Зміст

1 Рівняння третьої та четвертої степені

1.1 Формула для знаходження коренів рівняння третьої степені.(Формула Кардано-Тарталья)

Для початку розглянемо куб суми: $(a+b)^3 = a^3 + b^3 + 3ab(a+b)$ нехай $x = a+b$, тоді отримуємо кубічне рівняння:

$$x^3 - 3abx - a^3 - b^3 \tag{1}$$

. **Перший спосіб**

Поміти, що $(a+b)$ є його корнем.

Спробуємо звести довільне кубічне рівняння $a\widetilde{x}^3 + b\widetilde{x}^2 + c\widetilde{x} + d = 0$ до такого вигляду (1):

1. Обнулім коеффіціент при $\widetilde{x}^2$. Для цього після ділення рівняння на a:
$\widetilde{x}^3 + \frac{b}{a}\widetilde{x}^2 + \frac{c}{a}\widetilde{x} + \frac{d}{a} = 0$, застосуємо заміну $\widetilde{x} = x - \frac{b}{3a}$ отримуємо

$$\left(x - \frac{b}{3a}\right)^3 + \frac{b}{a}\left(x - \frac{b}{3a}\right)^2 + \frac{c}{a}\left(x - \frac{b}{3a}\right) + \frac{d}{a} = 0$$

$$\left(x^3 - \cancel{\frac{b}{a}x^2} + \frac{b^2}{3a^2}x - \frac{b^3}{27a^3}\right) + \left(\cancel{\frac{b}{a}x^2} - \frac{2b}{3a}x + \frac{b^2}{9a^2}\right) + \left(\frac{c}{a}x - \frac{cb}{3a^2}\right) + \frac{d}{a} = 0$$

$$x^3 + x\Bigg(\underbrace{\frac{b^2}{3a^2} - \frac{2b}{3a} + \frac{c}{a}}_{p}\Bigg) + \Bigg(\underbrace{\frac{d}{a} - \frac{b^3}{27a^3} + \frac{b^2}{9a^2} - \frac{cb}{3a^2}}_{q}\Bigg) = 0$$

$$x^3 + px + q = 0$$

2. Тепер зведемо рівняння $x^3 + px + q = 0$ до вигляду (1). Отримуємо систему відностно a і b:

$$\begin{cases} ab = -\dfrac{p}{3} \\ a^3 + b^3 = -q \end{cases} \Rightarrow \begin{cases} a^3b^3 = -\dfrac{p^3}{27} \\ a^3 + b^3 = -q \end{cases} \quad (*)$$

З системи $(*)$ видно, що a^3 с b^3 є корнями квадратного рівняння(По формулі Віетта):

$$x'^2 + qx' - \frac{p^3}{27} = 0$$

його дискрименант дорівнює: $\mathfrak{D} = q^2 + \dfrac{4p^3}{27}$, а самі корні:

$$\begin{cases} a^3 = \dfrac{-q + \sqrt{q^2 + \dfrac{4p^3}{27}}}{2} \\ b^3 = \dfrac{-q - \sqrt{q^2 + \dfrac{4p^3}{27}}}{2} \end{cases} \quad \begin{cases} a^3 = -\dfrac{q}{2} + \sqrt{\dfrac{q^2}{4} + \dfrac{p^3}{27}} \\ b^3 = -\dfrac{q}{2} - \sqrt{\dfrac{q^2}{4} + \dfrac{p^3}{27}} \end{cases}$$

Звідки, так як ми звели р-ня до вигляду (1), то $x = a + b$ є корнем, та підставляя вираження для a и b отримуємо формулу:

$$\begin{cases} x = \sqrt[3]{-\dfrac{q}{2} + \sqrt{\dfrac{q^2}{4} + \dfrac{p^3}{27}}} + \sqrt[3]{-\dfrac{q}{2} - \sqrt{\dfrac{q^2}{4} + \dfrac{p^3}{27}}} \\ a \cdot b = -\dfrac{p}{3} \end{cases}$$

Умови $a \cdot b = -\frac{p}{3}$ береться з переходу $ab = -\frac{p}{3} \Rightarrow a^3b^3 = -\frac{p^3}{27}$, та дозволяє вирішити питання з неоднозначністю **извлечения** корня третої степені.

Другий спосіб Нехай x_1, x_2, x_3 корні рівняння $x^3 + px + q = 0$, тоді по теоремі Вієтта отримуємо:

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1x_2 + x_1x_3 + x_2x_3 = p \\ x_1x_2x_3 = -q \end{cases} \Rightarrow y_1 = -(y_2 + y_3)$$

Звідки бачимо що один з корнів р-ня є сумою двух інших. Спробуємо його так і шукати, нехай $x = z + t$:

$$\begin{aligned} &(z+t)^3 + p(z+t) + q = 0 \\ &z^3 + 3z^2t + 3zt^2 + t^3 + p(z+t) + q = 0 \\ &z^3 + t^3 + 3zt(z+t) + p(z+t) + q = 0 \\ &z^3 + t^3 + (z+t)(3zt + p) + q = 0 \end{aligned}$$

Тепер поклавши $3zt + p = 0$, тобто $zt = -\frac{p}{3}$, що рівносильно рішенню системи:

$$\begin{cases} zt = -\frac{p}{3} \\ z^3 + t^3 = -q \end{cases} \Rightarrow \begin{cases} z^3t^3 = -\frac{p^3}{27} \\ z^3 + t^3 = -q \end{cases}$$

Що приводить нас до минулого випадка.

1.2 Тригометричний спосіб Вієтта

Для початку розглянемо приклад $4x^3 - 3x = \frac{1}{2}$, згадавши формулу косінуса тройного кута: $\cos 3\alpha = 4\cos^3\alpha + 3\cos\alpha$. Звідки отримуємо, при $x = \cos\varphi$:

$$\cos 3\varphi = -\frac{1}{2} \Rightarrow \varphi = \frac{2\pi}{3} + 2\pi k, k \in \mathbb{Z}$$

Тепер розглянемо довільне кубічне рівняння $\tilde{x}^3 + p\tilde{x} + q = 0$, за допоммогою замінни $\tilde{x} = kx$, спробуємо його звести до вигляду $4x^3 - 3x = a$, після замінни отримуємо:

$$x^3k^3 + pkx + q = 0$$

і підібравши k так, щоб $\frac{k^3}{pk} = \frac{4}{3}$, тобто $k = 2\sqrt{\frac{p}{3}}$, отримуємо необхідне.

1.3 рівняння четвертої степенні та формула Ферарі

Довільне рівняння четвернтої $Ay^4 + By^3 + Cy^2 + Dy + F = 0$ поділивши на A та зробивши замінну $y = x - \frac{B}{4A}$, зводиться до вигляду:

$$x^4 + ax^2 + bx + c = 0$$

Розглянемо два випадки:

1. $b = 0$, наше рівняння четвертої степені є біквадратним, та замінною $x^2 = t$ зводить до рішення квадратного.

2. $b^2 - 4ac = 0$, тобто $ax^2 + bx + c$ - повний квадрат, тоді рівняння теж зводиться до квадратного а його ми вміємо вирішувати.

Спробуємо звести довільне рівняння 4-ї степені до випадку 2. Для цього введемо параметр:

$$\left(\frac{t^2}{2}+\frac{t}{2}\right)^2+(a-t)x^2+bx+c-\frac{t^2}{4}$$

Та підберемо його так, щоб $b^2-4(a-t)\left(c-\frac{y^2}{4}\right)=0$, звевши подібні отримуємо кубічне рівняння:

$$t^3-at^2-4cy+4ac-b^2=0 \tag{2}$$

а кубічні рівняння ми вже вміємо вирішувати.

2 Скінчені розширення полів

2.1 Основні поняття

Нехай K, L - поля та $K \subset L$ - підполе, та нехай $\alpha \in L$. Тоді

$K[\alpha]=\left\{f(\alpha)\in L \,\middle|\, f\in K[x]\right\}$

$K(\alpha)=\left\{f(\alpha)\in L \,\middle|\, f\in K(x)\right\}$

Приклад 1. *Коли* $K[\alpha]=K(\alpha)$*:*

1. *Нехай* $K=\mathbb{Q}$ *та* $\alpha=\sqrt{2}$*, тоді розглянемо* $\dfrac{1}{a+\sqrt{2}b}$ *де* a, b *— довільні раціональні числа, тоді домноживши знаменик на* $a-\sqrt{2}b$*, отримуємо* $\dfrac{a-\sqrt{2}b}{a^2-2b^2}=\dfrac{a}{a^2-2b^2}-\sqrt{2}\dfrac{b}{a^2-2b^2}\in\mathbb{Q}[\sqrt{2}]$*. Отримали* $\forall a\in\mathbb{Q}(\sqrt{2}):\ a\in\mathbb{Q}[\sqrt{2}]\Rightarrow\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}[\sqrt{2}]\Rightarrow\mathbb{Q}[\sqrt{2}]=\mathbb{Q}(\sqrt{2})$

2. *Провести анологічне для* $\alpha=\sqrt[3]{2}$

Означення 1. *Нехай* $K\subset L$ *— розширення та* $\alpha\in L$*. Елемент* α *називається алгебраїчним над полем* K*, якщо* $\exists f\in K[x]\colon f\neq 0$ *і* $f(\alpha)=0$*.*

Означення 2. *Розширення* L *над* K *називається алгебраїчним, якщо кожен його елемент алгебраїчен.*

Означення 3. *Мінімальним многочленом елемента* α*, називається мн-н* $\mu_\alpha(x)\in K[x]$ *такий, що*

1)*коеффіцієнт при старшей степені дорівнює 1;*

2)$\mu_\alpha(\alpha)=0$*;*

3)$\forall f\in K[X]\colon f(\alpha)=0\Rightarrow f(x)\,\vdots\,\mu_\alpha(x)$*.*

Твердження 1. $\mu_\alpha(x)$ *- незвідний многочлен над полем* K

Доведення. *Припустимо супротивне, нехай* $\mu_\alpha(x)$ *— звідий, тобто* $\mu_\alpha(x)=u(x)v(x)$*, де* $u(x),v(x)\in K[x]$*. Причому* $\deg u<\deg\mu_\alpha, \deg v<\deg\mu_\alpha$*. Та враховуючи, що* α *є корінем або* $u(x)$*, або* $v(x)$*, отримуємо протиріччя з мінімальністю* $\mu_\alpha(x)$*.*

Теорема 1. *Наступні умови на* $\alpha\in L/K$ *еквівалентні:*

1. α *- алгебраїчен над* K*;*

2. $K(\alpha)=K[\alpha]$*;*

3. $[K(\alpha):K]=dim_K K(\alpha)<\infty$*.*

При виконанні цих умов $[K[\alpha] : K] = \dim_K K[\alpha] = \deg(\mu_\alpha) = \deg\alpha$ *та називається ступіню розширення.*

Доведення. *1*

(1) $\Longrightarrow$ (2) *Розглянемо довільний елемент* $\frac{1}{f(x)} \in K(x)$, $f(x) \in K[x]$, *такий, що* $f(\alpha) \neq 0$, *тобто НСД*$(f, \mu_\alpha) = 1$. *Звідки* $\exists v, u \in K[x] : uf + v\mu_\alpha = 1$, *звідки* $\frac{1}{f(\alpha)} = u(\alpha) \in K[\alpha]$.

(2) $\Longrightarrow$ (1) *Якщо* $\alpha = 0$, *то все доведенно. Нехай* $\alpha \neq 0$ *та* $K[\alpha] = K(\alpha)$, *тоді* $\exists f(x) \in K[x] : \frac{1}{\alpha} = f(\alpha)$. *звідки отримуємо, що* α *є коренем рівняння* $xf(x) - 1 = 0$, *звідки* α *— алгебраїчен.*

(1) $\Longrightarrow$ (3) *Нехай* $\mu_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ *— мінімальний многочлен* α. *Тоді* $K[\alpha] = \left\{b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1} \middle| b_0, \ldots, b_{n-1} \in K\right\}$, *так як при* $m > n$, *отримуємо* $\alpha^m = (\alpha^n)^{m-n} = (-a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1})^{n-m}$. *Тобто отримали, що* $K[\alpha]$ *- векторний простір з базисом* $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. *Звідки* $\dim K[\alpha] = \deg(\mu_\alpha) = \deg\alpha < \infty$.

(3) $\Longrightarrow$ (1) *Так, як* $\dim_K K[\alpha] < \infty$, *то* $\exists k \in \mathbb{N} : \alpha, \alpha^2, \ldots, \alpha^k$ *- лінійно залежні, тобто* $\exists a_1, a_2, \ldots, a_k : a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} = 0$. *Звідки* α *- алгебраїчний.*

Зауваження. *Помітим що при доказі* (3) $\Rightarrow$ (1), *ми одразу довели, що кожне скінчене розширення - алгебраїчне.*

Теорема 2. *Мн-н* $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x = a_0 \in \mathbb{Z}[x]$ *є незвідним над* $\mathbb{Z}(\mathbb{Q})$, *якщо існує просте* p *таке, що* $p \nmid a_n, p \mid a_{n-1}, a_{n-2}, \ldots, a_0$ *та* $p^2 \nmid a_0$.

Приклад 2. $x^2 - 2 = 0$ *— є незвідним на* $\mathbb{Q}$, *так як немає раціональних коренів. Звідки* $deg\sqrt{2} = [Q(\sqrt{2} : Q] = 2$

Приклад 3. $\cos\frac{2\pi}{5}$ *— алгебраїчен над* $\mathbb{Q}$. *Розглянемо рівняння* $x^5 - 1 = 0$, *як відомо його кореннями є* $\cos(\frac{2\pi k}{5}) + i\sin(\frac{2\pi k}{5})$, *де* $k \in \{0, 1, 2, 3, 4\}$. *Та наприклад по теоремі Вієтта сума усіх коренів в нашому випадку дорівню нулю. А звідки і сума усіх дійсних частин коренів, якими є необхідні косинуси, рівна нулю:*

$$2\cos\frac{2\pi}{5} + 2\underbrace{\cos\frac{4\pi}{5}}_{2\cos^2\frac{2\pi}{5}-1} + 1 = 0$$

$$1 + 2\cos\frac{2\pi}{5} + 4\cos^2\frac{2\pi}{5} - 2 = 0$$

Зробивши заміну $x = \cos(\frac{2\pi}{5})$, *отримуємо квадратне рівняння:*

$$4x^2 + 2x - 1 = 0$$

Звідки $cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$ *та* $cos\frac{4\pi}{5} = \frac{-1-\sqrt{5}}{4}$ *— алгебрачні, так як є коренняси квадратного рівняння.*

Приклад 4. $\cos\frac{2\pi}{9}$ *— алгебрачний над* $\mathbb{Q}$. *Як було показанно, за допомогою формули потрійного кута:* $4\cos^3\varphi - 3\cos\varphi = \cos 3\varphi$, *цей косінус є розв'язком рівняння* $4x^3 - 3x - \frac{1}{2} = 0$.

Задача 1. *Чи є незвідним* $x^5 - 4 = 0$?

Задача 2. *При яких* $a, \deg\sqrt[n]{a} = n$, *чи інакше кажучи при яких* a, *многочлен* $x^n - a$ *— незвідний над* $\mathbb{Q}$.

1. $a > 0, n$ *- непарне;*

2. $a < 0, n = 2^k$, *де* $k \in \mathbb{Z}$;

3. *загальний випадок.*

Лема 1 (О вежах)**.** *Нехай є вежа розширень* $K - L - P$, *де* $K \subset L \subset P$ *— поля та* $\dim_K P = m, \dim_L P = n$. *Тоді* $dim_K P = [P : K] = mn$.

Доведення. *Нехай* $e_1, \dots e_n$ *- базис в* L/K *та* $h_1, \dots h_m$ *базис в* P/L, *покажемо, що* $\{e_i h_j\}$ *- є базисом в* P/K.

1. *Покажем, що* $< e_i h_j >= spane(\{e_i h_j\}) = P$

   Нехай $p \in P$, *тоді існують* $a_1, \dots, a_n \in L$ *такі, що* $p = \sum_j^m a_j h_j$, *так як* $\{h_i\}$ *- базис* P/L. *В свою чергу для кожного* a_j *існують* $b_{j1}, \dots, b_{jm} \in K$ *такі, що* $a_i = \sum_i^m b_{ji} e_i$, *так, як* $\{e_i\}$ *— базис* L/K.

   Ну тоді отримуємо $\forall p \in P \;\; \exists b_{ij} \in K : \;\; p = \sum_j \sum_i b_{ji} h_j e_i$.

2. *Покажем, що* $\{e_i h_j\}$ *— лінійно незалежні:*

   Нехай $\sum_i \underbrace{\sum_j b_{ji} e_j}_{a_i} h_i = 0$, *звідки* $a_i = 0$ *так, як* $\{h_i\}$ *— лініно незалежні. Враховуючи* $a_i = \sum_j b_{ij} e_j = 0$, *та лінійну незалежність* e_j, *отримуємо* $b_{ij} = 0 \; \forall i, j$.

Зауваження.
$$\begin{tikzcd} & B \arrow[dl] \\ A \arrow[ur] \arrow[dr] & F \\ & C \arrow[ul] \end{tikzcd}$$

Теорема 3. *Нехай* L *над* K *— будь-яке розширення. Мн-на* $A = \{\alpha \in L \,\big|\, \exists f(x) \in K[x] : \; f(\alpha) = 0\}$ *— усіх алгебраїчних чисел є полем над* K.*(Зокрема* $\mathbb{A}$ *— поле)*

Доведення. *Достатньо показати, що* A *замкнена відностно операцій. Нехай* $\alpha, \beta \in A$, *тобто довільні алгебраїчні над* K *елементи, покажем, що* $K(\alpha, \beta) \in A$.

Для цього розглянемо вежу полів $K \overset{\leq \infty}{—} K(\alpha) \overset{\leq \infty}{—} K(\alpha, \beta)$, *Звідки бачимо, що* $[K(\alpha, \beta) : K] < \infty$ *по лемі о вежах.*

2.2 Спряжені елементи

Означення 4. *Нехай* $\mu_\alpha^K(x) = (x - \alpha_1) * \dots * (x - \alpha_n)$ *-мінімальний многочлен* $\alpha = \alpha_1$ *над* K, *де* $\alpha_i \in L \supset K$. *Тоді всі корні* $\alpha_1, \dots, \alpha_n$ *— називаються спряжиними елементами до* α *над полем* K.

Приклад 5.

1. $\mathbb{C}/\mathbb{R}, x^2 + 1$

2. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

3. $\mathbb{Q}(\sqrt[3]{3}/\mathbb{Q})$

4. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$

5. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$

6. $x^4 - 2$ *над* $\mathbb{Q}(\sqrt[4]{2})$

Теорема 4. *Будь-який симетричний многочлен $f(x_1,\dots,x_n)$, може бути представлений у композиції:*

$$f(x_1,\dots,x_n) = F\Big(\sigma_1(x_1,\dots,x_n),\dots,\sigma_n(x_1,\dots,x_n)\Big)$$

де F — якийсь многочлен, а σ_i - елементарні симетричні многочлени

Твердження 2. *Нехай $h(x) = (x-\alpha_1)\dots(x-\alpha_n) \in K[x]$, тоді, якщо многочлен $f(y_1,\dots,y_m,x_1,\dots,x_n)$ — симетричний по x_i, тоді $f(y_1,\dots,y_m,\alpha_1,\dots,\alpha_n) \in K[y_1,\dots,y_m]$*

Доведення. *Так, як многочлен $f(y_1,\dots,y_m,x_1,\dots,x_n)$ симетричний по змінних x_i, то по основній теоремі о симетричних многочленах, існує многочлен $g[y_1,\dots,y_m] \in K[y_1,\dots,y_n,x_1,\dots,x_m]$ такий, що $f(y_1,\dots,y_m,x_1,\dots,x_n) = g(y_1,\dots,y_m,\sigma_1(x_1,\dots,x_n),\dots,\sigma_n(x_1,\dots,x_n))$, Тоді $f(y_1,\dots,y_m,\alpha_1,\dots,\alpha_n) = g(y_1,\dots,y_m,\sigma_1(\alpha_1,\dots,\alpha_n),\dots,\sigma_n(\alpha_1,\dots,\alpha_n))$, но α_i — корні $h(x) \in K[x]$, а елементарні симетричні многочлени від коренів це як відома формулам Віетта коффіцієнти $h(x)$, тобто $\sigma_i(\alpha_1,\dots,\alpha_n) \in K$, тоді $f(y_1,\dots,y_m,\alpha_1,\dots,\alpha_n) \in K[y_1,\dots,y_n]$*

Нехай $\alpha,\beta \in L \supset K$ - алгебраїчні, та нехай $\alpha_1,\dots,\alpha_n$ і $\beta_1,\dots,\beta_m$ - всі спряжені з α та β відповідно. З'ясуємо які будуть спряженні з $\alpha+\beta$,$\alpha-\beta$,$\alpha\beta$,$\dfrac{\alpha}{\beta}$, розглянемо многочлен $f_{+}(x) = \prod\limits_i^n \prod\limits_j^m (x-(\alpha_i+\beta_j)) = \prod\limits_i^n \prod\limits_j^m (x-\alpha_i-\beta_j)$, по минулому твердженню він належить $K[x]$, звідки всі спряжені з $\alpha+\beta$ містяться в множині $\Big\{\alpha_i+\beta_j \Big| i \in \{1,\dots,n\}, j \in \{1,\dots,m\}\Big\}$. Відповідно розглянувши многочлени f_-, f_*, f отримуємо анологічне, для спряжених к $\alpha-\beta, \alpha*\beta, \alpha/\beta$.

Теорема 5. *Нехай α — алгебраїчний над K, та $\alpha_1,\dots,\alpha_n$ — всі його спряжені, тоді $\forall f(x) \in K[x]$ всі спряжені з $f(\alpha)$ є $f(\alpha_1),\dots,f(\alpha_n)$.*

Доведення. .

(1)*Покажемо, що $f(\alpha_1),\dots,f(\alpha_n)$ спряжені з $f(\alpha)$:*

Нехай $\mu_{f(\alpha)}(t)$ — мінімальний многочлен $f(\alpha)$, розглянемо мн-н $\mu_{f(\alpha)} \circ f(t) = \mu_{f(\alpha)}(f(t))$. Так, як α є його корнем, то $\mu_\alpha \,\Big|\, \mu_{f(\alpha)(f(t))}$, звідки α_i також корені $\mu_{f(\alpha)}\big(f(t)\big)$, но тоді $f(\alpha_i)$ корені $\mu_{f(\alpha)}(t)$, звідки вони спряжені з $f(\alpha)$;

(2)*Інших спряжених немає:*

Розглянемо многочлен $\varphi(x) = \big(x-f(\alpha_1)\big)\dots\big(x-f(\alpha_n)\big)$. Так як $\varphi(x)$ — симетричний по α_i, то по твердженню више $\varphi \in K[x]$. Так як $f(\alpha)$ є його коренем, то $\mu_{f(\alpha)}(x) \,\big|\, \varphi(x)$. Маємо, що $f(\alpha_i)$ — спряжені з $f(\alpha)$, та мінімальний многчлен ділить многочлен $\varphi(x)$, усі корені корені якого є $f(\alpha_i)$, звідки тільки вони спряжені з $f(\alpha)$.

Твердження 3. *Якщо $charK = 0$ та $\mu_\alpha(x)$ — мінімальний многочлен. Тоді $\mu_\alpha(x)$ - не має кратних коренів.*

Доведення. *Так, як характеристика поля $char\,K = 0$, то $\deg f'(x) = \deg f(x)$, якщо $f(x) \neq const$. Звідки отримуємо, що $\deg \mu'_\alpha(x) = \deg \mu_\alpha(x) - 1$. А так як μ_α — незвідний над K, то НСД$(\mu_\alpha, \mu'_\alpha) = 1$, тобто μ_α немає кратних коренів.*

,

2.3 Побудова циркулем та лінійкою

Ми можемо вибирати довільні точки на площині, відкладати одинчний відрізок задопомогою циркуля, та з'єднувати любі дві точки за допомогою лінійки. Що ми можемо побудувати?. По перше, так як ми можемо будувати одинчний відрізок на прямій, то ми можемо будувати і будь який відрізок натуральної довжини, а обравший якусь точку за нуль, ми можемо будувати і усі цілі числа $\mathbb{Z}$. Далі замість того щоб казати: "побудувати відрізок задоної довжини будемо просто про подуви самого числа по модулю рівного довжині відрізка.

InOtherTime OTheeeeeeeeeeerTIMEEEEEEEEEEEEEE

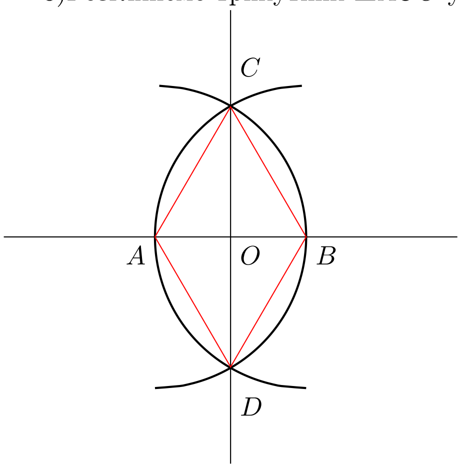
Перпендикуляр та ділення відрізка навпіл

Нехай є дві довільні точки A та B на прямій. Проведомо кола радіуса $|AB|$ з точки A та B(тобто кола $B(A,|AB|), B(B,|AB|)$). Позначемо перетин цих кіл точками C, D $\Big(C, D \in B(A,|AB|) \cap B(B,|AB|)\Big)$. Покажемо, що відрізки CD та AB перпендикулярні, та точка їх перетину $O = AB \cap CD$ - є серединою відрізка AB:

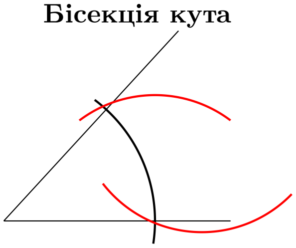
1) $|AC| = |CB| = |BD| = |AD| = |AB|$ - як радіуси кіл. Звідки $\triangle ACD = \triangle ADB$, причому вони обидва рівносторонні. Звідки кути $\angle CAB = \cdots = \angle BDA = 60°$.

2)$\triangle CAD = \triangle CBD$

3)Розглянемо трикутник $\triangle ACO$ у ньому $\angle OAC = 30°$ та $\angle ACO = 30° \Rightarrow \angle AOC = 90°$.

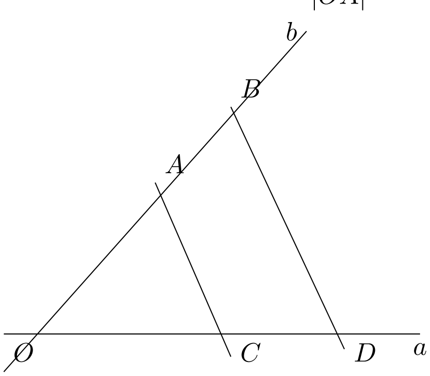


Бісекція кута

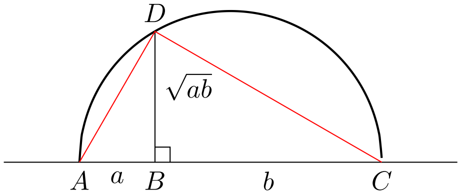


Раціональні числа $\mathbb{Q}$

За теоремою Фалеса $\dfrac{|OA| + |OB|}{|OA|} = \dfrac{|OC + OD|}{|OC|} \Rightarrow \dfrac{|AB|}{|OA|} = \dfrac{|CD|}{|OC|}$



Квадратний корень з числа



Висновок о можливих побужовах

Чому все що ми можемо робити це додовати, віднімати, множити, ділити, та брати квадратні радикали з чисел за допомогою циркуля та лінійки. Так як кожна пряма на площині задається рівнянням $y = kx + c$, та кожне коло на площині задається рівнянням $(x - a)^2 + (y - b)^2 = R^2$. То фактично все що ми можемо робити, це будувати точки які є перетаними двух прямих, двух кіл або прямою та кола. Тобто всі числа які ми можемо отримаєти є розв'язками одної з систем:

$$\textbf{(1)} \begin{cases} y = k_1 x + c_1 \\ y = k_2 + c_2 \end{cases} \quad \textbf{(2)} \begin{cases} (x - a_1)^2 + (y - b_1)^2 = R_1^2 \\ (x - a_2)^2 + (y - b_2)^2 = R_2^2 \end{cases} \quad \textbf{(3)} \begin{cases} y = kx + c \\ (x - a)^2 + (y - b)^2 = R^2 \end{cases}$$

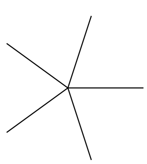
Розв'язки яких якраз виражаються через операції "$+, -, *, /, \sqrt{}$ такі числа називаються поліквадратичними. Тобто отримали це все, що ми можемо робити за допомогою циркуля та лінійки.

Означення 5. *Розширення L над K називаеться поліквадратичним, якщо існюе башня подполів $K = K_0 \overset{2}{—} K_1 \overset{2}{—} \dots \overset{2}{—} K_n = L$ така, що $[K_n : K_{n-1}] = 2$.*

Помітимо, що якщо $\alpha \in K$, но $\sqrt{\alpha} \not\in K$, тоді $[K : K(\sqrt{\alpha})] = 2$. та навпаки, нехай $[L : K] = 2$, та $\alpha \in L$, $\alpha \not\in K$. тоді $1, \alpha$ - базис в L/K. Но тоді $\exists p, q \in K : \alpha^2 = pa + q \Rightarrow \left(\alpha - \frac{p}{2}\right)^2 = q + \frac{p^2}{4} \Rightarrow L = K\left(\sqrt{q + \frac{p^2}{4}}\right)$.

Зауваження. *Якщо $[L : K] = 2^k$, це не гарантює поліквадратичність цього розширення, як приклад: $x^4 - 2x - 2 = 0$*

2.3.1 Побудова правильних многокутників



Знайдемо мінімальний многочлен для ε_{p^k}:

(1) Нехай $k = 1$

Розглянемо многочлен $x^p - 1$, він звіднийб но ε_p його корень, спробуємо звести його до незвідного.

Твердження 4. *Многочлен $\frac{x^p - 1}{x - 1} = x^{p-1} + \dots + x + 1$ — незвідний над $\mathbb{Q}$.*

Доведення. *Розглянемо $\frac{x^p - 1}{x - 1}$, зробимо заміну $y = x - 1$, отримуємо $\frac{(y+1)^p - 1}{y} = y^{p-1} + py^{p-2} + \frac{p(p-1)}{2} y^{p-3} + \dots + C_p^k y^{k-1} + \dots + \frac{p(p-1)}{2} y + p$.*

$C_p^k = \frac{p!}{k!(p-k)!}$, *так як p - просте, то оно не скоротить не з чим в знаменику $\frac{1}{k!(p-k)!}$. Звідки бачимо, що всі коеффіціенти многочлена, окрім коеффіціента при y^{p-1} діляться на p, та вільний член не ділиться на p^2, звідки про признаку Ейзінштейна цей многочлен незвідний над $\mathbb{Q}$, тобто він мінімальний для ε_p.*

(2) $k \in \mathbb{N}$

Наслідок 1. $\deg \varepsilon_{p^k} = p^{k-1}(p-1)$. *та для того, щоб* ε_{p^k} *— було поліквадратичним необхідно, щоб* $p^{k-1}(p-1)$ *було степіню двійки, тобто* $p^{k-1}(p-1) = 2^j$*, що можливо тільки при*

$$\begin{cases} k = 1 \\ 2^t = p - 1 \end{cases}$$

Коли $2^t + 1$ *може бути простим? Якщо* $t = dk$*, де* d *- непарне, то* $(2^t + 1) \vdots (2^{\frac{t}{d}} + 1)$*.* $\Big(((2^{\frac{t}{d}})^d + 1) \vdots (2^{\frac{t}{d}} + 1)$*, Якщо позначити через* $x = 2^{\frac{t}{d}}$*, отримуємо* $(x^d + 1) \vdots (x + 1)$*, що дійстно так*$\Big)$*. Звідки* t *- не містить непарних дільників, ну тоді* t *— степень двійки. Звідки нам підходять лише прості числа вигляду* $F_i = 2^{2^i}, i \in \mathbb{N} \cup \{0\}$*. Тобто прості числа Ферма.*

Теорема 6 (Гаусса-Ванцеля)**.** *Правильний n-кутник будується тоді і лише тоді, коли n є добудтком степенів двійки та(або) простих чисел Ферма.*

2.3.2 Побудова правильного 17-ти кутника

Так як $17 = 2^4 + 1$, тобто є простим Ферма, то є можливість, що правильний 17-кутник будується за допомогою циркуля та лінійки. Требо знайти башню $\mathbb{Q} = K_0 \overset{2}{—} K_1 \overset{2}{—} K_2 \overset{2}{—} K_3 \overset{2}{—} K_4 = \mathbb{Q}(\varepsilon_{17})$, Помітим також, що $[K(\alpha) : K] =$ "кількість спряжених з α". Тобто для побудови даної башні достаньо кожен раз приєднувати $\alpha \in Q(\varepsilon_{17})$, щоб кількість з ним спряжених була $2, 4, 8, 16$ над Q.

Нехай $\varepsilon = \varepsilon_{17}$. Як відомо $\varepsilon, \varepsilon^2, \ldots, \varepsilon^{16}$ спряженні між собою. Та $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{15}$ утворюють базис в $\mathbb{Q}(\varepsilon)$. Ну тоді кожне $\alpha \in L$ розкладається в $\alpha = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + \cdots + a_{15}\varepsilon^{15}$. Та всі спряжені з α дорівнюють:

$$\begin{aligned}
&\alpha = \alpha_0 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + \cdots + a_{15}\varepsilon^{15} \\
&\alpha_1 = a_0 + a_1\varepsilon^2 + a_2\varepsilon^4 + a_3\varepsilon^6 + \cdots + a_{15}\varepsilon^{30} \\
&\ldots \\
&\alpha_{15} = a_0 + a_1\varepsilon^{15} + a_2\varepsilon^{30} + a_3\varepsilon^{45} + \cdots + a_{15}\varepsilon^{225}
\end{aligned}$$

І ми хотіли б легко розуміти коли якісь зі спряженик звіпали, але в данному розкладі це не дуже зручно. Для більшої зручності передемо до базиса $\varepsilon, \varepsilon^2, \ldots, \varepsilon^{16}$ та впорядкуємо його по іншому. А сама так, як $< 3 >= \mathbb{Z}_{17}$. То можно розглянути базис $\varepsilon, \varepsilon^3, \varepsilon^{3^2}, \varepsilon^{3^3}, \ldots, \varepsilon^{3^{15}}$. Тепер маємо

$$\begin{aligned}
&\alpha_0 = a_0\varepsilon + a_1\varepsilon^3 + a_2\varepsilon^{3^2} + a_3\varepsilon^{3^3} + \cdots + a_{15}\varepsilon^{3^{15}} \\
&\alpha_1 = a_0\varepsilon^3 + a_1\varepsilon^{3^2} + a_2\varepsilon^{3^3} + a_3\varepsilon^{3^4} + \cdots + a_{15}\varepsilon^{3^{16}} \\
&\ldots \\
&\alpha_{15} = a_0\varepsilon^{3^{15}} + a_1\varepsilon^{3^{16}} + a_2\varepsilon^{3^{17}} + a_3\varepsilon^{3^{18}} + \cdots + a_{15}\varepsilon^{3^{30}}
\end{aligned}$$