Полиноми с комплексни и с реални коефициенти. Алгебрическа затвореност на полето на комплексните числа.

Казваме, че полето F е *алгебрически затворено*, ако всеки полином $f(x) \in F[x]$ с $\deg f \geq 1$ има поне един корен в F. Ако $\alpha_1, \alpha_2, \dots, \alpha_n$ са корените на полинома $f(x) = a_0x^n + \dots + a_n, a_0 \neq 0, n \geq 1$, то от разлагането

$$f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

следва, че когато F е алгебрически затворено, то $\alpha_1, \alpha_2, \dots, \alpha_n \in F$.

Знаем, че полетата $\mathbb{Q}$ и $\mathbb{R}$ не са алгебрически затворени. Например полиномът с рационални коефициенти $f(x) = x^2 - 2$ няма рационален корен, а полиномът с реални коефициенти $g(x) = x^2 + 1$ няма реален корен. Произволно поле от остатъци $\mathbb{Z}_p$, където p е просто число, също не е алгебрически затворено. Например за неконстантният полином$h(x) = x^p - x + \overline{1} \in \mathbb{Z}_p[x]$ е в сила, че $F(\overline{k}) = \overline{1} \neq \overline{0}$ за $\forall \overline{k} \in \mathbb{Z}_p$, т.к. теоремата на Ойлер-Ферма гласи, че $\overline{k}^p = \overline{k}$ за $\forall \overline{k} \in \mathbb{Z}_p$. Полето $\mathbb{C}$ обаче притежава това важно свойство, както твърди

Основна теорема на алгебрата. *Полето $\mathbb{C}$ е алгебрически затворено.*

Доказателство. Нека

$$f(x) = a_0x^n + \dots + a_n \in \mathbb{C}[x], a_0 \neq 0, n \geq 1$$

е полиномът, който ще разглеждаме. Ще разделим доказателството на няколко стъпки.

<u>Стъпка 1:</u> Ако $f(x) \in \mathbb{R}[x]$ и n е нечетно число, то $f(x)$ има дори реален корен.

Наистина, като полином с реални коефициенти $f(x)$ определя непрекъснатата функция

$$f : \mathbb{R} \longrightarrow \mathbb{R},$$

за която е в сила, че $\lim_{x\to\infty} f(x) = a_0(+\infty)$ и $\lim_{x\to-\infty} f(x) = a_0(-\infty)$. Тогава $\exists a, b \in \mathbb{R}$, такива че $f(a) < 0$ и $f(b) > 0$. Нека за определеност $a < b$. Според теоремата на Болцано от Диференциалното и интегрално смятане трябва да съществува число $c \in (a, b)$, такова че $f(c) = 0$. И така, $f(x)$ има реален корен c.

<u>Стъпка 2:</u> Ако $f(x) \in \mathbb{R}[x]$, то f има комплексен корен.

Нека $\alpha_1, \alpha_2, \ldots, \alpha_n$ са корените на $f(x)$ и P е неговото поле на разлагане над $\mathbb{C}$ (т.е. P съдържа $\mathbb{C}$ и $\alpha_1, \alpha_2, \ldots, \alpha_n$). Степента на f е $\deg f = n$ и е ясно, че имаме представянето $n = 2^k m$ за цели числа $k \geq 0, m \geq 0$ и $2 \nmid m$. Ще проведем индукция по k. Основа на индукцията – ако $k = 0$, то $2 \nmid n$ и според Стъпка 1 $f(x)$ има дори реален корен. Индукционно предположение – нека твърдението е вярно за всички естествни числа по-малки от k. Индукционна стъпка – ще докажем, че е вярно за k. Фиксираме число $r \in \mathbb{R}$. Разглеждаме елементите $\beta_{ij} = \alpha_i\alpha_j + r(\alpha_i + \alpha_j)$ за $1 \leq i < j \leq n$. Ясно е, че $\beta_{ij} \in P$ и броят им е $n = \binom{n}{2} = \dfrac{n(n-1)}{2} = 2^{k-1}m(2^k m - 1)$. Числото $m' = m(2^k m - 1)$ е нечетно, т.к. $k \geq 1$. И така, $n' = 2^{k-1}m', 2 \nmid m'$. Разглеждаме полинома

$$g(x) = \prod_{1 \leq i < j \leq n} (x - \beta_{ij}) \in P[x].$$

Старшият му коефициент е 1, а степента му е n', като $2^{k-1} \mid n'$, но $2^k \nmid n'$. Ще покажем, че $g(x) \in \mathbb{R}[x]$. Наистина, нека

$$g(x) = x^{n'} + b_1 x^{n'-1} + \cdots + b_{n'} \in P[x]$$

за коефициенти $b_i \in P$, $i = 1, 2, \ldots, n'$. От формулите на Виет е ясно, че коефициентите зависят от елементите β_{ij} и по-точно са техни симетрични полиноми

$$b_t = (-1)^t \sigma_t(\ldots, \beta_{ij}, \ldots), \quad t = 1, 2, \ldots, n'.$$

Произволна пермутация $\alpha_{p_1}, \alpha_{p_2}, \ldots, \alpha_{p_n}$ на $\alpha_1, \alpha_2, \ldots, \alpha_n$ пермутира и елементите β_{ij} до $\beta_{p_i p_j}$. Т.к. при пермутация на елементите β_{ij} полиномите σ_t не се променят, то можем да заключим, че произволна пермутация на $\alpha_1, \alpha_2, \ldots, \alpha_n$ не променя коефициентите b_t и всъщност b_t са симетрични полиноми и на $\alpha_1, \alpha_2, \dots, \alpha_n$ с коефициенти от $\mathbb{R}$. Това означава, че елементите $b_t \in \mathbb{R}$ за $\forall t = 1, 2, \dots n'$ и всъщност $g(x) \in \mathbb{R}$. Сега $g(x) \in \mathbb{R}[x]$ и $2^k \nmid \deg g = n'$. Според индукционното предположение $g(x)$ има поне един комплексен корен, т.е. $\beta_{ij} \in \mathbb{C}$ за поне една двойка $(i, j), 1 \leq i < j \leq n$. И така, за $\forall r \in \mathbb{R}$ съществуват числа $i, j, 1 \leq i < j \leq n$, зависещи от r, такива че $\beta_{ij} = \alpha_i\alpha_j + r(\alpha_i + \alpha_j) \in \mathbb{C}$. При това числата $r \in \mathbb{R}$ са безбройно много, а двойките (i, j) са краен брой и следователно съществуват числа $r_1, r_2 \in \mathbb{C}, r_1 \neq r_2$, такива че за едни и същи i, j е изпълнено $c = \alpha_i\alpha_j + r_1(\alpha_i + \alpha_j) \in \mathbb{C}$ и $d = \alpha_i\alpha_j + r_2(\alpha_i + \alpha_j) \in \mathbb{C}$. Тогава

$$c - d = (\alpha_i + \alpha_j)(r_1 - r_2)$$

като $r_1 - r_2 \neq 0$ и можем да изразим

$$\alpha_i + \alpha_j = \frac{c - d}{r_1 - r_2} = p \in \mathbb{C}.$$

От друга страна

$$\alpha_i\alpha_j = c - r_1(\alpha_i + \alpha_j) = c - r_1 p = q \in \mathbb{C}.$$

Така получихме $\alpha_i + \alpha_j = p \in \mathbb{C}$ и $\alpha_i\alpha_j = q \in \mathbb{C}$ и според формулите на Виет това са корените на уравнението

$$x^2 - px + q = 0.$$

Според формулите за корените на квадратно уравнение намираме

$$\alpha_i, \alpha_j = \frac{p \pm \sqrt{p^2 - 4q}}{2}$$

и т.к. $p^2 - 4q \in \mathbb{C}$, то по формулата на Моавър и $\sqrt{p^2 - 4q} \in \mathbb{C}$ и така $\alpha_i, \alpha_j \in \mathbb{C}$. Така $f(x)$ има дори два комплексни корена. Принципа на математическата индукция доказава текущата стъпка.

Стъпка 3: Ако $f(x) \in \mathbb{C}[x]$, то $f(x)$ има комплексен корен.

Нека $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{C}[x], n \geq 1$. Да разгледаме полинома

$$\overline{f}(x) = \overline{a_0}x^n + \overline{a_1}x^{n-1} + \cdots + \overline{a_{n-1}}x + \overline{a_n} \in \mathbb{C}[x],$$

чиито коефициенти са комплексните спрегнати на коефициентите на $f(x)$. От свойствата на комплексното спрягане за произволно число $\alpha \in \mathbb{C}$ имаме, че

$$\begin{aligned}\overline{f}(\overline{\alpha}) &= \overline{a_0}.\overline{\alpha}^n + \overline{a_1}.\overline{\alpha}^{n-1} + \dots + \overline{a_{n-1}}.\overline{\alpha} + \overline{a_n} \\ &= \overline{a_0\alpha^n + a_1\alpha^{n-1} + \dots + a_{n-1}\alpha + a_n} = \overline{f(\alpha)}.\end{aligned}$$

Разглеждаме полинома $h(x) = f(x)\overline{f}(x)$. Ако $h(x) = c_0x^{2n} + c_1x^{2n-1} + \dots + c_{2n}$ за $c_k \in \mathbb{C}, k = 1, 2, \dots, 2n$, то имаме, че $c_k = \sum_{i+j=k} a_i\overline{a_j}$. Сега

$$\overline{c_k} = \overline{\sum_{i+j=k} a_i\overline{a_j}} = \sum_{i+j=k} \overline{a_i}a_j = \sum_{i+j=k} a_j\overline{a_i} = c_k,$$

което доказва, че $c_k \in \mathbb{R}$ за $\forall k = 1, 2, \dots, 2n$ и всъщност $h(x) \in \mathbb{R}[x]$. От Стъпка 2 следва, че съществува комплексно число $\alpha \in \mathbb{C}$, такова че $h(\alpha) = 0$, т.е. $f(\alpha)\overline{f}(\alpha) = 0$. Последното означава, че $f(\alpha) = 0$ и/или $\overline{f}(\alpha) = 0$. Ако $f(\alpha) = 0$, то f има комплексен корен и твърдението е доказано. Нека сега $\overline{f}(\alpha) = 0$. Тогава $\overline{f}(\alpha) = \overline{f(\overline{\alpha})}$ и $\overline{f(\overline{\alpha})} = 0$. Т.к. $\overline{0} = 0$, последното всъщност означава, че $f(\overline{\alpha}) = 0$ и $\overline{\alpha}$ е корен на $f(x)$. Така окончателно получихме, че всеки полином $f(x) \in \mathbb{C}[x]$ с $\deg f \geq 1$ има корен в $\mathbb{C}$. С това приключва и доказателството на теоремата. $\square$

По този начин доказахме, че за всеки полином $f(x) \in \mathbb{C}[x], \deg f \geq 1$ със старши коефициент a_0 е в сила представянето

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)$$

за $\alpha_i \in \mathbb{C}, i = 1, 2, \dots, n$. С други думи неразложимите полиноми в $\mathbb{C}[x]$ са само тези от степен 1.

Твърдение. *Нека $f(x) \in \mathbb{R}[x]$. Ако $\alpha \in \mathbb{C}$ е корен на f, то $\overline{\alpha}$ също е корен на f, като при това α и $\overline{\alpha}$ имат еднаква кратност.*

Доказателство. Ако $\alpha \in \mathbb{R}$, то $\alpha = \overline{\alpha}$ и няма какво да доказваме.

Нека $\alpha \notin \mathbb{R}$. Тогава $\alpha \neq \overline{\alpha}$. От $f(\alpha) = 0$ имаме, че $0 = \overline{f(\alpha)} = \overline{f}(\overline{\alpha}) = f(\overline{\alpha})$, защото $f \in \mathbb{R}[x]$. С други думи $\overline{\alpha}$ също е корен на f. И така, $(x - \alpha) \mid f$ и $(x - \overline{\alpha}) \mid f$, но $\alpha \neq \overline{\alpha}$ и следователно $(x - \alpha)(x - \overline{\alpha}) \mid f$. Нека означим

$$\varphi(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}.$$

Нека още $p = -(\alpha + \overline{\alpha}) \in \mathbb{R}$ и $q = \alpha\overline{\alpha} \in \mathbb{R}$. По този начин получихме, че $\varphi(x) = x^2 + px + q \in \mathbb{R}[x]$ и $\varphi(x) \mid f(x)$. При това $D(\varphi) < 0$, защото φ няма реални корени. Нека $k \in \mathbb{N}$ е най-голямото число, за което $(\varphi(x))^k \mid f(x)$. Тогава $f(x) = (\varphi(x))^k g(x)$ за $g(x) \in \mathbb{R}[x]$ и очевидно $g(\alpha) \neq 0$ (в противен случай също $g(\overline{\alpha}) = 0$ и това влече $(\varphi(x))^{k+1} \mid f(x)$, което е противоречие). Също така $g(\overline{\alpha}) \neq 0$. Така $(x - \alpha) \nmid g$ и $(x - \overline{\alpha}) \nmid g$, което значи че $\varphi(x) \nmid g(x)$. Така накрая получихме, че $f(x) = (x - \alpha)^k(x - \overline{\alpha})^k g(x)$ и α и $\overline{\alpha}$ имат еднаква кратност. $\square$

От последното твърдение можем да си извадим извод, че ако $\alpha \in \mathbb{R}$, то $(x - \alpha) \mid f(x)$, а ако $\alpha \notin \mathbb{R}$, то $(x^2 + px + q) \mid f(x)$. И така за всеки полином $f(x) \in \mathbb{R}[x]$ с $\deg f \geq 1$ е в сила

$$f(x) = a_0(x - \alpha_1)^{k_1} \dots (x - \alpha_s)^{k_s}(x^2 + p_1x + q_1)^{l_1} \dots (x^2 + p_tx + q_t)^{l_t}$$

за $s, t \geq 0; k_i, l_j \geq 1; \alpha_i \in \mathbb{R}; p_j, q_j \in \mathbb{R}$ и $D_j = p_j^2 - 4q_j < 0$. Оттук следва, че наразложимите над $\mathbb{R}$ полиноми са само тези от степен 1 и тези от степен 2 с отрицателна дискриминанта.