Малко предистория

Предполагам помните $C_n = \{\alpha \in \mathbb{C} \mid \alpha^n = 1\}$ - цикличната група от n-ти ред, $n \in \mathbb{N}$ (тя е единствена с точност до изоморфизъм)

Елементите на C_n са n-тите корени на единицата, т.е.
Missing superscript or subscript argument ?
Освен това, w е елемент от ред n (т.е. $o(w) = |w| = n$), следователно той е пораждащ за C_n, или иначе казано:

$$C_n = <w> = \{1, w, w^2, \ldots, w^{n-1}\}$$

Сега се досещаме, че за $\forall d > 0 : \ d|n \Longrightarrow C_d < C_n$
Последното е долу-горе очевидно, ако някой желае - да го докаже :)

Друго не чак толкова очевидно, но и не чак толкова трудно даказуемо е следното… твърдение:
Missing superscript or subscript argument ?

ето една може би формална

Дефиниция (примитивен n-ти корен на 1)

Ако $w \in C_n$ и ако $o(w) = n$, то w е **примитивен** *n*-ти корен на единицата.

Разбира се, не е трудно да се види, че един елемент $w^k \in C_n$ е примитивен *n*-ти корен на единицата, т.с.т.к. $(n, k) = 1$
Затова не е трудно да се досетим, че примитивните *n*-ти корени на единицата са $\varphi(n)$ на брой.
Припомням: $\varphi(n)$ е броят на всички естествени числа, които са по-малки от n и взаимно прости с n.

/* Впрочем всичко казано дотук е казвано и на лекции и на упражнения по няколко пъти и е стар материал, който е само въведение към новия. А ето го и него.. */

Дефиниция(n-ти циклотомичен полином)

Полиномът

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \xi_i) \tag{1}$$

където $\xi_1, \xi_2, \ldots, \xi_{\varphi(n)}$ са примитивните *n*-ти корени на единицата, наричаме **циклотомичен n-ти полином**.

Разбира се, очевидно е, че $\Phi_n(x) \in \mathbb{C}[x]$, тък като в общия случай *n*-тите корените на единицата са комплексни числа.

Примери

При $n = 1 \Longrightarrow C_n = \{1\}$
Тук 1 е примитивен корен, тъй като $o(1) = 1 = n$ и от дефиницията, следва, че $\Phi_1(x) = x - 1$

При $n = 2 \Longrightarrow C_n = \{1, -1\}$
Тук $o(1) = 1 \neq n$ и $o(-1) = 2 = n$, т.е само -1 е примитивен корен и $\Phi_2(x) = x + 1$

При $n = 4 \Longrightarrow C_n = \{1, i, -1, i\}$
Проверяваме, че $o(1) = 1 \neq n,\ o(-1) = 2 \neq n,\ o(i) = o(-i) = 4 = n$, т.е $\Phi_4(x) = (x - i)(x + i) = x^2 + 1$

Теорема

$$x^n - 1 = \prod_{k=0}^{n-1}(x - w^k) = \prod_{d|n} \Phi_d(x) \tag{2}$$

Официално доказателство на теоремата не е приложено на лекции, така че нямам намерение аз да си го смуча от пръстите ;)
Но, ако се замислите, не изглежда нелогично.

Още примери

От горната теорема следва, че

$$x^3 - 1 = \Phi_3(x)\Phi_1(x) \Longrightarrow \Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1 \tag{3}$$

Аналогично

$$\Phi_6(x) = \frac{x^6 - 1}{\underbrace{\Phi_3(x)\Phi_1(x)}_{x^3-1}\Phi_2(x)} = \frac{(x^3 - 1)(x^3 + 1)}{(x^3 - 1)(x + 1)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1 \tag{4}$$

Освен това, ако p е просто число, то

$$x^p - 1 = \Phi_p(x)\Phi_1(x) \Longrightarrow \Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \tag{5}$$

Теорема

Циклотомичният *n*-ти полином е с цели коефициенти.

$$\Phi_n(x) \in \mathbb{Z}[x] \tag{6}$$

Доказателство:
Индукция по n:

1. За $n = 1, 2, \ldots, 7$ видяхме, че $\Phi_n(x) \in \mathbb{Z}[x]$
2. Нека за $k <= n - 1 \Longrightarrow \Phi_k(x) \in \mathbb{Z}[x]$
3.

(7)

$$x^n-1=\prod_{d|n}\Phi_d(x)\Longrightarrow\Phi_n(x)=\frac{x^n-1}{\underbrace{\prod_{d|n,d<n}\Phi_d(x)}_{\in\mathbb{Z}[x]}}$$

От индукционната хипотеза знаменателят е с цели коефициенти, освен това старшият му коефициент е 1.
$\Longrightarrow\Phi_n(x)\in\mathbb{Z}[x]$

Теорема

Нека $n\in\mathbb{N},\ n>1$ и $d|n$
Тогава:

$$1.\ \Phi_n(q)\Big|\ \frac{q^n-1}{q^d-1}\ ,\ q>1,q\in\mathbb{N} \tag{8}$$

$$2.\ \Phi_n(q)\nmid q-1,\ q>1,\ q\in\mathbb{N} \tag{9}$$

Доказателство:
1.

$$x^n-1=\prod_{t|n}\Phi_t(x)=\underbrace{\prod_{t|d}\Phi_t(x)}_{x^d-1}.\prod_{t_1|n,\ t_1\nmid d,\ t_1<n}\Phi_{t_1}(x).\ \Phi_n(x) \tag{10}$$

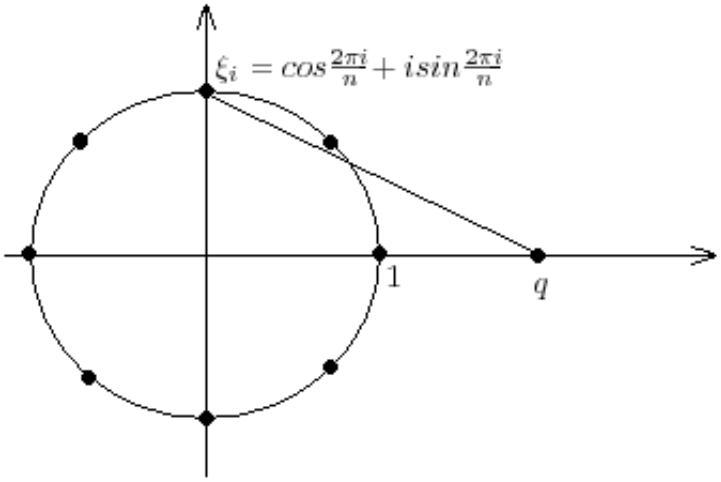
$$\Longrightarrow\frac{x^n-1}{x^d-1}=\Phi_n(x).\prod_{t_1|n,\ t_1\nmid d,\ t_1<n}\Phi_{t_1}(x) \tag{11}$$

$$\xrightarrow{q\in\mathbb{N}}\Phi_n(q)\Big|\ \frac{q^n-1}{q^d-1} \tag{12}$$

2.
Първи случай: $n>2$

$$\Phi_n(q)=\prod(q-\xi_i) \tag{13}$$

ξ_i е примитивен *n*-ти корен на единицата.



От геометрична гледна точка, имаме, че $|q-\xi_i| > |q-1|$
Изпълнено е за всеки корен на единицата (без самата нея), независимо дали е примитивен или не.
Идеята е, че най-късото растояние от точка до окръжност е растоянието от самата точка до пресечената точка на окръжността с отсечката, която свързва първата точка и центъра на окръжността.[1]

Тогава:

$$\Phi_n(q)| = \left|\prod(q-\xi_i)\right| > \prod_{i=1}^{\varphi(n)} |q-1| = |q-1|^{\varphi(n)} = (q-1)^{\varphi(n)} \geq q-1 \tag{14}$$

$$\Longrightarrow \Phi_n(q) \nmid q-1 \tag{15}$$

Втори случай: $n = 2$
$\Longrightarrow \Phi_2(x) = x+1$ **?**

Тогава $\Phi_2(q) = q+1$, което очевидно не дели $q-1$.

/*ПП: не знам защо точно се разглеждат тези два случая, но се доверявам на доц. Великова :)*/ □

Твърдение

$\Phi_n(x)$ е неразложим полином с цели коефициенти.

Доказателство:
Приемаме го на доверие :))

Дефиниция (тяло)

Пръстен с единица, в който всеки ненулев елемент е обратим, наричаме **тяло**.[2]

Пример

Знаем за групата на кватернионите: $\{\pm 1, \pm i, \pm j, \pm k\}$ (всъщност, знаем ли я?)
Кватернион в wikipedia

За тази група, знаем, че не е абелева, защото $ij = k = -ji$

Следното линейно пространство е нещо супер абстрактно (не че нещата дотук се срещат всеки ден в живота)

$$D = \{a_0 + a_1 i + a_2 j + a_3 k \mid a_i \in \mathbb{R}\} \tag{16}$$

Непосредствено се проверяват всички условия, за да бъде D пръстен, в който всеки ненулев елемент е обратим.
D **не** е поле, тъй като нямаме комутативност! (понеже 'кватернионите' не комутират!)

Та.. D се нарича *тялото на кватернионите*.

Друго нещо, с което D е известно, е че е *двумерно разширение* на$\mathbb{C}$

$$D = \{a_0 + a_1 i + \underbrace{a_2 j + a_3 k}_{(a_2 + a_3 i)j}\} \tag{17}$$

Знаем, че

$$\mathbb{C} = \{a_0 + a_1 i | a_i \in \mathbb{R}\} \tag{18}$$

Т.е всяко комплексно число е *реално число + реално число*имагинерна единица*

За елементите на D можем да считаме, че са *комплексно число + комлексно число*друга имагинерна единица*

Теорема на Ведербърн (за крайните тела)

Нека D е тяло и $|D| < \infty \Longrightarrow D$ е поле.

Всяко крайно тяло е поле.[3]

Доказателство:

Доказателството протича през няколко стъпки, които обхващат голяма част от материала до тук.

Припомням: център на пръстен/група е множеството от всички елементи, които комутират със всички останали (или, казано по друг начин, издържат на спрягане;

т.е не се променят при спрягане с кой да е друг елемент).

$$\mathcal{Z}(D) = \{a \in D \mid ax = xa \iff x^{-1}ax = a,\ \forall x \in D\} \tag{19}$$

1. $\mathcal{Z}(D)$ поле. (Нека, за удобство, $\mathcal{Z}(D) = F$)

Скрий

Очевидно $\mathcal{Z}(D) \subset D$

Нека $a,\ b \in \mathcal{Z}(D)$
Тогава:

- $(a-b)x = ax - bx = xa - xb = x(a-b) \implies a - b \in \mathcal{Z}(D)$
- $(ab)x = abx = axb = xab = x(ab) \implies ab \in \mathcal{Z}(D)$

$\implies \mathcal{Z}(D)$ е подпръстен на D.

$\implies \mathcal{Z}(D)$ е пръстен с единица.

Това, че всеки ненулев елемент си има обратен, следва от това, че елементите на центъра са елементи и на тялото.
И, освен това е очевадно, че всички елементи комутират (нали е център все пак ;))

От всичко дотук, можем да твърдим, че $\mathcal{Z}(D)$ е поле.

2. D в линейно пространство над F

Скрий

не знам ;)... сигурно защото са изпълнени онези 8 аксиоми от дефиницията за линейно пространство (Алгебра 1)

Освен това, $|D| < \infty \implies \dim_F D = k \implies |D| = |F|^k$

3. $F = \mathcal{Z}(D) \implies \mathcal{Z}(D^*) = F^*$

Знаем, че D^* е мултипликативната група на D.
$D^* = \{a \in D \mid a -$ обратим $\}$

И, тъй като D е тяло, то $D^* = D \setminus \{0\}$
Сега горното твърдение изглежда логично, нали? (дано!)

4. Разглеждаме *действието* на D^* върху D^* със спрягане.
Тогава D^* се разбива по следния начин:

$$D^* = F^* + O(x_1) + O(x_2) + \cdots + O(x_m) \tag{20}$$

където $x_1, x_2, \ldots, x_m$ - по един представител от всяка орбита с дължина, по-голяма от 1.

Следователно, е изпълнено, че:

$$|D^*| = |F^*| + \sum_{i=1}^{m} |O(x_i)| = |F^*| + \sum_{i=1}^{m} |D^* : C_{D^*}(x_i)| \tag{21}$$

Тук с $C_{D^*}(x_i)$ е означен е централизаторът(стабилизаторът) на x_i относно групата D^* при действието чрез спрягане.

$$C_D(x) = \{z \in D \mid x^{-1}zx = z\} \tag{22}$$

Очевидно $C_D(x) \subset \mathcal{Z}(D)$
Освен това, ако $z_1,\ z_2 \in C_D(x)$, то:

1. $(z_1 \pm z_2)x = z_1x \pm z_2x = xz_1 \pm xz_2 = x(z_1 \pm z_2) \Longrightarrow z_1 \pm z_2 \in C_D(x)$
2. $(z_1z_2)x = z_1(z_2x) = z_1(xz_2) = (z_1x)z_2 = x(z_1z_2) \Longrightarrow z_1z_2 \in C_D(x)$
3. $z_1x = xz_1 \Rightarrow z_1xz_1{}^{-1} = x \Rightarrow xz_1{}^{-1} = z_1{}^{-1}x \Longrightarrow z_1{}^{-1} \in C_D(x)$

$\Longrightarrow C_D(x)$ е тяло.

6. Нека $|F| = q \Longrightarrow |F^*| = q - 1$

Освен това,

$$D^* = |F|^k - 1 = q^k - 1 = q - 1 + \sum_{i=1}^{m} \frac{q^k - 1}{q^{s_i} - 1},\ |C_D(x_i)| = q^{s_i},\ s_i|k \tag{23}$$

//малко ми е мъгла тук

$$\begin{aligned} &\Phi_k(q)|q^k - 1 \\ &s_i|k \Longrightarrow \Phi_k(q)\left|\frac{q^{k-1}}{q^{s_i} - 1}\right. \\ &\Longrightarrow \Phi_k(q)\left|(q^k - 1) - \sum_{i=1}^{m} \frac{q^k - 1}{q^{s_i} - 1}\right. \\ &\Longrightarrow \Phi_k(q)|q - 1 \\ &\Longrightarrow k = 1 \end{aligned} \tag{24}$$

Т.е получихме, че $\dim_F D = 1 \Longrightarrow F = D \Longrightarrow D$ е поле. $\square$

Footnotes

1. Best sentence ever!

2. Или, също вярната, дефиниця на Наско (от 3-та): "Тяло е поле без комутативност." Каквито си искате асоциации могат да се правят с тази дефиниция ;)
3. Пуснете си въображението на макс! ;)

page revision: 16, last edited: 1 Jul 2009, 21:02 (1466 days ago)