilon + \tau^2\varepsilon + \tau^4\varepsilon = \varepsilon + \varepsilon^2 + \varepsilon^4$ belongs to $H_2^\dagger$. $H_2^\dagger = \mathbf{Q}(\theta_2)$, respectively $\mathbf{Q}^*(\theta) = H_2$. $[\mathbf{Q}(\varepsilon) : \mathbf{Q}(\theta_2)] = |H_2| = 3$. $[\mathbf{Q}(\theta_2) : \mathbf{Q}] = 2$.

Remark The attentive reader will note that the fact that $\mathbf{Q}(\theta_2) = H_2^\dagger$ has to be proved. $\mathbf{Q}(\theta_2) \subseteq H_2^\dagger$ because $\theta_2 \in H_2^\dagger$. Hence $[\mathbf{Q}(\varepsilon) : \mathbf{Q}(\theta)] \geq |H_2| = 3$ and respectively $[\mathbf{Q}(\theta_2) : \mathbf{Q}] \leq |\Gamma| : |H_2| = 6 : 3 = 2$. It remains to prove that $[\mathbf{Q}(theta_2) : \mathbf{Q}] > 1$, i.e. $\theta_2 \notin \mathbf{Q}$. If $\theta_2 \in \mathbf{Q}$ then ε is a root of polynomial $\theta_2 = x^4 + x^2 + x$ with rational coefficients of the degree less that 6. This is in the contradiction with the fact that polynomial $\frac{x^7-1}{x-1}$ is irreducible). Hence $[\mathbf{Q}(\theta_2) : \mathbf{Q}] > 1$. Thus we prove that $[\mathbf{Q}(\theta_2) : \mathbf{Q}] = 2$ [18]

$H_3^\dagger$ it is subfield of elements which are remained fixed under all transformations from the subgroup H_3. The element $\theta_3 = \varepsilon + \tau^3\varepsilon = 2\cos\frac{2\pi}{7}$ belongs to $H_3^\dagger$. $\mathbf{Q}^*(\theta_3) = H_3$. (Indeed this proves that $\mathbf{Q}(\theta_3) \subseteq H_3^\dagger$, respectively according to FTGT $H_3 \leq \mathbf{Q}^*(\theta_3)$. In the same way like in the previous example one can check that $\theta_3 \notin \mathbf{Q}$: $\theta_3 = \varepsilon + \varepsilon^6 \Rightarrow \varepsilon\theta_3 = \varepsilon^2 + 1$ $\Rightarrow \varepsilon$ is a root of quadratic equation $x^2 - \theta_3 x + 1 = 0$ over $\mathbf{Q}(\theta)$. $\Rightarrow [\mathbf{Q}(\varepsilon) : \mathbf{Q}(\theta)] = 2$ because θ is real and ε is not real. Hence $[\mathbf{Q}(\theta_3) : \mathbf{Q}] = 3$ and $|\mathbf{Q}^*(\theta_3)| = [\mathbf{Q}(\varepsilon) : \mathbf{Q}(\theta_3)] = 2$. Hence $|H_3| = |\mathbf{Q}^*(\theta_3)| = 2$, i.e. $H_3 = \mathbf{Q}^*(\theta_3)$, $\mathbf{Q}(\theta_3) = H_3^\dagger$.)

$H_6^\dagger$ it is subfield of elements which are remained fixed under identity transformation. It is $\mathbf{Q}(\varepsilon)$.

Splitting field of the polynomial $x^{17} - 1$. Solution of equation $x^{17} - 1 = 0$

Consider polynomial $x^{17} - 1$. Its splitting field $\Sigma(x^{17} - 1) = \mathbf{Q}(\varepsilon_{17})$, ($\varepsilon_{17} = e^{\frac{2\pi i}{17}}$). We know that $[\mathbf{Q}(\varepsilon_{17}) : \mathbf{Q}] = 16$, because 17 is prime number and polynomial $\frac{x^{17}-1}{x-1}$ is irreducible.

[18] This consideration works for arbitrary prime p. Just for this example one can check straightforwardly that θ_2 is not rational: Calculate explicitly $\theta_2^2 = (\varepsilon + \varepsilon^2 + \varepsilon^4)$ and note that θ_2 is a root of quadratic irreducible polynomial. Hence $[\mathbf{Q}(theta_2) : \mathbf{Q}] = 2$

The Galois group $\Gamma(x^{17}-1)$ is cyclic group. It contains 16 elements. They are defined by transformation $\varepsilon \mapsto \varepsilon^k$, $k = 1, 2, \dots, 16$ ($\varepsilon = e^{\frac{2\pi i}{17}}$). Galois group is $\{1, \tau, \tau^2, \dots, \tau^{15}\}$ where ($\tau(\varepsilon) = \varepsilon^3$).

$16 = 2 \times 2 \times 2 \times 2$. Hence we have subgroups of orders 1,2,4,8:

$$\Gamma = H_1 > H_2 > H_4 > H_8 > H_{16} = \{\mathbf{id}\} \tag{107}$$

$$H_1 = \{1, \tau, \tau^2, \dots, \tau^{15}\},\ H_2 = \{1, \tau^2, \tau^4, \tau^6, \tau^8, \tau^{10}, \tau^{12}, \tau^{14}\}$$

$$H_4 = \{1, \tau^4, \tau^8, \tau^{12}\},\ H_8 = \{1, \tau^8\},\ H_{16} = \{1\}$$

Corresponding subfileds are

$$\mathbf{Q} \subset \mathbf{Q}(\theta_2) \subset \mathbf{Q}(\theta_4) \subset \mathbf{Q}(\theta_8) \subset \mathbf{Q}(\varepsilon) \tag{108}$$

where $\mathbf{Q}(\theta_2) = H_2^\dagger$, $\mathbf{Q}(\theta_4) = H_4^\dagger$, $\mathbf{Q}(\theta_8) = H_8^\dagger$

The number of elements in every subgroup is twice more than in the precedent. Hence by Galois Theorem we have the Tower of iterated quadratic extensions. Hence ε is a root of quadratic equation with coefficients in $\mathbf{Q}(\theta_8)$.

Respectively θ_8 is a root of quadratic equation with coefficients in $\mathbf{Q}(\theta_4)$

Respectively θ_4 is a root of quadratic equation with coefficients in $\mathbf{Q}(\theta_2)$

And finally θ_2 is a root of quadratic equation with coefficients in $\mathbf{Q}$.

Thus we see that $\varepsilon = e^{\frac{2\pi i}{17}}$ is iterated quadratic irrationality.

Give a sketch of these calculations

Calculate these equations. First calculate θ_2

$$\theta_2 = (1 + \tau^2 + \tau^4 + \dots + \tau^{16})\varepsilon = \varepsilon + \varepsilon^9 + \varepsilon^{13} + \varepsilon^{15} + \varepsilon^{16} + \varepsilon^8 + \varepsilon^4 + \varepsilon^2 = \tag{109}$$

$$(\varepsilon + \varepsilon^{16}) + (\varepsilon^{15} + \varepsilon^2) + (\varepsilon^{13} + \varepsilon^4) + (\varepsilon^9 + \varepsilon^8)$$

$$2\cos\varphi + 2\cos 2\varphi + 2\cos 4\varphi + 2\cos 8\varphi$$

where $\varphi = \frac{2\pi}{17}$ The second root of quadratic equation is $\theta'_2 = \tau\theta_2$: $\theta + \theta'$ and $\theta \cdot \theta'$ are rationals, because they are invariant under the action of all Galois group:

$$\theta'_2 = \tau\theta_2 = \varepsilon^3 + \varepsilon^{10} + \varepsilon^5 + \varepsilon^{11} + \varepsilon^{14} + \varepsilon^7 + \varepsilon^{12} + \varepsilon^6 \tag{110}$$

$$(\varepsilon^3 + \varepsilon^{14}) + (\varepsilon^5 + \varepsilon^{12}) + (\varepsilon^6 + \varepsilon^{11}) + (\varepsilon^7 + \varepsilon^{10})$$

$$2\cos 3\varphi + 2\cos 5\varphi + 2\cos 6\varphi + 2\cos 7\varphi$$

The straightforward calculations give:

$$\theta_2 + \theta'_2 = -1, \theta_2\theta'_2 = -4$$

We see that θ is a root of quadratic equation

$$x^2 + x - 4 = 0 \tag{111}$$

Now find θ_4 as a root of quadratic equation with coefficients in $\mathbf{Q}(\theta_2)$ The group H_4 is $\{1, \tau^4, \tau^8, \tau^{12}\}$. Hence

$$\theta_4 = (1 + \tau^4 + \tau^8 + \tau^{12})\varepsilon = \varepsilon + \varepsilon^{13} + \varepsilon^{16} + \varepsilon^4 = \tag{112}$$

$$2\cos\varphi + 2\cos 4\varphi$$

and

$$\theta_4' = 2\cos 2\varphi + 2\cos 8\varphi$$

θ_4 is a root of quadratic polynomial

$$x^2 - \theta_2 x - 1 = 0 \tag{113}$$

with coefficient defined by the quadratic polynomial (111).

The last but one step: to calculate $\theta_8 = 2\cos\varphi$ as root of quadratic polynomial.

We see that to solve equation $x^{17} - 1 = 0$ in radicals, i.e. to express $\varepsilon = e^{\frac{2\pi i}{17}}$ in radicals we have to solve three quadratic equations. First equation with rational coefficients to obtain number α, then quadratic equation with coefficients in $\mathbf{Q}(\alpha)$, then...

Spliting field of polynomial $x^{19} - 1$

Its splitting field $\Sigma(x^{19} - 1) = \mathbf{Q}(\varepsilon_{19})$, ($\varepsilon_{19} = e^{\frac{2\pi i}{19}}$). We know that $[\mathbf{Q}(\varepsilon_{19}) : \mathbf{Q}] = 18$, because 19 is prime number and polynomial $\frac{x^{19}-1}{x-1}$ is irreducible.

The Galois group contains 18 transformations defined by transformations $\varepsilon \mapsto \varepsilon^k$, $k = 1, 2, 3, 4, 5, 6, \dots, 18$ It is cyclic group. Denote by

$$\tau \colon \varepsilon \mapsto \varepsilon^2 \tag{114}$$

Then

$$\Sigma(x^{19} - 1) = \{1, \tau, \tau^2, \tau^3, \tau^4, \tau^5 \dots, \tau^{17}\}, \tau^{18} = 1 \tag{115}$$

where we denote by 1 the identity transformation.

$$\tau^2 \colon \varepsilon \mapsto \varepsilon^4,\ \tau^3 \colon \varepsilon \mapsto \varepsilon^8,\ \tau^4 \colon \varepsilon \mapsto \varepsilon^{16}\ , \tau^5 \colon \varepsilon \mapsto \varepsilon^{13}, \tag{116}$$

$$\tau^6 \colon \varepsilon \mapsto \varepsilon^7,\ \tau^7 \colon \varepsilon \mapsto \varepsilon^{14}, \tau^8 \colon \varepsilon \mapsto \varepsilon^9, \tau^9 \colon \varepsilon \mapsto \varepsilon^{18},$$

$$\tau^{10} \colon \varepsilon \mapsto \varepsilon^{17}, \tau^{11} \colon \varepsilon \mapsto \varepsilon^{15}, \tau^{12} \colon \varepsilon \mapsto \varepsilon^{11}, \tau^{13} \colon \varepsilon \mapsto \varepsilon^3, \tau^{14} \colon \varepsilon \mapsto \varepsilon^6,$$

$$\tau^{15} \colon \varepsilon \mapsto \varepsilon^{12}, \tau^{16} \colon \varepsilon \mapsto \varepsilon^5, \tau^{17} \colon \varepsilon \mapsto \varepsilon^{10}, \tau^{18} \colon \varepsilon \mapsto \varepsilon$$

This group contain six subgroups

$$H_1 = \{1, \tau, \tau^2, \tau^3, \tau^4, \tau^5, \dots, \tau^{17}\}, H_2 = \{1, \tau^2, \tau^4, \tau^6, \tau^8, \tau^{10}, \tau^{12}, \tau^{14}, \tau^{16}\}, \tag{117}$$

$$H_3 = \{1, \tau^3, \tau^6, \tau^9, \tau^{12}, \tau^{15}\}, H_6 = \{1, \tau^6, \tau^{12}\}, H_9 = \{1, \tau^9\}, H_{18} = \{1\} \tag{118}$$

(we denote by subindex the index of the subgroup)

According FTGT there are six corresponding subfields. They all are normal extensions, because these subgroups are normal subgroups. These subfields are:

$$H_1^\dagger = \mathbf{Q}, \quad H_2^\dagger = \mathbf{Q}(\theta_2), H_3^\dagger = \mathbf{Q}(\theta_3), \quad H_6^\dagger = \mathbf{Q}(\theta_6), H_9^\dagger = \mathbf{Q}(\theta_9), \quad H_{18}^\dagger = \mathbf{Q}(\varepsilon), \tag{119}$$

According to FTGT:

$$\begin{array}{cccc} H_1 & > H_2 & > H_6 & > H_{18} \\ \mathbf{Q} & \subset \mathbf{Q}(\theta_2) & \subset \mathbf{Q}(\theta_6) & \subset \mathbf{Q}(\varepsilon) \end{array} \tag{120}$$

$$\begin{array}{cccc} H_1 & > H_3 & > H_6 & > H_{18} \\ \mathbf{Q} & \subset \mathbf{Q}(\theta_3) & \subset \mathbf{Q}(\theta_6) & \subset \mathbf{Q}(\varepsilon) \end{array} \tag{121}$$

In more detail:

$H_1^\dagger$ it is subfield of elements which are remained fixed under all transformations from the Galois group $\Gamma = H_1$. It is $\mathbf{Q}$.

$H_2^\dagger$ it is subfield of elements which are remained fixed under all transformations from the subgroup H_2. The element

$$\theta_2 = \varepsilon + \tau^2\varepsilon + \tau^4\varepsilon + \cdots + \tau^{16}\varepsilon = \varepsilon + \varepsilon^4 + \varepsilon^{16} + \varepsilon^7 + \varepsilon^9 + \varepsilon^{17} + \varepsilon^{11} + \varepsilon^6 + \varepsilon^5 \tag{122}$$

belongs to $H_2^\dagger$. It is a root of quadratic polynomial with rational coefficients. Note that another root of this quadratic polynomial is $\theta_2' = \tau\theta_2$ because elements $\theta_2 + \theta_2'$ and $\theta_2 \cdot \theta_2'$ are invariant under the action of all Galois group and are rationals.

$\mathbf{Q}(\theta_2)^* = H_2$. $[\mathbf{Q}(\varepsilon) : \mathbf{Q}(\theta_2)] = |H_2| = 9$. $[\mathbf{Q}(\theta_2) : \mathbf{Q}] = 2$. (the corresponding quadratic polynomial is irreducible, $\theta_2 \notin \mathbf{Q}$, because in other case ε would be a root of polynomial of degree less than 18. This contradicts to irreducibility of polynomial $\frac{x^{19}-1}{x-1}$)

$H_3^\dagger$ it is subfield of elements which are remained fixed under all transformations from the subgroup H_3. The element $\theta_3 = \varepsilon + \tau^3\varepsilon + \tau^6\varepsilon + \tau^9\varepsilon + \tau^{12}\varepsilon + \tau^{15}\varepsilon$ belongs to $H_3^\dagger$. $\mathbf{Q}(\theta_3)^* = H_3$. $[\mathbf{Q}(\varepsilon) : \mathbf{Q}(\theta_3)] = |H_3| = 6$. $[\mathbf{Q}(\theta_2) : \mathbf{Q}] = 3$. θ_3 is a root of cubic equation: According to FTGT $[\mathbf{Q}(\varepsilon) : \mathbf{Q}(\theta_3)] = |H_3| = 6$, $[\mathbf{Q}(\theta_3) : \mathbf{Q}] = |\Gamma| : |H_3| = 18 : 6 = 3$

$H_6^\dagger$ it is subfield of elements which are remained fixed under all transformations from the subgroup H_6. The element $\theta_6 = \varepsilon + \tau^6\varepsilon + \tau^{12}\varepsilon$ belongs to $H_6^\dagger$. $\mathbf{Q}(\theta_6)^* = H_3$. $[\mathbf{Q}(\varepsilon) : \mathbf{Q}(\theta_3)] = |H_6| = 3$. $[\mathbf{Q}(\theta_6) : \mathbf{Q}] = |\Gamma| : |H_6| = 18 : 3 = 6$.

$H_9^\dagger$ it is subfield of elements which are remained fixed under all transformations from the subgroup H_9. The element $\theta_9 = \varepsilon + \tau^9\varepsilon = 2\cos\frac{2\pi}{19}$ belongs to $H_9^\dagger$. $\mathbf{Q}(\theta_9)^* = H_9$. $[\mathbf{Q}(\varepsilon) : \mathbf{Q}(\theta_9)] = |H_9| = 2$. $[\mathbf{Q}(\theta_9) : \mathbf{Q}] = 2$.

$H_{18}^\dagger$ it is subfield of elements which are remained fixed under identity transformation. It is all the field $\mathbf{Q}(\varepsilon)$.

4 Construction by Ruler and compass II

In the subsection 2.4 we staudy constructions by ruler and compass. In particular we showed that if complex number α is constructible then $[\mathbf{Q}(\alpha);\mathbf{Q}] = 2^r$. This gives necessary conditions. What about inverse implication? Of course it is not true that if $[\mathbf{Q}(\alpha):\mathbf{Q}] = 2^r$ then α is constructible. What is sufficient and necessary condition that α is constructible?

We try to answer on this question in this section using basic ideas of Galois theory.. In particular we try to answer the following question: Find all N such that one can divide a circle by ruler and compasses on N equal arcs, i.e. find all N such that a number $\varepsilon_N = e^{\frac{2\pi i}{N}}$ is constructible.

The answer is following.

The prime number p is called Fermat prime number if $p-1$ has not odd divisors, i.e. $p-1 = 2^k$ One can see that if p is Fermat prime number then k has not odd divisors too, i.e. for Fermat prime number

$$p = 2^k + 1, k = 2^n \text{ and } p = 2^{2^n} + 1 \tag{123}$$

(Indeed if k *has* odd divisors then evidently p is not prime) Numbers $2^{2^n} + 1$ sometimes are called Fermat numbers. Fermat number $2^{2^n} + 1$ is *Fermat prime number* if it is prime.

One can see that Fermat numbers $p = 2^{2^n} + 1$ is Fermat prime if $n = 0, 1, 2, 3, 4$, $p = 3, 5, 17, 257, 65337$. But not all Fermat numbers are Fermat prime numbers.

It turns out that Fermat prime numbers are very important for considerations below.

This section is devoted to analysis and proof of the following statement which comes from ancient geometry:

Theorem (Gauss) The number N has property:

$$\textbf{one can divide a circle by ruler and compasses on } N \textbf{ equal arcs.} \tag{124}$$

if and only if the decomposition of N in prime factors have the following form:

$$N = 2^k p_1 \dots p_s\,, \tag{125}$$

where all $p_1, \dots, p_s$ are *different* Fermat prime numbers.

For example circle can be divided on N equal parts if $N = 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, \dots, 30, 32, \dots$ and circle cannot be divided on N equal parts if $N = 7, 9, 11, 13, 18, 19, 21, 22, \dots$

($30 = 2^2 \cdot 3 \cdot 5$, 3 and 5 are Fermat primes, $9 = 3^2$ it is square of odd prime, 7 and 11 are not Fermat primes)

We see that 7 is the smallest number such that circle cannot be divided on the 7 parts with ruler and compasses [19].

Plan of our considerations is following.

To divide circle on N equal arcs by ruler and compasses it is the same that to express all roots of the polynomial

$$x^N - 1 = 0$$

only via arithmetic operations and the extraction of square roots. (We will give exact formulation to this sentence later.)

We will formulate and prove Lemma and Theorem claiming that roots of a polynomial are expressed "via arithmetic operations and the extraction of square roots" if and only if the Galois group of polynomial contains 2^p elements. And finally we will calculate the order of Galois group for polynomial $x^N - 1$ and show that it is equal to 2^p if and only if N has expansion (125).

4.1 Iterated quadratic irrationalities

Take some interval $[AB] = 1$. Then we can construct arbitrary rationals p/q, solve quadratic equations with rational coefficients, solve quadratic equations with coefficients which are roots of quadratic equations and so on... (We did it already in the subsection §2.4.)

Roughly speaking iterated quadratic irrationality it is the number which can be expressed via rational numbers by arithmetic operations and square roots.

Definition.

A complex number $\alpha \in \mathbf{C}$ is called quadratic irrationality if it is a root of quadratic polynomial with rational coefficients.

A complex number $\alpha \in \mathbf{C}$ is called iterated quadratic irrationality if it is a rational number or if it is a root of quadratic polynomial with coefficients which are iterated quadratic irrationalities.

This recursive definition seems to be vicious circle. In fact it states following: a number α is an iterated quadratic irrationality if it is a root of quadratic polynomial p_n whose coefficients are defined in the following way:

[19] May be it is the reason why 50 pence coin has 7 edges?..

one can consider the sequence $\{p_1(x), p_2(x), \ldots, p_n(x)\}$ of quadratic polynomials such that quadratic polynomial $p_1(x)$ has rational coefficients, coefficients of quadratic polynomial p_2 are rational functions of roots of polynomial p_1, coefficients of quadratic polynomial p_3 are rational functions of roots of polynomials p_2 and p_1, coefficients of quadratic polynomial p_4 are rational functions of roots of polynomials p_1, p_2 and p_3 and so on... till we arrive finally to quadratic polynomial p_n such that coefficients of this quadratic polynomial p_n are rational functions of roots of polynomials $p_1, p_2, \ldots, p_{n-1}$

For example consider polynomials $p_2(t) = t^2 + x_1 t + x_2$ where coefficients x_1, x_2 are roots of polynomial $p_1(t) = t^2 - 5t - 1$. Then roots of polynomial $p_2(t)$ are iterated quadratic irrationalities.

Another example: the number

$$\alpha_0 = \sqrt{2 + \sqrt{3 + \sqrt{5}}} + \sqrt{7}\,,\ \text{is a root of polynomial } (t - \alpha_1)^2 - 7 \tag{126}$$

where the number

$$\alpha_1 = \sqrt{2 + \sqrt{3 + \sqrt{5}}} \text{ is a root of polynomial } t^2 - 2 - \alpha_2\,, \tag{127}$$

where the number

$$\alpha_2 = \sqrt{3 + \sqrt{5}} \text{ is a root of polynomial } t^2 - 3 - \alpha_3\,, \tag{128}$$

where the number

$$\alpha_3 = \sqrt{5} \text{ is a root of polynomial } t^2 - 5\,, \tag{129}$$

We see that α_3 is iterated quadratic irrationality, because it is quadratic irrationalitity. Hence α_2 is iterated quadratic irrationality, hence α_1 is iterated quadratic irrationality, hence α_0 is iterated quadratic irrationality.

The notion of iterated quadratic irrationality can be naturally formalized in the following way.

Definition. The complex number $\alpha \in \mathbf{C}$ is called iterated quadratic irrationality if there exists a field $M \subset \mathbf{C}$ containing α such that extension $M : \mathbf{Q}$ can be represented by iterated quadratic extensions, i.e. it can be considered as a Tower of quadratic extensions of $\mathbf{Q}$, i.e. there exist fields $\{M = M_1, M_2, \ldots, M_n\}$ such that

$$\mathbf{Q} \subset M_n \subset M_{n-1} \subset \cdots \subset M_1 = M \ni \alpha \tag{130}$$

and all extensions $M_k : M_{k-1}$, $M_n : \mathbf{Q}$ are quadratic.

For example the quadratic irrationality $\alpha_0 = \sqrt{2 + \sqrt{3 + \sqrt{5}}} + \sqrt{7}$ belongs (126) to field $\mathbf{Q}(\alpha_0)$ and we have a following tower of quadratic extensions of $\mathbf{Q}$:

$$\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{5}) \subseteq \mathbf{Q}(\sqrt{3+\sqrt{5}}) \subseteq \mathbf{Q}(\sqrt{2+\sqrt{3+\sqrt{5}}}) \tag{131}$$

$$\subseteq \mathbf{Q}(\sqrt{2+\sqrt{3+\sqrt{5}}}, \sqrt{7}) = \mathbf{Q}(\sqrt{2+\sqrt{3+\sqrt{5}}} + \sqrt{7}) \tag{132}$$

Another very important **example.** Consider the number

$$\varepsilon_{17} = e^{\frac{2\pi i}{17}}$$

We analysed this number in the fifth example in the last subsection of the previous section. In particular we obtained in (107) that there is a tower of intermediate fields which are iterated quadratic extensions. This means that number $\varepsilon_{17} = e^{\frac{2\pi i}{17}}$ is iterated quadratic irrationality, i.e. circle can be divided on 17 equal arcs by ruler and compasses (It is the problem which was solved by Gauß)

Now simple but very important lemma:

Lemma If number α is an iterated quadratic irrationality then the degree of extension $\mathbf{Q}(\alpha) : \mathbf{Q}$ is equal to 2^r.

The proof is obvious: Suppose α is algebraic irrationality and $\alpha \in M$. Hence by Tower law the degree of extension $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ divides the degree of extension $[M : \mathbf{Q}]$. Hence it follows from Tower Law that $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ is a degree of 2 too. ■

Remark Pay attention that the fact that degree of an extension $\mathbf{Q}(\theta) : \mathbf{Q}$ is equal to 2^k does not follow that θ is iterated quadratic irrationality.

Even this very simple lemma can be used for answering on questions which was posed by Ancient Greeks.

Theorem *The following conditions are equivalent*

a) The number α is constructible in finite number of steps by ruler and compasses

b) The number α is an iterated quadratic irrationality *c) The splitting field of minimum polynomial of number α is extension of rationals of degree 2^k for some k*

Pay attention that the fact that degree of an extension $\mathbf{Q}(\theta) : \mathbf{Q}$ is equal to 2^k does not follow that θ is iterated quadratic irrationality. The condition that the degree of the minimum polynomial of the number α is equal 2^k does not imply that degree of the splitting field will be power of 2 also

From this theorem follows

The condition that the degree of extension $\mathbf{Q}(\alpha) : \mathbf{Q}$ is a power of 2 is necessary condition for number α to be constructed.

This fact was already proved in the subsection §2.4.

Now we prove more: Theorem defines us sufficient condition for onstructibility. In particular Theorem tells that the condition $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^r$ is suffucient condition if $\mathbf{Q}(\alpha)$ is a splitting field of polynomial, i.e. if $\mathbf{Q}(\alpha) : \mathbf{Q}$ is normal extension. (This happens for $\alpha = \varepsilon_N = e^{\frac{2\pi i}{N}}$ where extension is normal extension and ε_N is constructible if and only if $[\mathbf{Q}(vare_N) : \mathbf{Q}] = 2^r$, see in detail next subsection.)

The implication $a \Rightarrow b$) follows from the fact that performing every step in constructing by ruler and compasses we remain in the same field or we pass to the field of degree of extension 2, all constructions by ruler and compasses: intersection of two lines, intersections of line and circle, intersections of two circles lead to linear or quadratic equations. Hence by definition α is iterated irrationality if α can be constructed in finite number of steps by ruler and compasses.

The implication $b \Rightarrow a$) follows from the definition of iterated irrationalities and from the fact that linear and quadratic equations can be solved by ruler and compasses.

the implication $b \Rightarrow c$) can be proved by induction.

Let α be iterated quadratic irrationality and p be minimum polynomial of α $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^k$ and there are fields $\{M_r\}$, $r = 1, \ldots, k$ such that $M_r = \mathbf{Q}(\theta_r)$ where θ_r are iterated quadratic irrationalities.

$$\mathbf{Q} = M_1 \subset M_2 \subset \cdots \subset \mathcal{M}_k = \mathbf{Q}(\alpha)$$

and $[M_{r+1} : M_r] = 2$. Consider all roots of this polynomial $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$, where $n = 2^k$ and normal closure of the last but one field $N_r = \bar{M}_r$. By induction hypothesis this field has degree power of 2. Consider Tower of fields

$$M_{k-1} \subset \mathbf{Q}(\alpha_1) \subseteq \mathbf{Q}(\alpha_1, \alpha_2) \subseteq \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3) \cdots \subseteq \Sigma(p) \qquad (133)$$

All field extensions $\mathbf{Q}(\alpha_i) : N_r$ are isomorphic. Hence their degree is equal to 2 or to 1. Hence in the Tower above all degrees of extension are 1 or 2. Hence degree of splitting field of polynomial p is equal to power of 2.

It remains to prove the last implication $c) \Rightarrow b)$

The proof is founded on the following lemma

Lemma. If group G contains 2^n elements then it contains the series $\{G_n, G_{n-1}, \dots, G_2, G_1\}$ of subgroups such that

$$\{e\} = G_n < G_{n-1} < \cdots < G_2 < G_1 < G_0 = G\,, \tag{134}$$

where all subgroups G_{n+1} have an index 2 in G_n, i.e. order of an every subgroup G_k is equal to 2^{n-k}.

Note that all subgroups G_n are normal in G_{n+1}, because the subgroup of index 2 is always normal. It is evident: if $x \notin H$ then $xx \in H$.

The proof of this lemma see in Appendix 2.

Let f be minimum polynomial of complex number α and Galois Γ group of splitting field $\Sigma = \Sigma(f)$ of polynomial f contains 2^n elements. According to Lemma consider the series of subgroups

$$\{e\} = \Gamma_n < \Gamma_{n-1} < \cdots < \Gamma_2 < \Gamma_1 < \Gamma_0 = G\,, \tag{135}$$

of Galois subgroup and the subfields of $\{\Sigma_r\}$ corresponding to subgroups $\{\Gamma_r\}$.

$$\Sigma_r = \Gamma_r^\dagger = \{a \in \Sigma\colon\ \forall g \in \Gamma_r\ g(a) = a\}, \quad \Gamma_r = \Sigma_r^*$$

According to Fundamental Theorem of Galois Theory

$$\mathbf{Q} = \Sigma_0 < \Sigma_1 < \cdots < \Sigma_{n-2} < \Sigma_{n-1} < \Sigma_n = \Sigma(f)\,. \tag{136}$$

Please, pay attention on the reversing of the order in the formula (136) comparing with formula (178).

The normal extensions $\Sigma_r : \Sigma_{r-1}$ have degree 2 because $\Sigma_r : \Sigma_{r-1} = |\Gamma_r|/|\Gamma_{r-1}| = 2$ (see formula (84), (85).) It means that

every element of field Σ_r is a root of quadratic polynomial with coefficients in field Σ_r. Thus we come to tower of quadratic extensions: All elements of field $\Sigma(f)$ are quadratic irrationalities. ■

From this Proposition and Lemma it follows solutions of classical problems posed by Greeks (see also subsection §2.4):

For example consider the number $\alpha = \sqrt[3]{2}$. $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$. We come to

Corollary The cube cannot be duplicated using ruler and compasses constructions.

Considering equation $x^3 - 3x - 1$. $x = \cos 20^\circ$ and the polynomial is irreducible. Hence $[\mathbf{Q}(\cos 20^\circ) : \mathbf{Q}] = 3$. we come to

Corollary The angle 60° cannot be trisected using ruler and compasses. In other words one cannot divide circle on 9 equal parts.

Consider number π. It is transcendental. $[\mathbf{Q}(\pi) : \mathbf{Q}] = \infty$

Corollary The circle cannot be squared by ruler and compasses.

Consider the numbers $\cos \frac{2\pi}{7}$, $\sin \frac{2\pi}{7}$, $e^{\frac{2\pi i}{7}} = \cos \frac{2\pi}{7} + i \sin \frac{2\pi}{7}$ They are roots of third order and six order irreducible polynomials.

So these numbers *are not iterated quadratic irrationalities.*

Corollary One cannot divide the circle on 7 equal arcs by ruler and compasses

Can we construct the angle $\frac{2\pi}{257}$ by ruler and compasses:

Yes, we can. Indeed consider the number $\alpha = e^{\frac{2\pi i}{257}}$. Its minimum polynomial is $\frac{x^{257}-1}{x-1}$ because $p = 257$ is prime number. $\mathbf{Q}(\alpha)$ is a splitting field and degree of field extension is equal $256 = 2^8$.

4.2 Galois group of equation $x^N - 1$. Regular N-polygon

Apply Theorem for finding all N such that circle can be divided on equal N arcs.

We can divide circle on N equal arcs if and only if the number

$$\varepsilon_N = e^{\frac{2\pi i}{N}}$$

is iterated irrationality. The field $\mathbf{Q}(\varepsilon_N)$ is splitting field of the number ε_N. Hence it follows from the Theorem that

We can divide circle on N equal arcs if and only if if and only if the degree of extension $\mathbf{Q}(\varepsilon_N) : \mathbf{Q}$ is equal to the power of 2.

How to find all wonderful N?

Firs consider the case if $N = p$ is prime number. Then degree of the splitting field of polynomial $x^p - 1$ is equal to $p - 1$. The condition

$$p - 1 = 2^k$$

means that k is a power of 2 too: in other case if k possesses odd divisor ($k = (2q+1)r$) then $p = 2^k + 1$ possesses divisor $2^r + 1$.

So we see that in the case if $N = p$ is prime number then circle can be divided on N equal parts if and only if N is Fermat number: $N = 2^{2^k} + 1$ What happens in general case?

Recalling of Euler function $\varphi(N)$ For integer N denote by $\varphi(N)$ the number of all positive integers from the set $\{1, 2, 3, \dots, n-1\}$ which are coprime with N.

One can see that

$$\varphi(N) = \prod_k p_k^{n_k-1}(p_k - 1)\,, \tag{137}$$

where

$$N = \prod_k p_k^{n_k} \tag{138}$$

is an expansion of N by primes.

For example if $N = 135 = 3^3 \cdot 5$ then $\varphi(N) = 9 \cdot 2 \cdot 4 = 72$

Note that $\varphi(N)$ is equal to the number of invertible elements (units) in the ring $\mathbf{Z}/n\mathbf{Z}$, or the number of automorphisms of the ring $\mathbf{Z}/n\mathbf{Z}$. Another nice property of Euler function is that if a is coprime with N then $a^{\varphi(N)-1} - 1$ is divisible on N. See also appendix 1,

Theorem The order of Galois group of polynomial f_N, i.e. the order of minimum polynomial of the complex number $\varepsilon_N = e^{\frac{2\pi i}{N}}$

$$\textbf{is equal to } \varphi(N) \tag{139}$$

From this Theorem follows Gauss Theorem (124).

$|\Gamma_N|$ is just the degree of minimum polynomial for ε_N. If $N = p$ this a is simple statement $\varphi(p) = p - 1$. Using Eisenstein Test it is easy to see that polynomial

$$x^{p-1} + x^{p-2} + \cdots + 1 = \frac{x^p - 1}{x - 1} \tag{140}$$

is irreducible polynomial. (Consider substitition $x = u + 1$). The same argument works for $N = p^k$, ($\varphi(N) = p^k(p^k - 1)$). It is easy to see that again ε_{p^k} is a root of polynomial

$$x^{p^{k-1}(p-1)} + x^{p^{k-1}(p-2)} + \cdots + 1 = \frac{x^{p^k} - 1}{x^p - 1} \tag{141}$$

In the case if $N = 2p$ life is still not so hard: $\varphi(N) = p$ and polynomial

$$x^{p-1} - x^{p-2} + x^{p-3} - x^{p-3} + \cdots + 1 = \frac{x^{2p} - 1}{(x-1)(x+1)(x^{p-1} + x^{p-2} + \cdots + 1)}\,. \tag{142}$$

For example minimum polynomial for $\varepsilon_{10} = e^{\frac{\pi i}{5}}$ is equal to

$$x^4 - x^3 - x^2 + x - 1$$

In general case situation is more tricky. The explicit expression for minimum polynomial see in Appendix 1.

5 Solutions of equations in radicals and soluble groups. Insoluble quintic.

Definition A group G is called soluble if it contains a finite series of subgroups:

$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq \Gamma_n = G$$

such that 1) $\forall i < n$ G_i is normal subgroup in G_{i+1} (not necessarily in G_{i+k} for $k \geq 2$)

2) Factor-group $G_{i+1}/G_q i$ is abelian.

Theorem The polynomial equation $f(x) = 0$ ($f \in \mathbf{Q}[x]$) is soluble in radicals if and only if Galois group of polynomial f is soluble.

Using this Theorem consider the example of non-soluble quintic.

Proposition Group S_5 of permutations of 5 numbers is non-soluble.

Galois group of quintic is subgroup of S_5. Try to find polynomial such that its Galois group is exactly S_5.

Remark For the case of cubic equation S_3 and all its subgroups are soluble. It is an easy exercise to find polynomials with Galois group equal to given subgroup of group S_3. Indeed Galois group have to be subgroup of S_3. The equation $x^3 - 2$ has Galois group of order 6 and it is just S_3. For polynomial $x^2 - 3x - 1$ Galois group is cyclic subgroup of S_3. The polynomial $(x - a)(x^2 + px + q)$ where $a, p, q \in \mathbf{Q}$ has Galois group S_2 (has trivial Galois group) iff $x^2 + px + q$ has irrational roots.

Finally we consider an example of not soluble quintic.

Theorem The polynomial $x^5 - 6x + 3$ is not soluble by radicals.

To prove this one proves at first that this polynomial is irrdeucible then show that Galois group of this polynomial is indeed all group of permutations of 5 elements.

6 Appendices

6.1 Appendix A. The rational expressions for roots of cubic polynomial

In this appendix we show that irreducible cubic polynomial has roots wich are rationally expressable via each other i.e. $\mathbf{Q}(x_1) = \mathbf{Q}(x_2) = \mathbf{Q}(x_3)$ if and only if the discriminant D:

$$D = d^2, d = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$$

is square of rational It follows from Viète Theorem that

$$D = d^2 = (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$$

is rational expression. (In the case if $f = x^3 + px + q$ $d^2 = -27q^2 - 4p^3$) (See the beginning of the notes.)

It is easy to see that in the case Ia) square root of discriminant **has to be rational**. Indeed in the case Ia) the degree of extension $\mathbf{Q}(x_1, x_2, x_3) : \mathbf{Q}$ is equal to 3 because $\mathbf{Q}(x_1, x_2, x_3) = \mathbf{Q}(x_1)$. The field $\mathbf{Q}(d)$ belongs to the field $\mathbf{Q}(x_1, x_2, x_3)$. Hence by Tower law the degree of extension $\mathbf{Q}(d) : \mathbf{Q}$ can be equal 3 or 1. On the other hand $d^2 = D$ is rational. Hence the degree of the extension $\mathbf{Q}(d) : \mathbf{Q}$ can be 2 or 1. We come to the conclusion that the degree of the extension $\mathbf{Q}(d) : \mathbf{Q}$ is equal to 1. Hence d is rational.

The inverse statement is right too, i.e. in the case Ib) square root of discriminant **has to be not rational**. Or in other words if square root of discriminant of irreducible cubic is rational then then $[\mathbf{Q}(x_1, x_2, x_3)] : \mathbf{Q}] = 3$. We do it by "bare hands" doing straightforward calculations. Later when we will learn Galois theory we will see a very clear proof of this statement. Show first that in the field $\mathbf{Q}(d)$ roots of irreducible cubic polynomial are rationally expressed via each other. Do it. Without loss of generality suppose that $f = x^3 + px + q$, i.e. $x_1 + x_2 + x_3 = 0$ Denote by $u = x_1$ one of the roots and by $x = x_2$ another root of cubic polynomial. Then we have

$$\begin{gathered} x_1x_2 + x_1x_3 + x_2x_3 = p \Rightarrow x^2 + xu + u^2 + p = 0 \\ d = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) = \sqrt{-4p^3 - 27q^2} \Rightarrow \\ 2x^3 + 3ux^2 - 3u^2x + d - 2u^3 = 0 \end{gathered} \tag{143}$$

x is a root of cubic and quadratic equations. Multiply first equation on $2x+u$ and substract the second equation. We come to

$$x = \frac{d - 3u^3 - pu}{6u^2 + 2p} \tag{144}$$

(Denominator is not equal zero, because polynomial is irreducible and $[\mathbf{Q}(u) : \mathbf{Q}] = 3$.)

In other words all roots belong to the extension $\mathbf{Q}(x_1, d)$.

In the case if d is rational then it follows from the formula above that

$x_2, x_3 \in \mathbf{Q}(x_1)$ so the splitting field $\Sigma(f) = \mathbf{Q}(x_1, x_2, x_3) = \mathbf{Q}(x_1)$. It is just the case Ia.

If d is irrational then it is easy to see that $[\mathbf{Q}(x_1, x_2, x_3) : \mathbf{Q}] = 6$. Indeed $d \in \Sigma(f) = \mathbf{Q}(x_1, x_2, x_3)$. On the other hand the extension $\mathbf{Q}(d) : Q$ has the order 2. Hence by Tower Law order of the extension $\mathbf{Q}(x_1, x_2, x_3) : \mathbf{Q}$ cannot be equal to 3. It is equal to 6. It is just the case Ib.

We proved the following Proposition:

Proposition *Let f be irreducible cubic polynomial over $\mathbf{Q}$.*

Then the degree of splitting field is equal to 3 if square root of discriminant is rational. Otherwise it is equal to 6.

Exercise Find dependance of degree of the extension $\Sigma(f) : \mathbf{Q}$ for polynomial $f = x^3 - 3x - q$, where q is such rational number that f is irreducible [20]

Solution It follows from considerations above that $[\Sigma(f) : \mathbf{Q}] = 3$ iff $D = -4p^3 - 27q^2 = 108 - 27q^2$ is square of rational: $D = d^2, d \in \mathbf{Q}$. (We suppose that q obeys the condition that f is irreducible) Solve in rationals the equation

$$27q^2 + d^2 = 108, \qquad \text{where } d = \tfrac{r}{s} \in Q \tag{145}$$

One solution $q = 1, d = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) = \pm 9$ gives famous cubic $x^3 - 3x - 1$[21]. Use Diophantine method: Take a line crossing the point $q = 1, d = \pm 9$: $d = 9 + k(q-1)$ or $q = -9 + k(q-1)$. it is easy to see that $(q, d) \in \mathbf{Q}$ iff $k, w \in \mathbf{Q}$. Substitute in equation: $27q^2 + d^2 - 108 = 27q^2 + 81 + 18k(q-1) + k^2(q-1)^2 = 108$. $27(q^2 - 1) + 18k(q-1) + k^2(q-1)^2 = 0$. Dividing on $q - 1$ we come to

$$q = \frac{k^2 - 18k - 27}{27 + k^2}, \qquad d = \frac{243 - 9k^2 - 54k}{k^2 + 27} \tag{146}$$

We come to plenty examples of cubic polynomials such that square root of discriminant is rational. E.g. take $k = 1$ we come to the polynomial

$$q = -\frac{7}{11}, d = \frac{45}{11}.$$

Cubic equation

$$x^3 - 3x - \frac{11}{7} \tag{147}$$

has the same intriguing property that $x^3 - 3x - 1$: its roots are rationally expressed via each other.

[20] in other words the equation $q = x^3 - 4x$ has no solutions in rationales. One can see that sufficient condition is that for $q = \frac{m}{n}$ the integer n be free from cubes, i.e. for every prime number $l$the number l^3 does not divide n.

[21] You see that in fact the following identity is proved: $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) = 8(\cos 20^\circ + \cos 40^\circ)(\cos 40^\circ + \cos 80^\circ)(\cos 20^\circ + \cos 80^\circ) = 9$

6.2 Appendix B. Calculation of Galois group using primitive extension.

Let $L : K$ be finite normal separable extension. We already formulated theorem that this extension is a splitting field for some polynomial f (see subsection "Normal extensions") (f can be reducible too: e.g. $\mathbf{Q}(\sqrt{2}, \sqrt{5})$ is a splitting field for a polynomial $(t^2-2)(t^2-3)$).

One can calculate Galois group considering primitive element of field extension. For example let $L : \mathbf{Q}$ be finite normal extension of $\mathbf{Q}$, $L = \Sigma(f) = \mathbf{Q}(x_1, \dots, x_n)$ where $x_1, \dots, x_n$ are (complex) roots of f. (One can consider $\Sigma(f)$ as subfield of $\mathbf{C}$).

Let θ be a primitive element of splitting field (see the Theorem about splitting element in the section 2):

$$\Sigma(f) = \mathbf{Q}(x_1, \dots, x_n) = \mathbf{Q}(\theta)$$

Denote by R minimum polynomial of θ. We call this polynomial **resolvent polynomial of polynomial f**

Let $\theta_1, \theta_2 \dots, \theta_N$ be roots of resolvent polynomial. Denote by $\theta = \theta_1$. Extension $\mathbf{Q}(\theta) = \Sigma(p)$ is normal extension. Hence all roots θ_i of irreducible polynomial $R(x)$ belong to $\mathbf{Q}(\theta_1)$. Thus all extensions $\mathbf{Q}(\theta_i)$ are equal to extension $\mathbf{Q}(\theta)$:

$$\Sigma(f) = \mathbf{Q}(\theta_1) = \cdots = \mathbf{Q}(\theta_N) \tag{148}$$

Every transformation $\theta \to \theta_i$ defines automorphism φ_i of the field $\Sigma(f) = \mathbf{Q}(\theta)$. Vice versa every automorphism φ is uniquely defined by its value on θ and this value is equal to θ_i: $\varphi(\theta) = \theta_i$.

Every automorphism φ_i generates the permutation of roots. (But not every permutation of roots defines automorphism.)

One can see that $N \geq n$ and $N|n!$ in the case if f is irreducible polynomial. Indeed N is the number of elements in the subgroup Γ of the group of permutation S_n. Hence $|\Gamma|$ divides $|S_n| = n!$. We see in particularly that the degree N of resolvent polynomial is less or equal $n!$.

Let R be minimum polynomial of a primitive element of the extension $\Sigma(f)$, (resolvent polynomial of polynomial f) Then Galois group of polynomial f contains $N = \deg R$ elements. The Galois group is a group of automorphisms $\{\varphi_i\}$ where automorphism φ_i is uniquely defined by the condition $\tau_i(\theta_1) = \theta_i$, where θ_i are roots of resolvent polynomial R

Consider examples.

Example 1 Consider again polynomial $x^4 - 5x^2 + 6$ (See example in the subsection 3.1) Its roots are $x_{1,2} = \pm\sqrt{3}$, $x_{3,4} = \pm\sqrt{2}$. We noted that Galois group contains four elements $\{\mathbf{id}, \tau, \sigma, \tau \circ \sigma\}$ where:

$$\begin{aligned} \tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} \\ \sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\ \tau \circ \sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \end{aligned} \tag{149}$$

for every element $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in \Sigma(f)$, $a, b, c, d \in \mathbf{Q}$.

Calculate this Galois group using primitive element. Splitting field $\Sigma(f) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. We know already that primitive element of this extension is $\sqrt{2}+\sqrt{3}$: $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2}+$

$\sqrt{3}$). Minimum polynomial of primitive element $\theta = \sqrt{2} + \sqrt{3}$ (resolvent polynomial) is equal to $x = t^4 - 10t + 1$ (if $t = \sqrt{2} + \sqrt{3}$), then $t^2 = 5 + 2\sqrt{6}$, $(t^2 - 5)^2 - 24 = t^4 - 10t^2 + 1$. This polynomial is irreducible $b \Rightarrow a$ $[\mathbf{Q}(\theta) : \mathbf{Q}] = 4$). Roots of this polynomial are equal to

$$\theta = \theta_1 = \sqrt{2} + \sqrt{3},\ \theta_2 = \sqrt{2} - \sqrt{3},\ \theta_3 = -\sqrt{2} + \sqrt{3},\ \theta_4 = -\sqrt{2} - \sqrt{3}, \tag{150}$$

Galois automorphisms are $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ where

$$\begin{array}{lll} \varphi_1 \colon \theta_1 \to \theta_1, & \varphi_1(\sqrt{2} + \sqrt{3}) = \sqrt{2} + \sqrt{3}, & \varphi_1 = \mathbf{id} \\ \varphi_2 \colon \theta_1 \to \theta_2, & \varphi_2(\sqrt{2} + \sqrt{3}) = \sqrt{2} - \sqrt{3}, & \varphi_2 = \sigma \\ \varphi_3 \colon \theta_1 \to \theta_3, & \varphi_3(\sqrt{2} + \sqrt{3}) = -\sqrt{2} + \sqrt{3}, & \varphi_1 = \tau \\ \varphi_4 \colon \theta_1 \to \theta_4, & \varphi_4(\sqrt{2} + \sqrt{3}) = -\sqrt{2} - \sqrt{3}, & \varphi_1 = \tau \circ \sigma \end{array} \tag{151}$$

Example 2 Cubic polynomial $x^3 - 2$

Consider polynomial $f = x^3 - 2$ over $\mathbf{Q}$. Its splitting field

$$\Sigma(x^3 - 2) = \mathbf{Q}(x_1, x_2, x_3)\,, \quad x_1 = \sqrt[3]{2}\,, x_2 = \sqrt[3]{2}e^{\frac{2\pi i}{3}}\,, x_3 = \sqrt[3]{2}e^{\frac{-2\pi i}{3}}\,. \tag{152}$$

In other words

$$x_1 = \sqrt[3]{2}\,, x_{2,3} = \sqrt[3]{2}e^{\frac{\pm 2\pi i}{3}} = \sqrt[3]{2}\left(-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right)\,,$$

$$\Sigma(x^3 - 2) = \mathbf{Q}(x_1, x_2, x_3) = \mathbf{Q}(\sqrt[3]{2}, i\sqrt{3})\,.$$

Note that degree of extension $\Sigma(x^3 - 2) : \mathbf{Q}$ is equal to 6. Indeed $\Sigma(x^3 - 2) = \mathbf{Q}(\sqrt[3]{2}, i\sqrt{3})$. One can see that polynomial $x^3 - 2$ is irreducible over field $\mathbf{Q}(i\sqrt{3})$ (as well as it is irreducible over $\mathbf{Q}$). Hence by Tower Law $[\Sigma(x^3 - 2) : \mathbf{Q}] = [\Sigma(x^3 - 2) : \mathbf{Q}(i\sqrt{3})] \cdot [\mathbf{Q}(i\sqrt{3}) : \mathbf{Q}] = 6$. Another way to see it is to note that the filed $\Sigma(x^3 - 2)$ contains subfield $\mathbf{Q}(\sqrt[3]{2})$ of the degree 3 ($[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$) and subfield $\mathbf{Q}(i\sqrt{3})$ of the degree 2 ($[\mathbf{Q}(i\sqrt{3}) : \mathbf{Q}] = 3$) of degree 2. On the other hand the degree of the field $\Sigma(f)$ over $\mathbf{Q}(\sqrt[3]{2})$ is equal 2 or 1. Hence $[\Sigma(f) : \mathbf{Q}] = 6$. One can see that

$$\theta = x_2 - x_3 = i\sqrt{3}\sqrt[3]{2}\,.$$

is a primitive element of the extension: $\mathbf{Q}(i\sqrt{3}\sqrt[3]{2}) = \Sigma(x^3 - 2)$. (See also (57),(58), (61)). Element $\theta = i\sqrt[3]{2}\sqrt{3}$ is a root of polynomial $x^6 + 108$. $x^6 + 108$ is resolvent polynomial for polynomial $x^3 - 2$. (It is minimum polynomial because $[\Sigma(x^3 - 2) : \mathbf{Q}] = 6$). Roots are expressed via θ which is a root of a polynomial $x^6 + 108$. This polynomial is *resolvent* polynomial for the polynomial $x^3 - 2$. [22]

The Resolvent polynomial $x^6 + 108$ has 6 roots:

$$\theta_k = \theta e^{\frac{2\pi(k-1)}{6}}\,, \quad \text{where} \quad k = 1, 2, 3, 4, 5, 6$$

These roots are vertices of hexagon.

[22] in the case if $f = x^3 - 3x - 1$ then resolvent polynomial $R = f$, in the case if $f = x^5 - 1$ then resolvent polynomial is equal to $x^4 + x^3 + x^2 + x + 1$

$$\theta = \theta_1 = i\sqrt[3]{2}\sqrt{3}\,, \tag{153}$$

$$\theta_2 = \theta e^{\frac{2\pi i}{6}} = \theta e^{\frac{\pi i}{3}} = i\sqrt[3]{2}\sqrt{3}\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\,, \tag{154}$$

$$\theta_3 = \theta e^{\frac{4\pi i}{6}} = \theta e^{\frac{2\pi i}{3}} = i\sqrt[3]{2}\sqrt{3}\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)\,, \tag{155}$$

$$\theta_4 = \theta e^{\frac{6\pi i}{6}} = -\theta = -i\sqrt[3]{2}\sqrt{3}\,, \tag{156}$$

$$\theta_5 = \theta e^{\frac{8\pi i}{6}} = \theta e^{\frac{-2\pi i}{3}} = i\sqrt[3]{2}\sqrt{3}\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) \tag{157}$$

$$\theta_6 = \theta e^{\frac{10\pi i}{6}} = \theta e^{\frac{-\pi i}{3}} = i\sqrt[3]{2}\sqrt{3}\left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) \tag{158}$$

Note that roots of cubic polynomial $x^3 - 2$ are expressed via primitive element in the following way:

$$x_1 = -\frac{6}{\theta^2},\ x_2 = \frac{3}{\theta^2} + \frac{\theta}{2},\ x_3 = \frac{3}{\theta^2} - \frac{\theta}{2}$$

See (58) Galois group of polynomial x^3-2 contains exactly 6 automorphsims $\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6$ where $\varphi_i(\theta) = \theta_i$. It is just all permutations of roots of polynomial $x^3 - 2$: (φ_1 is identical transformations.)

Show e.g. that φ_2 is transposition of two roots and φ_3 is cyclic permutation:

Consider transformation $\varphi_2\colon \theta_1 \to \theta_2$. Then according to the formula expressing roots x_1, x_2, x_3 we see that

$$\begin{aligned} x_1 = -\tfrac{6}{\theta^2} \to -\tfrac{6}{\theta_2^2} &= \tfrac{-6}{(\theta e^{\frac{\pi i}{3}})^2} = \sqrt[3]{2}e^{\frac{-2\pi i}{3}} = x_3, \\ x_3 = \tfrac{3}{\theta^2} - \tfrac{\theta}{2} &\to \tfrac{3}{\theta^2 e^{\frac{2\pi i}{3}}} - \tfrac{\theta e^{\frac{\pi i}{3}}}{2} = x_1 \\ x_2 = \tfrac{3}{\theta^2} + \tfrac{\theta}{2} &\to \tfrac{3}{\theta^2 e^{\frac{2\pi i}{3}}} + \tfrac{\theta e^{\frac{\pi i}{3}}}{2} = x_2 \end{aligned} \tag{159}$$

Hence transformation φ_2 is transposition of roots x_1, x_3: $x_1 \to x_3, x_3 \to x_1$, the root x_2 remains fixed.

Consider transformation $\varphi_3\colon \theta_1 \to \theta_3$. Then according the formula expressing roots x_1, x_2, x_3 we see that

$$\begin{aligned} x_1 = -\tfrac{6}{\theta^2} \to -\tfrac{6}{\theta_3^2} &= \tfrac{-6}{(\theta e^{\frac{2\pi i}{3}})^2} = \sqrt[3]{2}e^{\frac{2\pi i}{3}} = x_1 e^{\frac{2\pi i}{3}} = x_2, \\ x_2 = \tfrac{3}{\theta^2} + \tfrac{\theta}{2} &\to \tfrac{3}{\theta^2 e^{\frac{4\pi i}{3}}} + \tfrac{\theta e^{\frac{2\pi i}{3}}}{2} = x_2 e^{\frac{2\pi i}{3}} = x_3 \\ x_3 = \tfrac{3}{\theta^2} - \tfrac{\theta}{2} &\to \tfrac{3}{\theta^2 e^{\frac{4\pi i}{3}}} - \tfrac{\theta e^{\frac{2\pi i}{3}}}{2} = x_3 e^{\frac{2\pi i}{3}} = x_1 \end{aligned} \tag{160}$$

We see that φ_3 is cyclic permutation of roots. In the same way one can consider other transformations.

6.3 Appendix C. Circle functions $\Phi_N(x)$

Consider the problem of expanding polynomial $x^N - 1$ on irreducible factors. If N is prime it is evident. In general case of course trivial factor is $(x-1)$. Note that even in the case $N = p_1 p_2$ it is not easy to calculate answer on pedestrians level.

For example if $N = 15 = 3 \cdot 5$

$$(x^{15} - 1) = (x^5 - 1)(x^{10} + x^5 + 1) = (x-1)(1 + x + x^2 + x^3 + x^4)(x^1 0 + x^5 + 1)$$

We are sure that there is irreducible factor $x^2 + x + 1$ How to extract it?
$(x^{15} - 1)$ has roots $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}, \bar{13}, \bar{14}\}$, where we denote by $\bar{k} = e^{\frac{2\pi ik}{15}}$ hence we see that polynomial $(1 + x + x^2 + x^3 + x^4)$ has roots $\{\bar{3}, \bar{6}, \bar{9}, \bar{12}\}$ and polynomial $(x^{10} + x^5 + 1)$ has ten roots $\{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}, \bar{10}, \bar{11}, \bar{13}, \bar{14}\}$ On the other hand polynomial $x^2 + x + 1$ has roots $\{\bar{5}, \bar{10}\}$. Hence the expression

$$\frac{(x^{10} + x^5 + 1)}{x^2 + x + 1}.$$

is a polynomial with eight roots $\{\bar{1}, \bar{2}, \bar{4}\bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$ It is polynomial for number ε_{15}. One can see that this is minimum polynomial. Now note that its roots are $\{\bar{k}\}$ where k is coprime with 15.

Denote by
$Phi_{15}(x)$ the polynomial with roots $\{\bar{1}, \bar{2}, \bar{4}\bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$ (which correspond to numbers coprime with 15). Denote in general by $\varphi_N(x)$ the polynomial with roots $\{\bar{a_1}, \dots, \bar{a_k}\}$, where a_i are numbers coprime with N. (We denote by $\bar{a}$ the root $e^{\frac{2pia}{N}}$).

One can see that

$$\Phi_{15}(x)\Phi_3(x)\Phi 5(x)\Phi_1(x) = (x^{15} - 1) \tag{161}$$

where $1, 3, 5, 15$ are divisors of 15.

Indeed $\Phi_{15}(x)$ has roots

$$\{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\},$$

(numbers $\{1, 2, 4, 7, 8, 11, 13, 14\}$ are coprime with 15)

$\Phi_5(x)$ has roots

$$\{\bar{3}, \bar{6}, \bar{9}, \bar{12}\},$$

(numbers $\{1, 2, 3, 4, 4\}$ are coprime with 5, $3 = 1 \cdot 3, 6 = 2 \cdot 3, 9 = 3 \cdot 3, 12 = 4 \cdot 3$),

$\Phi_3(x)$ has roots

$$\{\bar{5}, \bar{10}\},$$

(numbers $\{1, 2\}$ are coprime with 3) and $\Phi_1(x)$ has roots

$$\{\bar{0}\},$$

Thus we come to all roots

$$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}, \bar{12}, \bar{13}, \bar{14}\},$$

of polynomial $x^{15} - 1$. It is evident that this is right for every N:

$$\prod_{d = \text{divisors of N}} \Phi_d(x) = x^N - 1 \tag{162}$$

For example:

$$\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_5(x)\Phi_6(x)\Phi_{10}(x)\Phi_{15}(x)\Phi_{30}(x) = x^{30} - 1$$

We see that the last formula gives us the proof that polynomial $\Phi_N(x)$ has rational coefficients, because it can be obtained step by step from formula (162).

Moreover one can prove that polynomials φ_N are irreducible.

Theorem Minimum polynomial of $\varepsilon_N = e^{\frac{2\pi i}{N}}$ has degree $\varphi(N)$ (amount of numbers coprime with N). It is given by formula (162).

For example calculate some $\Phi_N(x)$:

$$\Phi_1(x) = x - 1\, \Phi_2(x) = x + 1,\ \ \Phi_3(x) = x^2 + x + 1$$

$$\Phi_4(x) = \frac{x^4 - 1}{\Phi_1(x)\Phi_2(x)} = \frac{x^4 - 1}{(x-1)(x+1)} = x^2 + 1$$

For every $N = p^2$

$$\Phi_N(x) = \frac{x^{p^2} - 1}{x^p - 1}$$

$$\Phi_5(x) = \frac{x^5 - 1}{\Phi_1(x)} = x^4 + x^3 + x^2 + x + 1\,,$$

(5 is prime it is easy)

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = x^2 - x + 1$$

$$\Phi_{10}(x) = \frac{x^{10} - 1}{\Phi_1(x)\Phi_2(x)\Phi_5(x)} = x^4 - x^3 + x^2 - x + 1$$

For every $N = 2p$

$$\Phi_N = \frac{x^p + 1}{x + 1}\,.$$

Now calculate for $N = 3 \cdot 5$

$$\Phi_{15}(x) = \frac{x^{15} - 1}{\Phi_1(x)\Phi_3(x)\Phi_5(x)} = \frac{\left(x^{15} - 1\right)\Phi_1(x)}{\left(\Phi_1(x)\Phi_5(x)\right)\left(\Phi_1(x)\Phi_5(x)\right)} =$$

$$\frac{\left(x^{15} - 1\right)(x-1)}{\left(x^5 - 1\right)\left(x^3 - 1\right)} = \frac{x^{10} + x^5 + 1}{x^2 + x + 1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

It is nice identity...

In general if $N = p_1 p_2$ ($p_1 \neq p_2$) then

$$\Phi_{p_1 p_2}(x) = \frac{\left(x^{p_1 p_2} - 1\right)(x-1)}{\left(x^{p_1} - 1\right)\left(x^{p_2} - 1\right)}\,.$$

Now calculate $\Phi_{30}(x)$.

$$\Phi_{30}(x) = \frac{x^{30}-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_5(x)\Phi_6(x)\Phi_{10}(x)\Phi_{15}(x)} \tag{163}$$

Note that according to indetity

$$\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_5(x)\Phi_6(x)\Phi_{10}(x)\Phi_{15}(x) =$$

$$(\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x))\,\Phi_5(x)\Phi_{10}(x)\Phi_{15}(x) =$$

$$= \bigl(x^6-1\bigr)\,\Phi_5(x)\Phi_{10}(x)\Phi_{15}(x) =$$

$$\frac{\bigl(x^6-1\bigr)\,[\Phi_1(x)\Phi_2(x)\Phi_5(x)\Phi_{10}(x)]\,[\Phi_1(x)\Phi_3(x)\Phi_5(x)\Phi_{15}(x)]\,\Phi_1}{[\Phi_1(x)\Phi_2(x)]\,[\Phi_1(x)\Phi_3(x)]\,[\Phi_1(x)\Phi_5(x)]} =$$

$$\frac{\bigl(x^6-1\bigr)\bigl(x^{10}-1\bigr)\bigl(x^{15}-1\bigr)(x-1)}{(x^2-1)(x^3-1)(x^5-1)}.$$

Hence we come to identity

$$\Phi_{30}(x) = \frac{\bigl(x^{30}-1\bigr)\bigl(x^2-1\bigr)\bigl(x^3-1\bigr)\bigl(x^5-1\bigr)}{(x^6-1)(x^{10}-1)(x^{15}-1)(x-1)} = \tag{164}$$

$$\frac{\bigl(x^{30}-1\bigr)}{(x^{15}-1)} \cdot \frac{\bigl(x^5-1\bigr)}{(x^{10}-1)} \cdot \frac{\bigl(x^3-1\bigr)}{(x^6-1)} \cdot \frac{\bigl(x^2-1\bigr)}{(x^{-}1)} = \tag{165}$$

$$\frac{(x^{15}+1)(x+1)}{(x^5+1)(x^3+1)} = \tag{166}$$

$$\frac{x^{10}-x^5+1}{x^2-x+1} = \tag{167}$$

$$= x^8+x^7-x^5-x^4-x^3+x+1 = \Phi_{15}(-x) \tag{168}$$

Yes do not be surprised! If N is odd then I think it is right that

$$\Phi_{2N}(x) = \Phi_N(x)$$

because $x^{2N-1} = \Phi_{2N}(x)\Phi_N(x)\cdots = \Phi_{2N}(x)$ (Try to prove by induction). nevertheless: If $N = p_1p_2p_3$ and all these primes are distinct then:

$$\Phi_N(x) = \frac{(x^{p_1p_2p_3}-1)(x^{p_1}-1)(x^{p_2}-1)(x^{p_3}-1)}{(x^{p_1p_2}-1)(x^{1p_1p_3}-1)(x^{p_2p_3}-1)(x-1)}.$$

One can prove the following improtant properties of circle functions

Proposition
The circlle function $\Phi_N(x)$ obey the following conditions:

$$\Phi_{4p+2}(x) = \Phi_{2p+1}(-x)\ \Phi_{8p+4}(x) = \Phi_{2p+1}(-x^2) \tag{169}$$

It is not worthless to consider these functions for $N = 1, 2, 3, 4, \ldots, ...$:

$$\Phi_1(x) = x-1\,,\ \Phi_2(x) = x+1\,,\ \Phi_3(x) = x^2+x+1\,,\ \Phi_4(x) = x^2+1\,, \tag{170}$$

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1\,,\; \Phi_6(x) = x^2 - x + 1\,, \tag{171}$$

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\;, \Phi_8(x) = x^4 + 1\,,\; \Phi_9(x) = x^6 + x^3 + 1\,,\,, \tag{172}$$

$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1\;, \Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\,,\,, \tag{173}$$

$$\Phi_{12}(x) = x^4 - x^2 + 1\;, \tag{174}$$

$$\Phi_{13}(x) = x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\,,\,, \tag{175}$$

$$\Phi_{14}(x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1\;, \Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1\,,\,, \tag{176}$$

Write using circle functions expansions:

$$x^{30} - 1 = \Phi_{30}(x)\Phi_{15}(x)\Phi_{10}(x)\Phi_6(x)\Phi_5(x)\Phi_3(x)\Phi_2(x)\Phi_1(x) =$$

$$(x^8 + x^7 - x^5 - x^4 - x^3 + x + 1)(x^8 - x^7 + x^5 - x^4 + x^3 - x + 1)\times$$

$$(x^4 - x^3 + x^2 - x + 1)(x^2 - x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x + 1)(x - 1)\,,$$

$$x^{20} - 1 = \Phi_{20}(x)\Phi_{10}(x)\Phi_5(x)\Phi_4(x)\Phi_2(x)\Phi_1(x) =$$

$$(x^8 - x^6 + x^4 - x^2 + 1)(x^4 - x^3 + x^2 - x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + 1)(x + 1)(x - 1)\,,$$

$$x^{12} - 1 = \Phi_{12}(x)\Phi_6(x)\Phi_4(x)\Phi_3(x)\Phi_2(x)\Phi_1(x) =$$

$$(x^4 - x^2 + 1)(x^2 - x + 1)(x^2 + 1)(x^2 + x + 1)(x + 1)(x - 1)$$

$$x^{36} - 1 = \Phi_{18}(x)\Phi_{12}(x)\Phi_9(x)\Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x) =$$

$$.......(x^4 - x^2 + 1)(x^6 + x^3 + 1)(x^2 - x + 1)(x^2 + 1)(x^2 + x + 1)(x + 1)(x - 1)$$

$$x^8 - 1 = \Phi_8(x)\Phi_4(x)\Phi_2(x)\Phi_1(x) =$$

$$(x^4 + 1)(x^2 + 1)(x + 1)(x - 1)$$

6.4 Appendix D. Every group of order 2^{k+1} possesses subgroup of the order 2^k

In this Appendix we will prove the lemma

Lemma. If group G contains 2^n elements then it contains the series $\{G_n, G_{n-1}, \ldots, G_2, G_1\}$ of subgroups such that

$$\{e\} = G_n < G_{n-1} < \cdots < G_2 < G_1 < G_0 = G\,, \tag{177}$$

where all subgroups G_{k+1} have an index 2 in G_k, i.e. order of an every subgroup G_k is equal to 2^{n-k}.

Proof of the lemma

Prove it by induction.

For $n = 1$ $G_1 = \{e\} < G$. Suppose lemma is proved for $n \leq k$. Consider G such that $|G| = 2^{k+1}$.

Prove first non-triviality of the centre of the group G, i.e. the existence of element $b \neq 1$ such that $bg = gb$ for every $g \in G$. Consider for every g the stability subgroup H_g and the class $\mathcal{O}_g$ of conjugated elements:

$$H_g = \{h:, hgh^{-1} = g\} \quad \mathcal{O}_g = \{h^{-1}gh\,, h \in G\}\,.\,, \mathcal{O}_g = G/H_g\,.$$

Let $\{g_1, g_2, \dots . g_r\}$ are all representatives of different classes. Then

$$\sum_r |\mathcal{O}_{g_r}| = 2^{k+1}\,.$$

all $|\mathcal{O}_{g_r}|$ are powers of 2 because the number of elements in $\mathcal{O}_{g_r}$ is divisor of $|G|$. The class $\mathcal{O}_e$ contains one element. The sum above is even number. Hence there exists $b \neq e$ such that class $\mathcal{O}_b$ contains odd number of elements. But all classes $\mathcal{O}_g$ contain powers of 2 number elements because the number of elements in $\mathcal{O}_{g_r}$ is divisor of $|G|$. Hence the odd number $|\mathcal{O}_b|$ is equal to 1, i.e. b commutes with all elements of G.

Now consider cyclic group generated by b. $\{1, b, b^2, \dots, b^r\}$. It contains 2^s elements, as subgroup of G. Hence it has an element $a = b^{\frac{r+1}{2}}$. $a^2 = e$ and a commutes with all group. Hence $H = \{e, a\}$ is a normal subgroup which contains two elements.

Consider factor-group

$$\tilde{G} = G/H$$

The group $\tilde{G}$ contains 2^k elements. Hence by inductive hypothesis it contains the series $\{\ \tilde{G}_n, \tilde{G}_{n-1}, \dots, \tilde{G}_2, \tilde{G}_1\}$ of subgroups such that

$$\{e\} = \tilde{G}_n < \tilde{G}_{n-1} < \cdots < \tilde{G}_2 < \tilde{G}_1 < \tilde{G}_0 = \tilde{G}\,, \tag{178}$$

where all subgroups $\tilde{G}_{k+1}$ have an index 2 in $\tilde{G}_k$, i.e. order of an every subgroup $\tilde{G}_k$ is equal to 2^{n-k}.

Now one can easy reconstruct subgroups G_r in G via groups $\tilde{G}_r$ and subgroup H. If $\{[a_i]\}$ are elements of group G_r then elements $\{a_i, a_i b\}$ consist group G_r obeying (178).