Лекции по Висша Алгебра

Силвия Бумова

2020

Съдържание

Глава 1

Делимост при цели числа. Най-голям общ делител, тъждество на Безу. Прости числа и основна теорема на аритметиката. Функция на Ойлер. Числови сравнения.

Теорема 1.1: Теорема за деление с остатък

За всеки $a, b, \in \mathbb{Z}, b \neq 0$ съществуват еднозначно определени числа p и q:

$$a = bq + r \text{ и } 0 \leq r < |b|.$$

Доказателство. Разглеждаме случая $a \geq 0, b > 0$.

Съществуване.

1. $a < b$

   Полагаме $q = 0, r = a \Rightarrow a = bq + r$ и $0 \leq r < b$.

2. Нека $a \geq b$ $q, q \in \mathbb{N}$ и е максималното естествено число такова, че

   $$qb \leq a < (q+1)b \Rightarrow 0 \leq r = a - qb < b$$

   и $a = qb + r$.

Единственост. Нека

$$\left| \begin{array}{lll} a & = q_1 b + r_1, & 0 \leq r_1 < b \\ a & = q_2 b + r_2, & 0 \leq r_2 < b \end{array} \right.$$

Изваждаме ги и получаваме

$$0 = (q_1 - q_2)b + r_1 - r_2$$
$$r_2 - r_1 = (q_1 - q_2)b.$$

Но $b > |r_2 - r_1| \Rightarrow$ е възможно само, ако

$$q_1 - q_2 = 0$$
$$r_2 - r_1 = 0,$$

т.е. $q_1 = q_2, r_1 = r_2$. □

q - частно при деление на a с b. r - остатък.

Дефиниция 1.2

Ненулевото число b "дели" a (или a се дели на b), $b \mid a$, ако $\exists q \in \mathbb{Z}$:

$$a = bq.$$

Твърдение 1.3

$$b \mid a \Leftrightarrow r = 0.$$

$b \nmid a$

Свойства на делимостта.

1. $a \neq 0, a \in \mathbb{Z} \Rightarrow a \mid a$.
2. Ако $b \mid a$ и $a \neq 0 \Rightarrow |b| \leq |a|$.
   (В частност, ако $b \mid a$ и $a \mid b \Rightarrow |a| = |b|$, т.е. $a = \pm b$.)
3. Ако $c \mid b$ и $b \mid a \Rightarrow c \mid a$.
4. Ако $b \mid a_1, \ldots, b \mid a_k \Rightarrow$ за произволни $t_1, \ldots, t_k \in \mathbb{Z}$ е в сила
   $$b \mid t_1 a_1 + \cdots + t_k a_k.$$
5. Ако $b \mid (a_1 + a_2)$ и $b \mid a_1 \Rightarrow b \mid a_2$.
   (В частност, ако $a_1 + a_2 = 0$ и $b \mid a_1 \Rightarrow b \mid a_2$.)

Твърдение 1.4

Нека $p \geq 2$ е фиксирано естествено число. Тогава всяко естествено число a може да се представи по единствен начин във вида:

$$a = c_n p^n + c_{n-1} p^{n-1} + \cdots + c_1 p + c_0,$$

където $c_n > 0$ и $0 \leq c_i < p, \forall i = 0, \ldots, n$. (Това е p-ичния запис на числото a или a в p-ична бройна система с p-ични цифри $c_0, c_1, \ldots, c_n$.)

Доказателство. (Схематично) **Съществуване.**
Индукция $a = pq + r, 0 \leq r < p$ и ИП за q.
$q = b_k p^k + b_{k-1} p^{k-1} + \cdots + b_0, 0 \leq b_i < p, b_k > 0 \Rightarrow$
$a = b_k p^{k+1} + b_{k-1} p^k + dots + b_0 p + r$, т.е. е представяне от вида:
$a = c_n p^n + \ldots c_0$.
Единственост.

$$\left| \begin{array}{ll} a = c_n p^n + \ldots c_0, & 0 \leq c_i < p, c_n > 0 \\ a = b_n p^n + \ldots b_0, & 0 \leq b_i < p, b_n > 0 \end{array} \right.$$

$\Rightarrow p / b_0 - c_0 \Rightarrow b_0 = c_0$
$\Rightarrow c_n p^n + \ldots c_1 = b_n p^n + \ldots b_1 \Rightarrow p / b_1 - c_1 \Rightarrow b_1 = c_1$ и т.н.

□

Твърдение 1.5

Нека $m, n, p \in \mathbb{N}, p > 1$.

$$m \mid n \Leftrightarrow p^m - 1 \mid p^n - 1.$$

Доказателство. $n = mq + r, 0 \leq r < m$

$$\begin{aligned} p^n - 1 &= p^{mq+r} - 1 = \\ &= p^{mq+r} - p^r + p^r - 1 = \\ &= p^r (p^{mq} - 1) + (p^r - 1) = \\ &= (p^m - 1) A + (p^r - 1), \end{aligned}$$

където $A = p^r (p^{m(q-1)} + \cdots + p^m + 1) \in \mathbb{Z}$. □

Дефиниция 1.6: НОД (най-голям общ делител)

Нека $a, b \in \mathbb{Z}$ и $(a, b) \neq (0, 0)$, т.е. поне едното число е различно от нула.
***Най-голям общ делител (НОД)** на числата a е b е d:*

1) $d \mid a, d \mid b$;

2) Ако $d_1 \mid a$ и $d_1 \mid b \Rightarrow d_1 \mid d$

$d = (a, b)$ ($d = НОД(a, b)$.)

Аналогично се дефинира НОД$(a_1, a_2, \ldots, a_k)$, $d = (a_1, a_2 \ldots, a_k)$.
НОД е еднозначно определен, ако е положителен.

1.1 Алгоритъм на Евклид.

Алгоритъмът на Евклид е едновременно доказателство и практическо правило за намирането на НОД(a, b).

Нека за определеност $a > 0, b > 0$ и

$$\begin{array}{lll} & a = bq_1 + r_1, & 0 \leq r_1 < b \\ \text{ако } r_1 \neq 0, & b = r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\ \text{ако } r_2 \neq 0, & r_1 = r_2q_3 + r_3, & 0 \leq r_3 < r_2 \\ & \dots & \\ \text{ако } r_{n-1} \neq 0, & r_{n-2} = r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1} \\ \text{ако } r_n \neq 0, & r_{n-1} = r_nq_{n+1} + r_{n+1}, & r_{n+1} = 0 \end{array}$$

Т.к. $r_1 > r_2 > r_3 > \dots$ процесът е краен, следователно след краен брой стъпки остатъка е равен на нула, т.е. $\Rightarrow r_{n+1} = 0$.

Връщаме се назад: $\Rightarrow r_n \mid a, r_n \mid b$.

Нека $d_1 \mid a, d_1 \mid b \Rightarrow d_1 \mid r_1$ и продължавайки надолу по равенствата $\Rightarrow d_1 \mid r_n$.

Следователно $r_n = (a, b)$.

Дефиниция 1.7:

Ако $(a, b) = 1 \Rightarrow a$ и b са взаимно прости.

Твърдение 1.8:

Ако

$$(a, b) = d \Rightarrow \exists\, u, v \in \mathbb{Z} : ua + vb = d.$$

(В частност, ако $(a, b) = 1 \Rightarrow \exists\, u, v \in \mathbb{Z} : ua + vb = 1$.)

Доказателство.

$$\begin{array}{ll} r_{n-1} = r_nq_{n+1} & \Rightarrow r_n = d \\ r_{n-2} = r_{n-1}q_n + r_n & \Rightarrow d = r_n = r_{n-2} - r_{n-1}q_n \\ r_{n-3} = r_{n-2}q_n + r_{n-1} & \Rightarrow r_{n-1} = r_{n-3} - r_{n-2}q_{n-2} \\ \dots & \\ a = bq_1 + r_1 & \Rightarrow r_1 = a - bq_1, \end{array}$$

т.е $d = ua + vb$ за подходящи цели числа u, v. □

Твърдение 1.9:

Ако $a, b \in \mathbb{Z},\ (a, b) \neq (0, 0), (a, b) = d\ d = ua + vb \Rightarrow (u, v) = 1$.??? Числата от тъждеството на Безу u, v са взаимно прости.

Доказателство.

$$\begin{array}{lll} (a,b)=d & \Rightarrow d=ua+vb/:d & \\ & \Rightarrow ua_1+vb_1=1 & \\ \text{Да допуснем, че } (u,v)=t & \Rightarrow u=u_1t, v=v_1t & \Rightarrow t(u_1a_1+v_1b_1)=1 \\ & \Rightarrow t\mid 1 & \Rightarrow (u,v)=1. \end{array}$$

□

Твърдение 1.10:

Ако $b \mid a_1a_2$ *и* $(b,a_1)=1 \Rightarrow b \mid a_2$.

Доказателство.

$$\begin{array}{ll} (b,a_1)=1 & \Rightarrow \exists u,v\in\mathbb{Z}: ub+va_1=1/.a_2 \\ & \Rightarrow uba_2+va_1a_2=a_2 \\ & \Rightarrow b\mid uba_2,\ b\mid va_1a_2 \qquad \Rightarrow b\mid a_2. \end{array}$$

□

Твърдение 1.11:

Ако $b_1 \mid a,\ b_2 \mid a$ *и* $(b_1,b_2)=1 \Rightarrow b_1b_2 \mid a$.

Доказателство. Нека $a=b_1q$.
$b_2 \mid a=b_1q$ и $(b_1,b_2)=1 \Rightarrow b_2 \mid q \Rightarrow b_1b_2 \mid b_1q=a$. □

Дефиниция 1.12: НОК (най-малко общо кратно

Най-малко общо кратно (НОК) *на* a *и* b $(a\neq 0$ *и* $b\neq 0)$ *е числото* $k=HOK(a,b)$, *ако*

1) $a \mid k,\ b \mid k$;

2) *ако* $a \mid k_1$ *и* $b \mid k_1 \Rightarrow k \mid k_1$.

$k=[a,b]$. *Аналогично* $k=[a_1,a_2,\ldots,a_n]$.

Твърдение 1.13:

В сила е

$$(a,b)[a,b]=ab.$$

(Ако $(a,b)=1 \Rightarrow [a,b]=ab$.*)*

Доказателство. ??? □

Дефиниция 1.14: Просто число

Естественото число $p > 1$ е просто, ако единствените му делители са ± 1 и $\pm p$.

Ако p е просто число и $(p, a) = 1$, то е еквивалентно на $p \nmid a$.

Твърдение 1.15:

Ако p е просто число, $p \mid a_1 a_2$ и $p \nmid a_1 \Rightarrow p \mid a_2$.

Доказателство. Тв. 1.10 □

Теорема 1.16: Основна лема на аритметиката

Всяко естествено число $n > 1$ се представя по единствен начин (с точност до реда на множителите) като произведение на прости числа.

Доказателство. **Съществуване.** Ако е просто число $\Rightarrow OK$.
n - не е просто $\Rightarrow n = n_1 n_2$
ИП за n_1 и n_2 и оттам за $n = \prod p_i$.
Единственост.
Нека $n = p_1 \dots p_k = q_1 \dots q_s$.
$\Rightarrow p_1 \mid q_1 \dots q_s \Rightarrow p_1 \mid q_1$ (например) q_1 - просто
$\Rightarrow p_1 = q_1$ съкращаваме на $p_1 \Rightarrow$
$p_2 \dots p_k = q_2 \dots q_s$ и продължаваме по същия начин $k = s, p_2 = q_2, \dots, p_k = q_s$.
□

Дефиниция 1.17: Канонично разлагане n на прости множители

***Каноничното разлагане на числото** n **на прости множители** е представянето му във вида:*

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

като $p_1, \dots, p_k$ са две по две различни прости числа и $\alpha_i > 0$ $(i = 1, \dots, k)$.

Теорема 1.18:

Съществуват безброй много прости числа.

Доказателство. □

1.2 Сравнения

Дефиниция 1.19:

Нека $n \in \mathbb{N}, a, b \in \mathbb{Z}$. *Казваме, че* a ***е сравнимо с*** b ***по модул*** n,

$$a \equiv b \pmod{n}, \text{ ако } n \mid a - b.$$

Ясно е, че $a \equiv b \pmod{n} \Leftrightarrow a$ и b имат равни остатъци при деление на n.

Свойства

1. $a \equiv a \pmod{n}$ $\forall a \in \mathbb{Z}$. (Рефлексивност)
2. Ако $a \equiv b \pmod{n}$, то $b \equiv a \pmod{n}$. (Симетричност).
3. Ако $a \equiv b \pmod{n}$ и $b \equiv c \pmod{n}$, то $a \equiv c \pmod{n}$. (Транзитивност).
4. Ако $a_1 \equiv b_1 \pmod{n}$ и $a_2 \equiv b_2 \pmod{n}$, то
   $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{n}$ и $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.
5. Ако $am \equiv bm \pmod{n}$ и $(m, n) = 1$, то $a \equiv b \pmod{n}$.

$\mathbb{Z}$ се разбива на непресичащи се класове от сравними помежду си числа по модул n - това са елементите на пръстена $\mathbb{Z}_n$

Дефиниция 1.20: Функцията на Ойлер $\varphi(n)$

Нека $n \in \mathbb{N}$. *Функцията на Ойлер означаваме с* $\varphi(n)$ *и равна на броя на естествените числа, ненадминаващи* n *и взаимно прости с* n, *т.е.*

$$\varphi(n) = |\{a \mid a \in \mathbb{N},\ a < n,\ (a, n) = 1\}|.$$

ПРИМЕРИ:

$\varphi(1) = \varphi(2) = 1$
$\varphi(3) = \varphi(4) = 2$
$\varphi(5) = 4$
$\varphi(6) = 2$
$\varphi(p) = p - 1$, p - просто число

Твърдение 1.21:

Ако p *е просто число и* $\alpha \in \mathbb{N}$, *то*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1).$$

Доказателство. От всички числа трябва да извадим тези, които не са взаимно прости с p, т.е числата ($p^{\alpha-1}$ на брой):

$$1.p, 2.p, \ldots, p.p, \ldots, p^{\alpha-1}.p$$

□

Дефиниция 1.22: Мултипликативна функция

Една аритметична функция f наричаме ***мултипликативна****, ако $f(mn) = f(m)f(n)$, когато m и n са взимно прости.*

Теорема 1.23:

Функцията на Ойлер е мултипликативна, т.е. ако $(a, b) = 1$, то

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Доказателство. Да разположим числата $1, 2, \ldots, ab$ в следната матрица:

$$A = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & a \\ a+1 & a+2 & \cdots & a+i & \cdots & 2a \\ \cdots & & & & & \\ (b-1)a+1 & (b-1)a+2 & \cdots & (b-1)a+i & \cdots & ba \end{pmatrix}$$

Твърдение: Свойство 1

Матрицата A притежава $\varphi(a)$ на брой стълба, състоящи се от числа взаимно прости с a.

В 1-вия ред има $\varphi(a)$ на брой числа взаимно прости с a. Числата, в кой и да е стълб на A са сравними по модул a, т.е. да разгледаме i -тия стълб

$$ka + i \equiv la + i \pmod{a}.$$

Твърдение: Свойство 2

Всеки стълб на матрицата A съдържа точно $\varphi(b)$ на брой числа, взаимно прости с b.

Числата в кой и да е стълб на A са две по две несравними по модул b.

Нека разгледаме l-тия стълб и съответно i-тия и j-тия ред.

$$\begin{pmatrix} l \\ a+l \\ \vdots \\ (i-1)a+l \\ \vdots \\ (j-1)a+l \\ \vdots \\ (b-1)a+l \end{pmatrix}$$

Числата в този стълб (в кой и да е стълб) са две по две несравними по модул b.

$$a_{il} - a_{jl} = (i-j)a \text{ и } b \nmid (i-j)a.$$

(Ако $b \mid (i-j)a, (a,b) = 1 \Rightarrow b \mid i-j$ - противоречие!)

Но числата в този стълб са b на брой и значи дават всички остатъци по модул $b - (1, 2, \ldots, b-1)$ - в някакъв ред. Следователно точно $\varphi(b)$ са взаимно прости с b.

От Св.1 и Св. 2 следва, че броя на естествените числа по-малки от ab и взаимно прости както с a, така и с b е равен на $\varphi(a)\varphi(b)$.

Но едно число е взаимно просто както с a, така и с b, точно когато е взаимно просто с ab. Следователно

$$\varphi(a)\varphi(b) = \varphi(ab).$$

□

Твърдение 1.24:

Нека $n \in \mathbb{N}, n > 1$ и $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ е каноничното му разлагане в произведение на прости множители. Тогава

$$\varphi(n) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right),$$

Доказателство. □

Теорема 1.25: Теорема на Ойлер-Ферма

Нека $n \in \mathbb{N}, r \in \mathbb{Z}$ и $(r, n) = 1$. Тогава

$$r^{\varphi(n)} \equiv 1 \pmod{n}.$$

В частност, ако p е просто число и $p \nmid r$, то $r^{p-1} \equiv 1 \pmod{n}$.

Доказателство. □

Теорема 1.26: Теорема на Уйлсън

Ако p е просто число, то

$$(p-1)! \equiv -1 \pmod{n}.$$

Доказателство. □

Глава 2

Групи - определение, примери, основни свойства.

Дефиниция 2.1: Бинарна операция

Нека G е непразно множество. Всяко изображение $G \times G \to G$ се нарича ***бинарна операция*** *в G.*

С други думи бинарната операция е правило, което можем да прилагаме на всяка наредена двойка от елементи от множеството G и получаваме нов елемент от G.

ПРИМЕРИ:

Нека F е числово поле. Бинарни операции $F \times F \to F$ са

- **събирането** : $(a, b) \to a + b$;
- **умножението** : $(a, b) \to ab$.

Дефиниция 2.2: Група

Непразното множество G се нарича ***група*** *спрямо бинарната операция $\star$, ако*

G1) $a \star b \in G,\ \forall a, b \in G$ *(затворено относно бинарната операция);*

G2) $(a \star b) \star c = a \star (b \star c)$ *за всяко $a, b, c \in G$ (асоциативност);*

G3) Съществува такъв елемент $e \in G$, че $a \star e = e \star a = a, \forall a \in G$ (съществуване на единица);

G4) $\forall a \in G$ *съществува такъв елемент $x \in G$, че $a \star x = x \star a = e$ (съществуване на обратен елемент).*

Бележим с $(G, \star)$ или $G(\star)$.

Дефиниция 2.3: Ред на група

Нека е група. G е ***крайна група****, ако има краен брой елементи, в противен случай -* ***безкрайна група****. Броят на елементите в G (бележи се с $|G|$), се нарича* ***ред*** *на G.*

Дефиниция 2.4: Комутиращи елементи и абелева група

Нека $(G, \star)$ е група и a и b са елементи от G. Казваме, че a и b ***комутират****, ако*

$$a \star b = b \star a.$$

Групата G е ***абелева****, ако всяка двойка елементи комутира, т.е.*

$$a \star b = b \star a, \ \forall a, b \in G.$$

За удобство операциата, когато не е изрично уточнена ще записваме като умножение. Операцията в група е асоциативна, т.е.

$$(ab)c = a(bc) = abc.$$

Това важи и за повече елементи, т.е.

$$\underbrace{a \cdots a}_{\text{n}} = a^n$$

По определение $a^0 = e$. Важат обичайните правила за действие със степени ...
$a^{-n} = (a^{-1})^n = (a^n)^{-1}$.
...

Твърдение 2.5

Нека G е група. Тогава

(a) единичният елемент e е единствен.

(b) всеки елемент $a \in G$ има единствен обратен.

(c) за всеки елемент $a \in G$ имаме $(a^{-1})^{-1} = a$.

(d) ако a и b са елементи от G, то $(ab)^{-1} = b^{-1}a^{-1}$.

Доказателство. (a) Нека e' и e'' са единици в групата G. Тогава

$$e'e'' = \begin{cases} e', \ e'' - \text{единица} \\ e'', \ e' - \text{единица} \end{cases} \Rightarrow \ e' = e''.$$

(b) Нека a' и a'' са обратни елементи на a. Тогава

$$a'aa'' = \begin{cases} a' \underbrace{(aa'')}_{e} = a' \\ \underbrace{(a'a)}_{e} a'' = a'' \end{cases} \quad \Rightarrow \; a' = a''.$$

(c) За всеки елемент $a \in G$ имаме

$$a^{-1}a = aa^{-1} = e.$$

Това означава, че a е обратния елемент на a^{-1}, т.е. $(a^{-1})^{-1} = a$.

(d) За да покажем, че обратния елемент на ab е $b^{-1}a^{-1}$ трябва да проверим, че произведението им дава единица. Имаме, че

$$(ab)(b^{-1}a^{-1}) = e, \quad \text{както и} \quad (b^{-1}a^{-1})(ab) = e$$

и следователно ab и $b^{-1}a^{-1}$ са обратни един на друг $\Rightarrow (ab)^{-1} = b^{-1}a^{-1}$.

□

Аналогично $(a_1a_2 \dots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1} \dots a_1^{-1}$.

$(G, +)$	$(G, .)$
мултипликативен запис	адитивен запис
произведение: ab	сума: $a + b$
единичен елемент	нулев елемент
$e = 1$	$e = 0$
$a^0 = 1$	$0a = 0$
обратен елемент	противоположен елемент
a^{-1}	$-a$
$a(bc) = (ab)c$	$a + (b + c) = (a + b) + c$
a^n	na
степен	кратно
$a^{-n} = (a^n)^{-1}$	$(-n)a = n(-a)$

ПРИМЕРИ:

- Адитивните групи на целите, рационалните, реалните и комплексните числа, т.е. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ (Абелеви групи).
- Нека $n \in \mathbb{N}$ е естествено число и $n\mathbb{Z} = \{na | a \in \mathbb{Z}\}$. Тогава $(n\mathbb{Z},+)$ е абелева група.
- Мултипликативните групи на целите, рационалните, реалните и комплексните числа, т.е. $(\mathbb{Z}^\star,.),(\mathbb{Q}^\star,.),(\mathbb{R}^\star,.),(\mathbb{C}^\star,.)$ са абелеви групи. Ако F е поле, то $F^\star = F \setminus \{0\}$ се нарича мултипликативна група на полето F.
- Нека $\mathbb{C}_n = \{x \in \mathbb{C} | x^n = 1\}$ са n -ти корени на единицата и $w_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, k = 0,1,\ldots,n$. $w_k = w_1^k$ Тогава $(\mathbb{C}_n,.)$ е абелева група.
- Нека V е линейно пространство, то $(V,+)$ относно операцията събиране на вектори е абелева група.
- **Общата линейна група от степен n над полето F,** т.е. множеството от всички неособени квадратни матрици от ред n с елементи от поле F

$$GL_n(F) = \{A \in M_n(F) | \det(A) \neq 0\}.$$

  Тази група не е абелева, при $n \geq 2$.
- **Специалната линейна група от степен n над полето F,** т.е. множеството от всички квадратни матрици от ред n с елементи от поле F с детеминанта 1,

$$SL_n(F) = \{A \in M_n(F) | \det(A) = 1\}.$$

  Тази група не е абелева, при $n \geq 2$.
- Нека Ω е множество и да означим с S_Ω множеството от всички биекции на Ω, т.е.

$$S_\Omega = \{f : \Omega \to \Omega | f - \text{биекция}\}.$$

  $(S_\Omega,.)$ с операцията произведение на изображения образува група. Ако Ω е крайно множество с n елемента, то пишем S_n вместо S_Ω. Това е защото не се интересуваме от самите елементи на множеството $\Omega = \{a_1,a_2,\ldots,a_n\}$, а от номерата им, т.е. $\Omega_n = \{1,2,\ldots,n\}$. Групата S_n се нарича **симетрична група от степен** n. Групата не е абелева при $n \geq 3$. Под произведение fg на две такива изображения f и g се нарича резултатът от тяхното последователно изпълнение (тяхната композиция), т.е.

$$fg(x) = f(g(x)), \forall x \in \Omega.$$

Дефиниция 2.6

Нека G е група и H е непразно подмножество на G. H е подгрупа на G, ако

1) $\forall a, b \in H \Rightarrow ab \in H$;

2) $\forall a \in H \Rightarrow a^{-1} \in H$.

Пишем $H \leq G$ или $H < G$.

Твърдение 2.7

Нека H е погрупа на G, т.е. $H \leq G$. Тогава:

1) $e \in H$;

2) H *е група относно операцията в* G;

3) $H_i \leq G \Rightarrow \cap H_i \leq G$;

4) ако $a, b \in H \Rightarrow ab^{-1} \in H$.

Доказателство. 1) $e \in H$;

2) H е група относно операцията в G;

3) $H_i \leq G \Rightarrow \cap H_i \leq G$;

4) ако $a, b \in H \Rightarrow ab^{-1} \in H$.

□

ПРИМЕРИ:

- Тривиални подгрупи на G са $\{e\} < G$ и $G \leq G$.
- $(n\mathbb{Z}_n, +) < (\mathbb{Z}, +) < (\mathbb{Q}, +)(\mathbb{R}, +) < (\mathbb{C}, +)$
- $(\mathbb{Q}^\star, .) < (\mathbb{R}^\star, .) < (\mathbb{C}^\star, .)$
  $(n\mathbb{C}_n, .) < (\mathbb{C}^\star, .)$
- $SL_n(F) < GL_nF$, операцията е умножение на матрици.

Дефиниция 2.8: Център на група

Център на групата *G, наричаме множеството:*

$$Z(G) = \{z \in G | zg = gz \ \forall g \in G\}.$$

$Z(G) \Leftrightarrow G$ е абелева група.

Твърдение 2.9

$Z(G) \leq G$, т.е. центърът на групата G е подгрупа на G.

Доказателство. 1) $a, b \in Z(G)$

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab) \Rightarrow ab \in Z(G)$$

2) $a \in Z(G)$

$$\begin{aligned} ag &= ga \ /a^{-1} \\ a^{-1}ag &= a^{-1}ga/a^{-1} \\ g &= a^{-1}ga/a^{-1} \\ ga^{-1} &= a^{-1}g \end{aligned}$$

$\Rightarrow a^{-1} \in Z(G)$.

□

Дефиниция 2.10: Хомоморфизъм на групи

*Нека $(G, \star)$ и $(G', \circ)$ са групи. Казваме, че φ е **хомоморфизъм на групи**, ако*

1) $\varphi : G \to G'$ е изображение;

2) $\forall a, b \in G$ е изпълнено:

$$\varphi(a \star b) = \varphi(a) \circ \varphi(b),$$

т.е. φ запазва груповата операция.

Ако φ е биекция, наричаме φ изоморфизъм.

Твърдение 2.11

Ако $\varphi : G \to G'$ е хомоморфизъм на групи, то

1) $\varphi(e) = e'$;

2) $\varphi(a^{-1}) = \varphi(a)^{-1}$, $a \in G$.

Доказателство. □

ПРИМЕРИ:

- $\varphi : \mathbb{C}_n \to \mathbb{C}^\star, \varphi(z) = z, z \in \mathbb{C}_n$ хомоморфизъм на групи.
- $\varphi : \mathbb{Z} \to \mathbb{Z}_n, \varphi(z) = nz, z \in \mathbb{Z}$ измоморфизъм на групи.
- Нека F е числово поле.
  $\det : GL_n(F) \to F^\star, \det : A \to \det(A)$, хомоморфизъм на групи.

Глава 3

Ред на елемент. Циклична група. Групата Zn.

3.1 Ред на елемент

Нека G е група и $g \in G$.

Дефиниция 3.1

Нека n е положително цяло число. Нека $(G, .)$ е група и $g \in G$. Дефинираме:

$$g^n = \underbrace{g \cdots g}_{n},\ g^0 = e \text{ и } g^{-n} = (g^{-1})^n.$$

Твърдение 3.2

Нека G е група, $g \in G$, $m, n \in \mathbb{Z}$. Тогава:

a) $g^m g^n = g^{m+n}$;

b) $(g^n)^{-1} = g^{-n}$;

c) $(g^m)^n = g^{mn}$.

Доказателство. а) $g^m g^n = g^{m+n}$;

Ако $m = 0$, то $g^{0+n} = g^n = eg^n = g^0 g^n$.

Аналогично, ако $n = 0$.

Нека $m, n \in Z \setminus \{0\}$. Нека $m > 0, n > 0$, тогава

$$g^m g^n = \underbrace{g \cdots g}_{m} \underbrace{g \cdots g}_{n} = \underbrace{g \cdots g}_{m+n} = g^{m+n},$$

Ако $m < 0, n < 0$, тогава

$$g^m g^n = \underbrace{g^{-1} \cdots g^{-1}}_{|m|} \underbrace{g^{-1} \cdots g^{-1}}_{|n|} = \underbrace{g^{-1} \cdots g^{-1}}_{|m|+|n|} = g^{m+n},$$

Нека $m, n \in \mathbb{Z} \setminus \{0\}$ са с различни знаци и $|m| \geq |n|$. Ако означим с $\varepsilon = sign(m)$ (където $sign(m) = \begin{cases} 1, & m > 0 \\ -1, & m < 0 \end{cases}$), тогава $sign(n) = -\varepsilon$ и

$$g^m g^n = \underbrace{g^{\varepsilon} \cdots g^{\varepsilon}}_{|m|} \underbrace{g^{-\varepsilon} \cdots g^{-\varepsilon}}_{|n|} = \underbrace{g^{\varepsilon} \cdots g^{\varepsilon}}_{|m|-|n|} = g^{m+n}.$$

b) За целта трябва да покажем, че g^{-n} е обратен на g^n, т.е.

$$g^{-n} g^n = g^n g^{-n} = e.$$

Това е директно следствие от а).

c) $(g^m)^n = g^{mn}$ Ако $n = 0$, то $g^m.0 = g^0 = e = (g^m)^0$.

Ако $n \in \mathbb{N}$, то

$$(g^m)^n = \underbrace{g^m \ldots g^m}_{n} = g^{\underbrace{m + \cdots + m}_{n}} = g^{mn}.$$

Ако $n \in \mathbb{Z}, n < 0$, то

$$(g^m)^n = \underbrace{(g^m)^{-1} \ldots (g^m)^{-1}}_{|n|} = \underbrace{g^{-m} \ldots g^{-m}}_{|n|} = g^{\underbrace{(-m) + \cdots + (-m)}_{|n|}} = g^{(-m)|n|} = g^{mn},$$

като използвахме, че $(g^m)^{-1} = g^{-m}$ и вече доказаното в а) за умножение на степени с равни основи.

□

Дефиниция 3.3

Нека G е група и $g \in G$. Да означим множеството от всички степени на g с

$$\langle g \rangle = \{g^k | k \in \mathbb{Z}\} \subseteq G.$$

Твърдение 3.4

$\langle g \rangle$ е подгрупа на G.

Доказателство. 1) $a, b \in \langle g \rangle \Rightarrow a = g^m, b = g^n, m, n \in \mathbb{Z}$
$\Rightarrow ab = g^m g^n = g^{m+n} \in \langle g \rangle$.

2) $a \in \langle g \rangle \Rightarrow a = g^n, n \in \mathbb{Z} \Rightarrow a^{-1} = (g^n)^{-1} = g^{-n} \in \langle g \rangle$.

□

Дефиниция 3.5: Циклична подгрупа

Подгрупата $\langle g \rangle$ се нарича ***циклична подгрупа*** *на групата G, породена от елемента g.*
Елементът g се нарича ***образуващ*** *или* ***пораждащ елемент*** *на цикличната подгрупа $\langle g \rangle$.*

ПРИМЕРИ:

- $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$.
- $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ поражда подгрупа в $SL_2(\mathbb{Z})$

Твърдение 3.6

Групата $\langle g \rangle$ е абелева група.
(Дори в случая, когато G не е абелева.)

Доказателство. $a, b \in \langle g \rangle$
$a = g^m, b = g^n, m, n \in \mathbb{Z}$
$\Rightarrow ab = g^m g^n = g^{m+n} = g^n g^m = ba.$ □

Да разгледаме подгрупите породени от числото 5 и i в групата $(\mathbb{C}^\star, .)$.

$$\langle 5 \rangle = \{5^0 = 1, 5^1, 5^{-1}, 5^2, 5^{-2} \dots\} \text{ - всички степени са различни}$$
$$\langle i \rangle = \{i, i^2 = -1, i^3 = -i, i^4 = 1\} \text{ - само 4 степени са различни}$$

За елементите на $\langle g \rangle$ има 2 възможности:

1. Всички степени на g са различни, т.е. $\forall m, n \in \mathbb{Z}, m \neq n$ е в сила $g^m \neq g^n$. Следователно реда на групата $\langle g \rangle$ е безкраен.

2. Поне две степени на елемента g са равни.

   $\exists \quad m,\ n \in \mathbb{Z},\ m \neq n : (m > n)$
   $g^m = g^n \ /.g^{-n} \Rightarrow g^{m-n} = e.$

   Т.е съществуват положителни степени на g, които са равни на e, т.е. съществува **естествено число** $r = m - n : g^r = e$.

Твърдение 3.7

Нека n е най-малкото естествено число, за което $g^n = e$. Тогава подгрупата има краен ред, т.е. $|\langle g\rangle| = n$ и и се изчерпва с елементите:

$$\langle g\rangle = \{e, g, g^2, \ldots, g^{n-1}\},$$

които са различни помежду си.

Доказателство. Ще докажем, че елементите $e, g, g^2, \ldots, g^{n-1}$ са

1. два по два различни;

   Нека $0 \leq k < m \leq n-1$ и да допуснем, че $g^k = g^m \ /.g^{-k}$
   $g^{m-k} = e \Rightarrow 0 < m-k < n \Rightarrow$ противоречие с избора на n.

2. всяка цяла степен на g е равна на някой от тях, т.е.
   $\forall m \in \mathbb{Z} \Rightarrow g^m = g^i, i = 0, 1, \ldots, n-1$.

   $k \in \mathbb{Z}$ -произволен
   $k = nq + r,\ 0 \leq r < n$
   $\Rightarrow g^k = g^{nq+r} = (g^n)^q g^r = g^r$.

□

Дефиниция 3.8: Ред на елемент

*Казваме, че елементът $g \in G$ има **безкраен ред**, ако всички негови степени са различни помежду си, т.е. ако $g^m = e$ е възможно, само тогава когато $m = 0$. ($\forall m, n \in \mathbb{Z}(m \neq n) \Rightarrow g^m \neq g^n$ $g^m = e \Leftrightarrow m = 0$.)*
*Казваме, че g има **краен ред** n, ако n е най-малкото естествено число, за което $g^n = e$.*
Бележим реда на g с $|g|, r(g), o(g), ord(g)$.

Ако $(G, .)$ е група, то G притежава единствен елемент от ред 1, а именно e и

$$\langle e\rangle \equiv \text{ единичната подгрупа.}$$

Твърдение 3.9

Ако $r(g) = n < \infty \Rightarrow |\langle g\rangle| = n$.

Доказателство. Всички елементи на цикличната група $\langle g\rangle$ в този случай са $e, g, g^2, \ldots, g^{n-1}$ и са различни помежду си. □

Твърдение 3.10

Ако $r(g) = n < \infty$, то $g^m = e \Leftrightarrow n/m$.

Доказателство. $\Rightarrow$) $g^m = e$ и $m = nq + r,\ 0 \leq r < n$
$\Rightarrow e = g^m = g^{nq+r} = (g^n)^q g^r = g^r$
$\Rightarrow r = 0 \Rightarrow n/m.$

$\Leftarrow$) n/m т.е. $m = nq \Rightarrow g^m = e.$

□

Дефиниция 3.11

Групата G се нарича ***периодична****, ако всички нейни елементи имат крайни редове и* ***група без торзии****, ако всички нейни елементи имат безкраен ред. G е* ***смесена****, ако тя притежава, както елементи от безкраен ред, така и неединични елементи от крайни редове.*

ПРИМЕРИ:

- Всяка крайна група е периодична.
- Без торзии са $(\mathbb{R}^+, .), (\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$.
- Смесени са $(\mathbb{Q}^\star, .), (\mathbb{R}^\star, .), (\mathbb{C}^\star, .)$. Съдържат както елементи от безкраен ред, така неединични и от краен ред (елемента -1).

3.2 Циклична група

Дефиниция 3.12: Циклична група

Групата G се нарича ***циклична****, ако тя се състои от степените на един от свойте елементи g, т.е. ако съвпада с някоя своя цикличната подгрупа,*

$$G \equiv \langle g \rangle.$$

Елементът g се нарича образуващ или пораждащ елемент на G.

ПРИМЕРИ:

- $(G,+) \Rightarrow G = \langle g \rangle = \{ng | n \in \mathbb{Z}\}$.
- $(G,.) \Rightarrow G = \langle g \rangle = \{g^n | n \in \mathbb{Z}\}$.
- G - циклична, следователно абелева.
- $(\mathbb{Z},+) = \langle 1 \rangle = \langle -1 \rangle$.
- n-ти те корени на единицата

$$(\mathbb{C}_n,.) = \langle w_1 \rangle = \{1, w_1, w_1^2, \ldots, w_1^{n-1}\},$$

където $w_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

Теорема 3.13

Нека G е циклична група.

а) Ако $|G| = \infty$, то $(G,.) \cong (\mathbb{Z},+)$.

b) Ако $|G| = n < \infty$, то $(G,.) \cong (\mathbb{C}_n,.)$.

Доказателство. а) $G = \langle g \rangle$ и $|G| = \infty$.
Разглеждаме изображението: $\varphi : G \to \mathbb{Z}$, $\varphi(g^k) = k$.

1. φ - биекция;
2. φ - хомоморфизъм

$$\varphi(g^k g^l) = \varphi(g^{k+l}) = k + l = \varphi(g^k) + \varphi(g^l) \Rightarrow \varphi \text{ - изоморфизъм.}$$

b) $G = \langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ циклична група от ред n
Разглеждаме изображението: $\varphi : G \to \mathbb{C}_n$, $\varphi(g^k) = w_1^k$, $k = 0, 1, \ldots n-1$.

1. φ - биекция;
2. φ - хомоморфизъм
   Ако $0 \le l, k < n$ и $k + l = nq + r$, $0 \le r < n$,

$$\varphi(g^k g^l) = \varphi(g^{k+l}) = \varphi(g^{nq+r}) = \varphi(g^r) = w_1^r = w_1^{nq+r} = w_1^{k+l} = w_1^k w_1^l = \varphi(g^k)\varphi(g^l)$$

$\Rightarrow \varphi$- изоморфизъм.

□

Благодарение на тази теорема може да говорим за безкрайната циклична група и крайната циклична група от ред n.

Твърдение 3.14

Всяка подгрупа на циклична група е циклична.

Доказателство. Нека $(G, .)$ е циклична група, т.е. $G = \langle g \rangle$ и $H \leq G$.

1) Ако $H = \{e\}$, то H е циклична група.

2) Нека $H \neq \{e\}$.

- H съдържа и положителни степени на g, защото ако $g^t \in H \Rightarrow g^{-t} \in H$.
- Нека k е най-малкото естествено число, такова че $g^k \in H$.
- Ще докажем, че H е циклична група с образуващ елемент g^k, т.е. $H = \langle g^k \rangle$.
  Нека g^l е произволен $g^l \in H$ и $l = kq + r,\ 0 \leq r < k$.
  Тогава $g^l = (g^k)^q g^r \Rightarrow g^r = (g^k)^{-q} g^l \in H, ((g^k)^{-q} \in H, g^l \in H)$.
  Ако допуснем, че $r \neq 0, g^r \in H$ при $0 < r < k$ противоречи с избора на k.
  $\Rightarrow r = 0$ и $l = kq$, т.е. $g^l = (g^k)^q$ и $H = \langle g^k \rangle$.

□

Теорема 3.15

Подгрупите на $\mathbb{Z}$ се изчерпват с групите $r\mathbb{Z}, r \in \mathbb{N}$ или $\{0\}$.

Доказателство. $H \leq \mathbb{Z}, H \neq \{0\}$. Записвайки предната теорема на адитивен език $\Rightarrow H = \langle r \rangle = r\mathbb{Z}$, където r е минималното число с свойството $r \in H$. □

Теорема 3.16

Ако $G = \langle g \rangle$ е циклична група от ред n, то нейната подгрупа $H = \langle g^m \rangle$, породена от елемента g^m е от ред $\frac{n}{d}$, където $d = (n, m)$.

Доказателство. $|H| = |g^m| \Rightarrow$ трябва да докажем, че $|g^m| = \frac{n}{d}$.
Ако $|g^m| = s \Rightarrow s$ е минималното число, за което $(g^m)^s = e$.
Но $|g| = n \Rightarrow n/ms \Rightarrow \frac{sm}{n}$ е цяло число.
Нека $d = (n, m) \Rightarrow n = n_1 d, m = m_1 d$
$\Rightarrow \frac{sm}{n} = \frac{sdm_1}{dn_1} = \frac{sm_1}{n_1} \in \mathbb{Z}$
s е минималното такова число $\Rightarrow s = n_1 = \frac{n}{d}$.

□

Следствие 3.17

Ако $G = \langle g \rangle$ е циклична група от ред n, то елемента g^m $(m \in \mathbb{Z})$ е също образуващ елемент на $G \Leftrightarrow (m, n) = 1$.

Теорема 3.18

Подгрупите на $\mathbb{C}_n$ се изчерпват с групите $\mathbb{C}_q$, q/n.

3.3 Групата $\mathbb{Z}_n$

Глава 4

Симетрична група. Алтернативна група. Теорема на Кейли.

4.1 Пермутации, цикли, транспозиции. Симетричната група.

Нека Ω е множество и да означим с S_Ω множеството от всички взаимно еднозначни преобразувания на S_Ω (биекции) на Ω, т.е.

$$S_\Omega = \{f : \Omega \to \Omega | f - \text{биекция}\}.$$

Нека $f, g \in S_\Omega$ са две взимно еднозначни изображения от Ω върху Ω. Въвеждаме операция произведение на изображения fg, т.е. резултатът от тяхното последователно изпълнение (тяхната композиция), т.е.

$$fg(x) = f(g(x)), \forall x \in \Omega.$$

$(S_\Omega, .)$ с въведената бинарна операция (произведение на изображения) образува група.

- **Асоциативност.**

  $$(fg)h = f(gh),\ f, g, h \in S_\Omega$$

  По определение :

  $$\Big((fg)h\Big)(x) = fg\Big(h(x)\Big) = f\Big(g\Big(h(x)\Big)\Big)$$
  $$\Big(f(gh)\Big)(x) = f\Big(gh(x)\Big) = f\Big(g\Big(h(x)\Big)\Big)$$

  следователно $(fg)h(x) = f(gh)(x), \forall x \in \Omega$, т.е. $(fg)h = f(gh)$, тъй като те съвпадат върху всяко $x \in \Omega$.

- **В S_Ω съществува единствен елемент.** Тъждественото изображение (бележи се с: $e, (1)$, id), което оставя всеки елемент на място, т.е. $e(x) = x,\ x \in \Omega$, е биекция. Това преобразувание е единицата на S_Ω, т.е.

$$fe = ef = f,\ \forall f \in S_\Omega$$

  Това следва от

$$fe(x) = f(e(x)) = f(x)$$
$$ef(x) = e(f(x)) = f(x).$$

- **Всеки елемент $f \in S_\Omega$ притежава обратен от S_Ω.**

  Нека $f \in S_\Omega$ е биекция, то за произволен елемент $x \in \Omega$ съществува единствен първообраз $y \in \Omega$, за който $f(y) = x$. Да разгледаме изображението f', където $f'(x) = y \Leftrightarrow f(y) = x$. Тогава $f' \in S_\Omega$ и

$$ff' = f'f = e,$$

  т.е. f' е обратен елемент на f.

Следователно S_Ω е група, която се нарича група от взаимно еднозначните преобразувания на множеството Ω или симетричната група на Ω.

Групата не е абелева, ако множеството има повече от два елемента. Нека a, b и c са 3 различни елемента от Ω. Нека f оставя всички елементи на място освен a и b т.е $f(a) = b$ и $f(b) = a$. Нека g размества само a и c, а останали са неподвижни под действието на g, т.е $g(a) = c$ и $g(c) = a$. Тогава $f, g \in S_\Omega$ и

$$fg \neq gf,$$

защото $gf(b) = c$, $fg(b) = a$ и $a \neq c$.

Нека множеството Ω съдържа краен брой елементи, т.е. $\Omega = \{a_1, a_2, \ldots, a_n\}$. Преобразуването $f \in S_\Omega$ означаваме с:

$$f = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a'_1 & a'_2 & \ldots & a'_n \end{pmatrix},$$

където $a'_i = f(a_i)$. Но не е важно какви са елементите на множеството Ω, можем да считаме, че Ω се състои от числата $1, 2, \ldots, n$ и тогава

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

където $i_k = f(k)$. Наричаме f **субституция, субституция от степен** n или **пермутация** (защото f е биекция и $i_1 i_2 \ldots i_n$ е пермутация на числата $12 \ldots n$). Групата S_Ω бележим с S_n и наричаме **симетрична група от степен** n. Елементите на S_n са $n!$ на брой, т.к. това са всички пермутации на n елемента.

Тъждествената субституция и обратната субституция f^{-1} са съответно:

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}, \quad \text{и} \quad f^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Ако $g \in S_n$ е друга субституция и $g(i_k) = j_k,\ k = 0, 1, \dots, n$, то

$$gf(k) = g(f(k)) = g(i_k) = j_k, \quad \text{т.е.:}$$

$$gf = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}.$$

Дефиниция 4.1: Цикъл

Нека $i_1, i_2, \dots, i_m$ са различни елементи от $\Omega_n = \{1, 2, \dots, n\}$ и изображението $\sigma : \Omega_n \to \Omega_n$ е дефинирано по следното правило:

$$\sigma : \begin{cases} i_1 \to i_2 \\ i_2 \to i_3 \\ \dots \\ i_{m-1} \to i_m \\ i_m \to i_1 \\ k \to k, \forall k \in \Omega_n \setminus \{i_1, i_2, \dots, i_m\}. \end{cases}$$

Тогава σ е елемент на S_n, означава се с $(i_1\ i_2\ \dots\ i_m)$ и се нарича ***цикъл с дължина*** *m или m* ***- цикъл****.*

Очевидно всеки цикъл с дължина 1 е тъждествената субституция.

Дефиниция 4.2: Транспозиция

Цикъл с дължина 2 се нарича ***транспозиция****.*

Твърдение 4.3

Всеки m-цикъл в S_n има ред m.

Доказателство. Нека $\sigma = (i_1\ i_2\ \dots\ i_m)$ е m-цикъл. Тогава трябва да покажем, че $\sigma^m = id$, т.е. $\sigma^m(i_k) = i_k$, за всяко $k, 1 \le k \le m$.

$$\begin{aligned} \sigma(i_1) &= i_2 \\ \sigma^2(i_1) &= \sigma(\sigma(i_1)) = \sigma(i_2) = i_3 \\ &\dots \\ \sigma^m(i_1) &= \sigma^{m-1}(\sigma(i_1)) = \dots = i_1 \end{aligned}$$

Аналогично за всяко $i_k,\ 2 \le k \le m$. □

Дефиниция 4.4: Независими цикъла

Два цикъла $(i_1\ i_2\ \ldots\ i_k)$ *и* $(j_1\ j_2\ \ldots\ j_s)$ *се наричат* ***независими****, ако*

$$\{i_1, i_2, \ldots, i_k\} \cap \{j_1, j_2, \ldots, j_s\} = \emptyset.$$

Теорема 4.5

Нека n *е естествено число и* S_n *е симетричната група от степен* n*.*

(a) Ако f *и* g *са независими цикли от* S_n*, то те комутират, т.е.* $fg = gf$*.*

(b) Всеки елемент от S_n *може да бъде представен като произведение на независими цикли и това представяне е единствено с точност до реда на множителите.*

(c) Всеки елемент на S_n *може да бъде представен като произведение на транспозиции.*

Доказателство. (a) Нека $k \in \Omega_n = \{1, 2, \ldots, n\}$ и нека f и g са независими цикли от S_n.

- Нека f и g оставят неподвижен елемента k, т.е. $f(k) = k$ и $g(k) = k$. Тогава

$$f(g(k)) = f(k) = k = g(k) = g(f(k)).$$

- Понеже f и g са независими цикли, то следва, че точно единия от тях мести k. Без ограничение на общността, можем да считаме, че f оставя неподвижен елемента k, а g го мести, т.е. $f(k) = k, g(k) = k_1$. Тогава $g(k)$ също остава неподвижен под действието на f и се мести от g следователно

$$f(g(k)) = g(k) = g(f(k)).$$

И като резултат получаваме, че $fg = gf$.

(b) Пример:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 7 & 6 & 2 & 3 & 8 & 4 & 9 \end{pmatrix} = (1\ 5\ 2)(3\ 7\ 8\ 4\ 6)$$

Да забележим, че $\sigma(1) = 5, \sigma(5) = 2, \sigma(2) = 1$, т.е. имаме цикъл $(1\ 5\ 2)$. Продължавайки с елемент,който не е от този цикъл: $\sigma(3) = 7, \sigma(7) = 8, \sigma(8) = 4, \sigma(4) = 6$ и $\sigma(6) = 3 \Rightarrow (3\ 7\ 8\ 4\ 6)$. На място остава 9.Така накрая получаваме, че $\sigma = (1\ 5\ 2)(3\ 7\ 8\ 4\ 6)$.

Съществуване. Нека $\sigma \in S_n$ и $\sigma \neq id$. Да означим с

$$Supp(\sigma) = \{\ i \mid \sigma(i) \neq i,\ 1 \leq i \leq n\}$$

носителя на пермутацията σ, т.е. множеството на числата от 1 до n, които не оставят на място под действието на σ. Нека броят на елементите в това множество да означим с $n_\sigma = |Supp(\sigma)|$.

Индукция по броя на разместваните от σ символи, т.е. n_σ.

- $n_\sigma \neq 1$, защото $\sigma \neq id$. Следователно съществува i, такова че $\sigma(i) \neq i$. Съществува и j, такова, че $\sigma(j) = i$ (σ - биекция). Пермутацията σ разсмества поне два символа, тъй като $i \neq j$. Ако σ размества само два символа (i и j), то $\sigma = (i\ j)$ е транспозиция. В този случай σ има посоченото разлагане.
- Индукционно предположение за $n_\sigma < k$...
- Нека σ размества $n_\sigma = k > 2$ символа. Нека $i_1 \in Supp(\sigma)$. Да разгледаме редицата от $n+1$ члена:

$$i_1, i_2 = \sigma(i_1), i_3 = \sigma(i_2), \ldots, i_{n+1} = \sigma(i_n).$$

Тъй като числата $i_1, i_2, \ldots i_{n+1}$ са естествени и не по-големи от n, то поне два члена от тази редица ще съвпадат. Нека i_s е първият член от редицата, който съвпада с някой от следващите членове, т.е.

$$i_s = i_t,\ s < t \leq n+1$$

и s е минималното число с това свойство. Ако $s > 1$, то

$$\sigma(i_{s-1}) = i_s = i_t = \sigma(i_{t-1}),$$

което означава, че $i_{s-1} = i_{t-1},\ s-1 < t-1$ и това е противоречие с избора на s. Следователно $s = 1 \Rightarrow i_1 = i_t,\ 3 \leq t \leq n+1$.

Нека $\tau = (i_1\ i_2\ \ldots i_{t-1})$ е цикъл с дължина $t-1 \geq 2$. Да разгледаме $\sigma_1 = \tau^{-1}\sigma$. Тогава σ_1 оставя неподвижни числата $\{i_1, i_2, \ldots i_{t-1}\}$ и всички числа, който σ остава неподвижни, т.е.

$$Supp(\sigma_1) = Supp(\sigma) \setminus \{i_1, i_2, \ldots i_{t-1}\}.$$

Следователно σ_1 размества $k-t+1$ символа.

  - Ако $k-t+1 = 0$, то тогава $\sigma_1 = id \Rightarrow \sigma = \tau$, т.е. е от искания вид.
  - Ако $k-t+1 > 0$, то $k > k-t+1$ може да приложим индукционното предположение $\sigma_1 = \tau_1 \ldots \tau_m$ е произведение на независими цикли $\Rightarrow \sigma = \tau\sigma_1 \Rightarrow \sigma = \tau\tau_1 \ldots \tau_m$.

Единственост. Допускаме, че σ има две разлагания на произведение на независими цикли дължина по-голяма от 2:

$$\sigma = \pi_1 \ldots \pi_t = \tau_1 \ldots \tau_m.$$

Всяко число от $Supp(\sigma)$ участва в записа на някой цикъл и в двете разлагания. Нека σ размества символа i_1, т.е. $i_1 \in Supp(\sigma)$. Следователно i_1

участва в един от циклите $\pi_1 \dots \pi_t$ и $\tau_1 \dots \tau_m$. Нека това да π_1 и τ_1 (ако е необходимо след преномериране). Тогава $\pi_1 = \tau_1$ (в противен случай получаваме противоречие, защото σ е биекция). Умножаваме отляво σ с τ_1^{-1} получаваме:

$$\pi_2 \dots \pi_t = \tau_2 \dots \tau_m.$$

Аналогични разсъждения водят до факта, че $\pi_2 = \tau_2, \dots \pi_t = \tau_t, m = t$.

(c) Всеки елемент на S_n може да бъде представен като произведение на транспозиции, например по следните начини:

$$(i_1\ i_2\ \dots\ i_n) = (i_1\ i_2)\ (i_2\ i_3)\ \dots\ (i_{n-1}\ i_n)$$
$$(i_1\ i_2\ \dots\ i_n) = (i_1\ i_n)\ (i_1\ i_{n-1})\ \dots\ (i_1\ i_2)$$

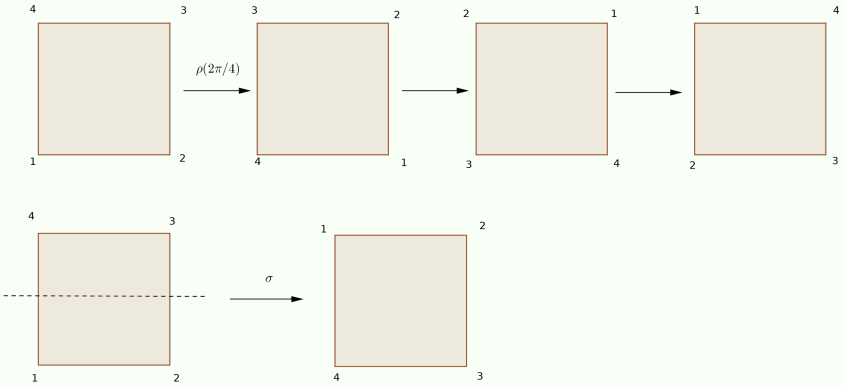
Представянето не е еднозначно, във всяко разлагане може да се добави $(ij)(ji) = e$. Например:

$$(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2) = (1\ 2)(2\ 3)(3\ 4)$$
$$(i\ j) = (1\ i)(1\ j)(1\ i).$$

□

ПРИМЕРИ:

- D_8. Всяка симетрия на квадрата, (т.е. всеки елемент от D_8) може да бъде разглеждан като функция на множеството $\{1,2,3,4\}$ от върховете на квадрата. С други думи всеки елемент от D_8 е пермутация на $\{1,2,3,4\}$, т.е. D_n подмножество на S_n.



$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$
$$a = \rho\left(\frac{2\pi}{4}\right) = (1\ 2\ 3\ 4),$$
$$a^2 = (1\ 2\ 3\ 4)(1\ 2\ 3\ 4) = (1\ 3)(2\ 4)$$
$$a^3 = (1\ 2\ 3\ 4)(1\ 2\ 3\ 4)(1\ 2\ 3\ 4) = (1\ 4\ 3\ 2)$$
$$a^4 = e$$
$$b = \sigma = (1\ 4)(2\ 3)$$
$$D_8 = \{e, a, a^2, a^3, b, ab = (2\ 4), a^2b = (1\ 2)(3\ 4), a^3b = (1\ 3)\}$$

ПРИМЕРИ:

-

Дефиниция 4.6

Пермутациите $\sigma, \tau \in S_n$ имат ***еднакъв цикличен строеж****, ако в разлаганията им в произведение на независими цикли имат един и същ брой независими цикли със (след евентуално разместване) съответно равен брой дължини.*

ПРИМЕРИ:

-

Лема 4.7

Нека $\sigma, \rho \in S_n$.

a) Ако $\sigma = (i_1\ i_2\ \ldots, i_m)$ е m-цикъл, то

$$\rho\sigma\rho^{-1} = (\rho(i_1)\ \rho(i_2)\ \ldots, \rho(i_m)).$$

b) Ако $\sigma = (i_1\ i_2\ \ldots, i_k)\ldots(j_1\ j_2\ \ldots\ j_s)$ е разлагането на σ в произведение на независими цикли, то

$$\rho\sigma\rho^{-1} = \Big(\rho(i_1)\ \rho(i_2)\ \ldots, \rho(i_k)\Big)\ \ldots\ \Big((\rho(j_1)\ \rho(j_2)\ \ldots, \rho(j_s)\Big).$$

Доказателство. a) Нека $a = \rho(i_k)$. Тогава $\rho^{-1}(a) = i_k$ следва, че

$$\sigma(\rho^{-1}(a)) = \sigma(i_k) = \begin{cases} i_{k+1}, & k < m \\ i_1, & k = m. \end{cases}$$

Следователно $\rho\sigma\rho^{-1}(a) = \rho(\sigma\rho^{-1}(a)) = \rho(i_{k+1})$ (или $\rho(i_1)$, ако $k = m$). Което означава, че $\rho\sigma\rho^{-1}$ е цъкъла, описан в лемата. Остава само да покажем, че ако a не е измежду числата $\rho(i_k)$, тогава $\rho^{-1}(a)$ не е равно на никои от i_k, което означава, че е фиксиран от σ. Така:

$$\rho\sigma\rho^{-1}(a) = \rho\rho^{-1}(a) = a.$$

Така твърдението е доказано.

b) Следва от a) и от

$$\begin{aligned}\rho\sigma\rho^{-1} &= \rho(i_1\ i_2\ \ldots, i_k)\rho^{-1}\rho(\ldots)\rho^{-1}\ldots\rho(j_1\ j_2\ \ldots\ j_s)\rho^{-1} \\ &= \Big(\rho(i_1\ i_2\ \ldots, i_k)\rho^{-1}\Big)\Big(\rho(\ldots)\rho^{-1}\Big)\ldots\Big(\rho(j_1\ j_2\ \ldots\ j_s)\rho^{-1}\Big) \\ &= \Big(\rho(i_1)\ \rho(i_2)\ \ldots, \rho(i_k)\Big)\ \ldots\ \Big((\rho(j_1)\ \rho(j_2)\ \ldots, \rho(j_s)\Big).\end{aligned}$$

□

Дефиниция 4.8: Спрегнати пермутации

*Две пермутации σ и τ се наричат **спрегнати**, ако $\tau = \rho\sigma\rho^{-1}$, за някоя пермутация $\rho \in S_n$.*

Теорема 4.9

Две субституции (пермутации) са спрегнати $\Leftrightarrow$ имат еднакъв цикличен строеж.

Доказателство. $\Rightarrow$) Нека σ и τ са спрегнати пермутации от S_n, т.е. $\tau = \rho\sigma\rho^{-1}$. От Лема 4.7 следва, че ако

$$\sigma = (i_1 \dots i_k) \dots (j_1 \dots j_k), \text{ то}$$
$$\tau = \rho\sigma\rho^{-1} = \Big(\rho(i_1) \dots \rho(i_k)\Big) \dots \Big(\rho(j_1) \dots \rho(j_k)\Big).$$

$\Leftarrow$) Нека

$$\sigma = (i_1 \dots i_k) \dots (j_1 \dots j_m),$$
$$\tau = (i'_1 \dots i'_k) \dots (j'_1 \dots j'_m),$$

са пермутации с еднакъв цикличен строеж. Да разгледаме изображението, определено по следния начин:

$$\rho = \begin{pmatrix} i_1 \dots i_k & \dots & j_1 \dots j_m & \{1 \dots n\} \setminus Supp(\sigma) \\ i'_1 \dots i'_k & \dots & j'_1 \dots j'_m & \{1 \dots n\} \setminus Supp(\tau) \end{pmatrix}.$$

То е зададено коректно, носителите на независимите цикли от разлагането на σ не се пресичат. Освен това е и биекция, защото и τ е произведение на независими цикли. Трябва само $\{1 \dots n\} \setminus Supp(\sigma)$ да се изобрази биективно върху пермутацията на числата $\{1 \dots n\} \setminus Supp(\tau)$. Тогава

$$\begin{aligned} \rho\sigma\rho^{-1} &= \rho(i_1\ i_2\ \dots, i_k) \dots (j_1\ j_2\ \dots\ j_s)\rho^{-1} \\ &= \Big(\rho(i_1)\ \rho(i_2)\ \dots, \rho(i_k)\Big)\ \dots\ \Big((\rho(j_1)\ \rho(j_2)\ \dots, \rho(j_s)\Big) \\ &= (i'_1\ i'_2\ \dots, i'_k) \dots (j'_1\ j'_2\ \dots\ j'_s) = \tau. \end{aligned}$$

С което се доказва, че ако две пермутации от S_n са с еднакъв цикличен строеж, то те са спрегнати.

□

Твърдение 4.10

Нека n е естествено число и нека $\sigma \in S_n$. Тогава редът на σ е НОК от дължините на циклите във разлагането на цикли на σ.

Доказателство. Нека $\sigma = \sigma_1 \dots \sigma_k$ е разлагането на $\sigma \in S_n$ на независими цикли и редовете на $r(\sigma_i) = r_i$, а на $r(\sigma) = r$. Циклите $\sigma_i, 1 \le i \le k$ са независими и от Теорема 4.5 а) те комутират. Тогава

$$\sigma^r = (\sigma_1 \dots \sigma_k)^r = \sigma_1^r \dots \sigma_k^r = id$$

Тъй като $\sigma_i,\ 1 \le i \le n$ са независими цикли следвателно те са определени върху непресичащи се подмножества на $\{1, 2, \dots n\}$. Тогава $\sigma_1^r \dots \sigma_k^r = id \Leftrightarrow \sigma_i^r = id,\ 1 \le i \le n$. Това се случва тогава и само тогава когато реда на всеки цикъл r_i дели r.

□

4.2 Четни и нечетни пермутации

Дефиниция 4.11: Четна (нечетна) пермутация

Нека $\sigma \in S_n$ *и*

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}.$$

Казваме, че σ *е* ***четна (нечетна) пермутация*** *(като елемент на* S_n*), ако вторият ред* $(i_1\ i_2\ \dots\ i_n)$ *на* σ *е четна (нечетна) пермутация на естествените числа от 1 до* n*.*

Броят на четните пермутации е равен на броя на нечетните и е $n!/2$. Ако в една пермутация разменим местата на 2 числа, то тя сменя четността си. Ако $\tau = (i\ j)$ е транспозиция, то τ е нечетна пермутация.

Твърдение 4.12

Нека $\sigma \in S_n$ *и* $(i\ j)$ *е транспозиция* $1 \le i < j \le n$*. Тогава пермутациите* $\sigma(i\ j)$ *и* σ *имат различни четности.*

Доказателство. Ако

$$\sigma = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ s_1 & \dots & s_i & \dots & s_j & \dots & s_n \end{pmatrix}, \text{ то}$$

$$\sigma(i\ j) = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ s_1 & \dots & s_j & \dots & s_i & \dots & s_n \end{pmatrix},$$

т.е. $\sigma(i\ j)$ се получава от σ, като във втория ред на σ си сменят местата s_i и s_j, което променя четността.

Аналогично се разглежда произведението $(i\ j)\sigma$. □

Твърдение 4.13

Една пермутация е четна $\Leftrightarrow$ *броят на множителите във всяко представяне като произведение на транспозиции е четно число.*

Доказателство. Следва от Твърдение 4.12.

□

4.3 Алтернативна група

4.4 Теорема на Кейли

Теорема 4.14: Теорема на Кейли

Всяка група от ред n е изоморфна на подгрупа на симетричната група S_n от степен n.

Доказателство. Нека G е крайна група, т.е. $|G| = n$ и да фиксираме елемент $a \in G$. Дефинираме изображението, умножение отляво с a:

$$L_a : G \to G$$
$$L_a : g \to ag$$
$$L_a(g) = ag$$

1) Ще докажем, че L_a е биекция;

   - L_a - инекция;
     Нека $g_1 \neq g_2$ и да допуснем, че $L_a(g_1) = L_a(g_2)$. Следователно
     $\Rightarrow ag_1 = ag_2 \ /.a^{-1}$ (умножаваме отляво) $\Rightarrow g_1 = g_2$, което е противоречие. От където следва, че от $g_1 \neq g_2 \Rightarrow L_a(g_1) \neq L_a(g_2)$.
   - L_a - изображение върху;
     Нека $g \in G$ е произволен елемент и $h = a^{-1}g$. Тогава

     $$L_a(h) = ah = a(a^{-1}g) = (aa^{-1})g = eg = g,$$

     т.е. всеки елемент от G си има първообраз.

   С което показахме, че L_a е биекция, т.е. $L_a \in S_G = S_n$.

2) Ще докажем, че $G' = \{L_a | a \in G\}$ е подгрупа на S_n. (Очевидно $G' \subseteq S_n$.) За целта трябва да покажем следното:

   - От $L_a, L_b \in G'$ следва ли, че $L_{ab} \in G'$. Нека $g \in G$ е произволен елемент.

     $$L_aL_b(g) = L_a(L_b(g)) = L_a(bg) = a(bg) = (ab)g = L_{ab}(g).$$

     $\Rightarrow L_aL_b = L_{ab} \in G'$.
   - Ако $L_a \in G'$, то следва ли, че $(L_a)^{-1} \in G'$. Имаме

     $$L_aL_{a^{-1}} = L_{aa^{-1}} = L_e = id,$$
     $$L_{a^{-1}}L_a = L_{a^{-1}a} = L_e = id,$$
     $$\Rightarrow (L_a)^{-1} = L_{a^{-1}} \in G'.$$

3) Ще покажем, че $G \cong G'$. Да разгледаме изображението:

$$\varphi : G \to G'$$
$$\varphi(a) = L_a.$$

Ще докажем, че φ е изоморфизъм.

- φ е хооморфизъм.

$$L_{ab} = L_a L_b \Rightarrow \varphi(ab) = \varphi(a)\varphi(b).$$

- φ е биекция:
  - φ е изображение "върху"(очевидно).
  - φ е инекция.
    Нека $a, b \in G, a \neq b$. Да допуснем, че $L_a = L_b \Rightarrow L_a(e) = L_b(e) \Rightarrow ae = be \Rightarrow a = b$, което е противоречие.

Така φ е изоморфизъм и получихме, че $G \equiv G' \leq S_n$.

□

Глава 5

Съседни класове. Теорема на Лагранж.

Дефиниция 5.1: Ляв (десен) съседен клас

Нека G е група, $H \leq G$ е подгрупа на G и $a \in G$. Множеството

$$aH = \{\ ah \mid h \in H\ \}$$

се нарича ***ляв съседен клас*** *на G относно H с представител a, а*

$$Ha = \{\ ha \mid h \in H\ \}$$

се нарича ***десен съседен клас*** *на G относно H с представител a.*

ПРИМЕРИ:

- Нека $G = S_3 = \{e, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$ и нека $H = \{e, (1\ 3)\} < G$.

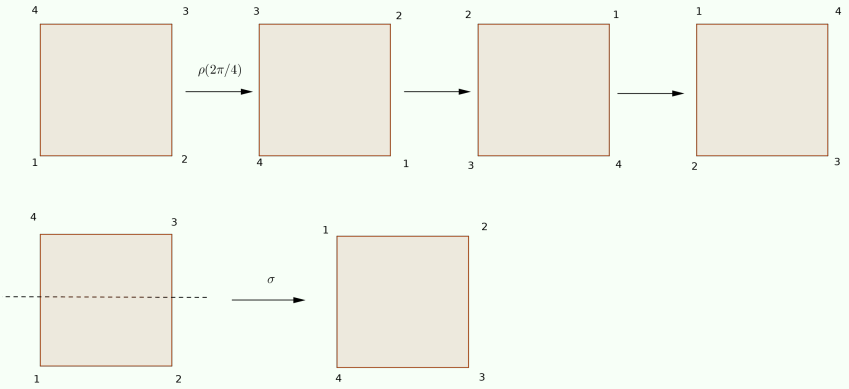
$$He = H = \{e, (1\ 3)\} = H(1\ 3)$$
$$H(1\ 2) = \{(1\ 2), (1\ 2\ 3)\} = H(1\ 2\ 3)$$
$$H(2\ 3) = \{(2\ 3), (1\ 3\ 2)\} = H(1\ 3\ 2)$$

- Нека $G = \mathbb{Z}_{12}$ $H = \{\overline{0}, \overline{4}, \overline{8}\}$

$$H = \{\overline{0}, \overline{4}, \overline{8}\}$$
$$H + \overline{1} = \{\overline{1}, \overline{5}, \overline{9}\}$$
$$H + \overline{2} = \{\overline{2}, \overline{6}, \overline{10}\}$$
$$H + \overline{3} = \{\overline{3}, \overline{7}, \overline{11}\}$$

ПРИМЕРИ:

- Нека $G = \mathbb{Z}_n$ $H = n\mathbb{Z} = \{na | a \in \mathbb{Z}\}$ $H, H + \overline{0}, \ldots, H + (n-1)$
- D_8. Всяка симетрия на квадрата, (т.е. всеки елемент от D_8) може да бъде разглеждан като функция на множеството $\{1, 2, 3, 4\}$ от върховете на квадрата. С други думи всеки елемент от D_8 е пермутация на $\{1, 2, 3, 4\}$, т.е. D_n подмножество на S_n.



$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$
$$a = \rho\left(\frac{2\pi}{4}\right) = (1\ 2\ 3\ 4),$$
$$a^2 = (1\ 2\ 3\ 4)(1\ 2\ 3\ 4) = (1\ 3)(2\ 4)$$
$$a^3 = (1\ 2\ 3\ 4)(1\ 2\ 3\ 4)(1\ 2\ 3\ 4) = (1\ 4\ 3\ 2)$$
$$a^4 = e$$
$$b = \sigma = (1\ 4)(2\ 3)$$
$$D_8 = \{e, a, a^2, a^3, b, ab = (2\ 4), a^2b = (1\ 2)(3\ 4), a^3b = (1\ 3)\}$$
$$H = \langle a \rangle = \{e, a, a^2, a^3\} < G$$
$$H = \{e, a, a^2, a^3\} = Ha = Ha^2 = Ha^3$$
$$Hb = \{b, ab, a^2b, a^3b\} = Hab = Ha^2b = Ha^3b$$

Следователно има 2 десни съседни класа на групата D_8 по подгрупата ѝ H породена от ротацията a и $D_8 = H \bigcup Hb$.

Подгрупата $H = eH = He$ е едновременно и ляв и десен съседен клас.

Освен това $a \in aH$, тъй като $a = a.e \in aH$. (Аналогично $a \in Ha, \forall a \in G$). Следователно

$$G = \bigcup_{a \in G} aH = \bigcup_{a \in G} Ha$$

Лема 5.2

Нека G е група, а H е подгрупа на G.

а) Всеки ляв съседен клас на групата G по подгупата H се поражда от всеки свой елемент, т.е. ако

$$b \in aH \Rightarrow aH = bH.$$

b) $aH = bH \Leftrightarrow a^{-1}b \in H$. (В частност $aH = H \Leftrightarrow a \in H$.)

Доказателство. а) Ако $b \in aH \Rightarrow aH = bH$.
$h \in H, H \leq H$
$\Rightarrow hH \subseteq H$ и $Hh \subseteq H$ (Защото всяко произведение на елементи от H остава в H)

Ако $b \in aH \Rightarrow b = ah$ и $a = bh^{-1}, h \in H$
$\Rightarrow bH = (ah)H = a(hH) \subseteq aH = (bh^{-1})H = b(h^{-1}H) \subseteq bH \Rightarrow aH = bH$.

b) $aH = bH \Leftrightarrow a^{-1}b \in H$.

$\Rightarrow$) $aH = bH \ /.a^{-1}$
$a^{-1}bH = H \Rightarrow a^{-1}b \in a^{-1}bH = H \Rightarrow a^{-1}b \in H$.

$\Leftarrow$) $a^{-1}b \in H \Rightarrow a^{-1}bH = H \ /.a \Rightarrow aH = bH$.

□

(Аналогично и за десни съседни класове).

Лема 5.3

Нека G е група, а H е подгрупа на G.

а) Всеки десен съседен клас на групата G по подгупата H се поражда от всеки свой елемент, т.е. ако

$$b \in Ha \Rightarrow Ha = Hb.$$

b) $Ha = Hb \Leftrightarrow ab^{-1} \in H$. (В частност $Ha = H \Leftrightarrow a \in H$.)

Лема 5.4

Два леви (десни) съседни класа на G по H или съвпадат или нямат общи елементи.

Доказателство. Нека $c \in aH \cap bH \Rightarrow aH = cH, bH = cH \Rightarrow aH = bH$. □

Лема 5.5

Нека G е група и H е подгрупа на G. Тогава $H = eH = He$ е единственият ляв (десен) съседен клас, който е подгрупа на G.

Доказателство. Нека $gH \neq H$ от Лема 5.4 следва, че gH и H или съвпадат или нямат общи елементи $\Rightarrow gH \cap H = \emptyset$. Понеже H е подгрупа $\Rightarrow e \in H$ и оттам $e \notin gH \Rightarrow gH$ не е подгрупа.

□

$G = \bigcup_{i \in I} a_i H = \bigcup_{j \in J} H b_j$, съответно ляво и дясно разлагане, т.е.

$$G = \bigcup \text{непресичащи се леви (десни) съседни класове}$$

Множеството $\{a_i | i \in I\}$ от елементи на групата G, които участат в разлагането на G, се наричат **пълна система от представители на левите съседни класове**, а множеството $\{b_j | j \in J\}$ - пълна система от представители на десните съседни класове на групата G по подгрупата H.

Лема 5.6

Ако H е подгрупа на G, то

a) всеки два съседни класа на G по H са равномощни.

b) множествата от леви и десни съседни класове на G по H са равномощни.

Доказателство. а) Да разгледаме изображението ():

$$\varphi : H \to aH$$
$$\varphi : h \to ah$$
$$\varphi(h) = ah$$

Ще докажем, че φ е биекция.

- φ - инекция;
  Нека $h_1 \neq h_2$ и да допуснем, че $\varphi(h_1) = \varphi(h_2)$. Следователно
  $\Rightarrow ah_1 = ah_2 \ / .a^{-1}$ (умножаваме отляво) $\Rightarrow h_1 = h_2$, което е противоречие.
  От където следва, че от $h_1 \neq h_2 \Rightarrow \varphi(h_1) \neq \varphi(h_2)$.
- φ - изображение върху;
  Нека $g \in aH$ е произволен елемент и $\Rightarrow g = ah$. Тогава

  $$\varphi(h) = g,$$

  т.е. всеки елемент от aH си има първообраз под действието на φ.

С което показахме, че φ е биекция.

b) Да разгледаме изображението ψ, което на всеки ляв съседен клас aH съпоставя десния съседен клас Ha^{-1}, т.е.

$$\psi : aH \to Ha^{-1}$$
$$\psi(aH) = Ha^{-1}$$

Ще докажем, че ψ е биекция.

- ψ - инекция;
  Нека $aH \neq bH$ и да допуснем, че $\psi(aH) = \psi(bH)$. Следователно $\Rightarrow \psi(aH) = Ha^{-1} = Hb^{-1} = \psi(bH)$. От Лема 5.3 b) следва, че $a^{-1}b \in H$, което според Лема 5.2 е еквивалентно на равенството $aH = bH$, което е противоречие.
- φ - изображение върху;

С което показахме, че ψ е биекция.

□

Следствие 5.7

a) Ако H е крайна подгрупа на G от ред m, то броя на елементите на всеки два съседни класа е един и същ, т.е. всеки съседен клас на G по H има m елемента,

$$|gH| = |H| = |Hg| = m.$$

b) Ако G е крайна група, то броят на левите съседни класове е равен на броя на десните съседни класове на G по H

Доказателство. Следват от Лема 5.6. □

Дефиниция 5.8: Индекс

Броя на левите(десните) съседни класове на групата G по подгрупата H се нарича ***индекс на H в G***, $|G : H|$.
Казваме, че подгрупата H има краен индекс в G, ако $|G : H|$ е крайно число, а в противен случай H има безкраен индекс в G.

ПРИМЕРИ:

- Нека $(G = \mathbb{Z}_n, +)$ и $H = n\mathbb{Z} = \{na | a \in \mathbb{Z}\} < \mathbb{Z} = G$. Тогава всички съседни класове на G по подгрупата H са

$$H, 1 + H, \ldots, (n-1) + H$$

Ако $a \in \mathbb{Z}$, то $a = nq + r, 0 \leq r < n$. Следователно

$$a + H = (nq + r) + H = r + (nq + H) = r + H,$$

защото $nq \in H$. Тези класове са различни, защото от

$$r + H = k + H, \quad 0 \leq r, k < n$$

следва, че $k - r \in H \Rightarrow n/(k-r) \Rightarrow k = r$. Следователно индекса на H в G е $|G : H| = n$.

- Нека $(G = \mathbb{C}^\star, .)$ и $U = \{x \in \mathbb{C} | |x| = 1\} < G$.
Индексът на H в G - $|G : H|$ е безкраен.
(От $aU \neq bU \Leftrightarrow a^{-1}b \notin U$, т.е $a^{-1}b \neq 1$ или $|a| \neq |b|$.
Така получихме, че множеството от левите съседни класове $\{aU | a \in G\}$ е безкрайно, защото съществуват безбройно много комплексни числа с различни модули.)

Теорема 5.9: Теорема на Лагранж

Нека G е крайна група и $H \leq G$. Тогава е изпълнено равенството

$$|G| = |H||G : H|.$$

Доказателство. Нека групата

$$G = \bigcup_{a \in G} aH$$

се разбива на непресичащи се леви (десни) съседни класове.

Броят на левите (десни) съседни класове е точно индексът на G по H, т.е. $|G : H|$.

А броят на елементите във всеки един съседен клас е равен на $|H|$. От където следва, че $|G| = |H||G : H|$. (Редът на всяка подгрупа H дели реда на G, G - крайна група).

□

Следствие 5.10

Нека G е крайна група.

a) ако $g \in G$, то $|g|/|G|$, т.е. редът на всеки елемент на една крайна група дели реда на групата.

b) ако редът на G е просто число, то G е циклична и се поражда от всеки свой неединичен елемент.

c) За всяко просто число p с точно до изоморфизъм, съществува единствена група от ред p, която е циклична.

Доказателство. a) Нека $g \in G$. Редът на g е равен на реда на цикличната подгрупа $|\langle g \rangle|$ и от Теоремата на Лагранж дели реда на групата.

b) Нека $|G| = p$ и p просто число. Ако $e \neq g \in G \Rightarrow |\langle g \rangle|/|G| \Rightarrow |\langle g \rangle| = p \Rightarrow \langle g \rangle = G$.

c) От b) следва, че всички групи от ред p са циклични и от Теорема 3.13, ако $|G| = n < \infty$, то $(G, .) \cong (\mathbb{C}_n, .)$

□

https://groupprops.subwiki.org/wiki/Abelian_group_of_prime_power_order

https://groupprops.subwiki.org/wiki/Subgroup_structure_of_symmetric_group:S3

http://www.math.ucsd.edu/~atparris/small_groups.html

http://homepages.math.uic.edu/~marker/math330/g6.pdf

https://en.wikipedia.org/wiki/List_of_small_groups

http://www.neverendingbooks.org/the-15-puzzle-groupoid-2

Глава 6

Нормални подгрупи. Факторгрупи. Теорема за хомоморфизмите при групи.

6.1 Нормални подгрупи.

Видяхме, че броя на левите съседни класове е равен на броя на десните съседни класове, или казано по друг начин множествата от леви и десни класове са равномощни. Въпросът е кога тези множества съвпадат и кога са различни? Ще дадем няколко примера:

ПРИМЕРИ:

- $G = D_8 = \langle a, b | a^4 = b^2 = 1, ba = a^3b \ (bab = a^3 = a^{-1}) \rangle = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$, a - ротация, b - симетрия.
  $H = \langle b \rangle < G, H = \{e, b\}$

Леви класове	Десни класове
$H = \{e, b\}$	$H = \{e, b\}$
$aH = \{a, ab\}$	$Ha = \{a, ba\}$
$a^2H = \{a^2, a^2b\}$	$Ha^2 = \{a^2, ba^2\}$
$a^3H = \{a^3, a^3b\}$	$Ha^3 = \{a^3, ba^3\}$

  $bab = a^3 / .b \Rightarrow b^2ab = ba^3 \Rightarrow ab = ba^3$, $a^2b = ?, a^3b = ?$ Лявото разлагане на групата G по H не съвпада с дясното разлагане.

ПРИМЕРИ:

- $G = D_8 = \langle a, b | a^4 = b^2 = 1, ba = a^3b \rangle = \langle 1, a, a^2, a^3, b, ab, a^2b, a^3b \rangle$, a - ротация, b - симетрия.

  $H = \langle a \rangle < G, H = \{e, a, a^2, a^3\}$

Леви класове	Десни класове
$H = \{e, a, a^2, a^3\}$	$H = \{e, a, a^2, a^3\}$
$bH = \{b, ba, ba^2, ba^3\}$	$Hb = \{b, ab, a^2b, a^3b\}$

  Лявото разлагане на групата G по H съвпада с дясното разлагане.

Дефиниция 6.1: Нормална подгрупа

Нека G е група и $H \leq G$. H е ***нормална подгрупа*** *на G, ако за всеки елемент $g \in G$ е изпълнено*

$$gH = Hg.$$

Означаваме $H \trianglelefteq G$ или $H \triangleleft G$.

ПРИМЕРИ:

- Тривиални нормални подгрупи $e \triangleleft G$; $G \trianglelefteq G$

  $(g\{e\} = \{g\} = \{e\}g$ и $gG = G = Gg)$.

- В абелева група всяка подгрупа е нормална.

- Центърът на G, $Z(G) \triangleleft G$.

- $G = D_8 = \langle a, b | a^4 = b^2 = 1, ba = a^3b \rangle = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$, a - ротация, b - симетрия.

  $H = \langle a \rangle < G, H = \{e, a, a^2, a^3\}$

Леви класове	Десни класове
$H = \{e, a, a^2, a^3\}$	$H = \{e, a, a^2, a^3\}$
$bH = \{b, ba, ba^2, ba^3\}$	$Hb = \{b, ab, a^2b, a^3b\}$

  Лявото разлагане на групата G по H съвпада с дясното разлагане.

Твърдение 6.2

Нека G е група, $H \leq G$ и индексът на H в G е $|G : H| = 2$. Тогава $H \triangleleft G$ е нормална подгрупа на G.

Доказателство. Нека G е група, $H \leq G$, $|G : H| = 2$ и $g \in G$.

- Ако $g \in H \Rightarrow gH = H = Hg$.
- Ако $g \in G/H \Rightarrow H \cap gH = \emptyset \Rightarrow G = H \cup gH \Rightarrow gH = G \setminus H$.
  Аналогично се получава, че $Hg = G \setminus H \Rightarrow gH = Hg \Rightarrow H \triangleleft G$.

□

Теорема 6.3

Ако $H \leq G$, то следните твърдения са еквиваленти:

(1) $H \triangleleft G$.

(2) $g^{-1}Hg = H,\ \forall g \in G$.

(3) $g^{-1}hg \in H,\ \forall g \in G,\ \forall h \in H$.

Доказателство.

- (1)⇒ (2) Ако $H \triangleleft G$, то $gH = Hg / .g^{-1}$ (отляво) $\Rightarrow H = g^{-1}Hg$.
- (2)⇒ (3) Твърдението следва от равенствата:

$$g^{-1}Hg = H, \text{ и}$$
$$g^{-1}Hg = \{g^{-1}hg \mid h \in H\}.$$

- (3) ⇒ (1)
  - Ако $g^{-1}hg \in H,\ \forall g \in G,\ \forall h \in H$, то $g^{-1}Hg \subseteq H,\ \forall g \in G$.
  - Да разгледаме елемента $g^{-1} \in G$. Тогава ще получим:

$$(g^{-1})^{-1}Hg^{-1} = gHg^{-1} \subseteq H \Rightarrow$$
$$H = g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1} \subseteq H \Rightarrow$$
$$gHg^{-1} = H \Leftrightarrow gH = Hg \Rightarrow H \triangleleft G.$$

□

Следствие 6.4

Нека $H_i \triangleleft G$, $i \in I$ са нормални подгрупи на G. Тогава сечението им е нормална подгрупа на G, т.е.

$$H_i \triangleleft G,\ i \in I \Rightarrow H = \bigcap_{i \in I} H_i \triangleleft G.$$

Доказателство. $g \in G, h \in H \Rightarrow h \in H_i (i \in I)$
$H_i \triangleleft G \Rightarrow g^{-1}hg \in H_i (\forall i \in I) \Rightarrow g^{-1}hg \in H$ от Тоерема 6.3 следва, че $H \triangleleft G$. □

Дефиниция 6.5

Два елемента $a, b \in G$ от групата G се наричат ***спрегнати****, ако*

$$\exists g \in G \ : \ b = g^{-1}ag.$$

Релацията спрегнатост е релация на еквивалентност и всички елементи на G се разбиват на класове спрегнати елементи.

$$H \leq G. H \trianglelefteq G \Leftrightarrow \text{ ако } h \in H, \text{ то и } g^{-1}hg \in H, \forall g \in G.$$

или с всеки свой елемент съдържа и всичките му спрегнати.

6.2 Факторгрупи.

Нека G е група и $H \triangleleft G$ е нормална подгрупа на G. Ще говорим само за съседни класове на G по H, защото всеки ляв съседен клас е и десен съседен клас. Да разгледаме множеството от всички съседни класове на G по H, т.е.

$$G/H = \{aH \mid a \in G\},$$

т.е. елементите на G/H са подмножества на G.

Да дефинираме бинарна операция - умножение на елементи на G/H,

$$(aH)(bH) = (ab)H,$$

като aH и bH са два произволни класа от G/H.

Теорема 6.6

Нека G е група и $H \triangleleft G$. Тогава $(G/H, .)$ е група относно операцията умножение.

Доказателство. (G1) Бинарната операция е коректно дефинирана, т.е. не зависи от избора на представител на съседния клас, т.е.

$$a_1H = aH \ \Rightarrow \ a_1^{-1}a \in H,$$
$$b_1H = bH \ \Rightarrow \ b_1^{-1}b \in H.$$

Искаме да проверим, че $(a_1b_1)H = (ab)H$, т.е. $(a_1b_1)^{-1}ab \in H$.

$$\Big(a_1b_1\Big)^{-1}ab \ = \ b_1^{-1}a_1^{-1}ab \ = \ b_1^{-1}a_1^{-1}a\Big(b_1b_1^{-1}\Big)b \ =$$

$$= \underbrace{\Big(b_1^{-1} \ \underbrace{(a_1^{-1}a)}_{\in H} \ b_1\Big)}_{\in H, \ (H \triangleleft G)} \underbrace{(b_1^{-1}b)}_{\in H}$$

Откъдето следва, че операцията е дефинирана коректно.

(G2) Асоциативност. Следва от асоциативността на G.

$$(aHbH)cH = \Big((ab)H\Big)cH = \Big((ab)c\Big)H = (abc)H$$
$$aH(bHcH) = aH\Big((bc)H\Big) = \Big(a(bc)\Big)H = (abc)H$$

(G3) Единичен елемент. Елементът $H = eH \in G/H$ е единичен елемент в G/H, защото

$$aHeH = (ae)H = aH,$$
$$eHaH = (ea)H = aH,$$

за всяко $aH \in G/H$.

(G4) Обратен елемент. Обратният елемент на $aH \in G/H$ е $a^{-1}H$, защото $a^{-1}H \in G/H$ и

$$(aH)\ (a^{-1}H) = (aa^{-1})H = eH = H,$$
$$(a^{-1}H)\ (aH) = (a^{-1}a)H = eH = H.$$

С което теоремата е доказана. □

Дефиниция 6.7: Фактор-група

Групата G/H се нарича ***фактор-група*** *на групата G по нормалната ѝ подгрупа H.*

Ако $|G| < \infty$, то $|G/H| = |G : H|$ и от Теоремата на Лагранж 5.9 се записва във вида:

$$|G| = |H|.|G/H|,$$

т.е. $G/H < \infty$ е крайна група и дели реда на G.

Ако G е абелева, то G/H също е абелева.

ПРИМЕРИ:

- $G/\{e\} \cong G, \quad G/G \cong \{e\}$.
- $G = \mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, \ldots, 11\}$ - абелева, следователно всички подгрупи са нормални.

  Нека $H = \{0, 4, 8\}$. Какво представлява групата G/H?

$$\begin{aligned} G/H &= \text{десни съседни класове на } G \text{ по } H \\ &= \{ \quad H = \{0, 4, 8\}, \\ &\qquad H + 1 = \{1, 5, 9\}, \\ &\qquad H + 2 = \{2, 6, 10\}, \\ &\qquad H + 3 = \{3, 7, 11\} \quad \} \end{aligned}$$

  $\Rightarrow G/H = \{H, H + 1, H + 2, H + 3\}$
- $G = (\mathbb{Z}, +)$,
  $H = n\mathbb{Z} = \{na | a \in \mathbb{Z}\}$
  $G/H = \{H, H + 1, , \ldots, H + (n - 1)\}$

6.3 Хомоморфизъм

Дефиниция 6.8: Хомоморфизъм на групи

Нека $(G, \star)$ и $(G', \circ)$ са групи. Казваме, че φ е ***хомоморфизъм на групи****, ако*

1) $\varphi : G \to G'$ е изображение;

2) $\forall a, b \in G$ е изпълнено:

$$\varphi(a \star b) = \varphi(a) \circ \varphi(b),$$

т.е. φ запазва груповата операция.

Ако φ е биекция, наричаме φ изоморфизъм.

Дефиниция 6.9: Ядро на хомоморфизъм

Нека φ е хомоморфизъм на групата G в G'. Тогава множеството

$$Ker(\varphi) = \{ \ a \in G \mid \varphi(a) = e' \ \} \subseteq G$$

наричаме ***ядро*** *на хомоморфизма φ.*

ПРИМЕРИ:

- Ако $n \geq 2, n \in \mathbb{N}$, тогава $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, зададено чрез $\varphi(a) = \overline{a}$ е хомоморфизъм. (Наистина $\varphi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \varphi(a) + \varphi(b)$). Следователно ядрото на φ е
$$Ker(\varphi) = \{\ a \in \mathbb{Z} \mid \overline{a} = \overline{0}\ \} = n\mathbb{Z}.$$
- Нека $G = (\mathbb{Z}, +), G' = (\mathbb{Q}^\star, .)$, тогава $\varphi : \mathbb{Z} \to \mathbb{Q}^\star$, зададено чрез $\varphi(a) = 2^a$ е хомоморфизъм. $\varphi(a+b) = 2^{a+b} = 2^a.2^b = \varphi(a).\varphi(b)$. Следователно ядрото на φ е
$$Ker(\varphi) = \{\ a \in \mathbb{Z} \mid 2^a = 1\ \} = \{0\}.$$
- Нека G и G' са групи, тогава $\varphi : G \to G'$, зададено чрез $\varphi(a) = e'$ е хомоморфизъм. $\varphi(a.b) = e = \varphi(a).\varphi(b)$. Следователно ядрото на φ е
$$Ker(\varphi) = \{\ a \in G \mid \varphi(a) = e'\ \} = G.$$

Твърдение 6.10

Нека $\varphi : G \to G'$ е хомоморфизъм на групи и $g \in G$. Тогава

(1) $\varphi(e) = e'$.

(2) $\varphi(g^n) = (\varphi(g))^n,\ n \in \mathbb{Z}$.

(3) $|g| = m < \infty \Rightarrow |\varphi(g)| / m$.

Доказателство. (1) $\varphi(e) = e'$. Да забележим, че

$$\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)\ /.\varphi(e)^{-1}$$
$$e' = \varphi(e), \quad e' \text{ е единицата в } G'$$

(2) $\varphi(g^n) = (\varphi(g))^n,\ n \in \mathbb{Z}$.

Да разгледаме случаите:

- ако $n > 0$, то
$$\varphi(g^n) = \varphi(\underbrace{gg\cdots g}_{n}) = \underbrace{\varphi(g)\cdots\varphi(g)}_{n} = \Big(\varphi(g)\Big)^n$$
- за $n = 0$ вече е доказано в (1).
- ако $n = -1$, то
$$\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e) = e'.$$

Аналогично и $\varphi(g)\varphi(g^{-1}) = e'$. Следователно $\varphi(g^{-1}) = \Big(\varphi(g)\Big)^{-1}$.

- за $n < -1$ комбинираме всичко доказано до тук.

(3) $|g| = m < \infty \Rightarrow |\varphi(g)|/m$. Имаме

$$\Big(\varphi(g)\Big)^m = \varphi(g^m) = \varphi(e) = e'.$$

Оттук и от Твърдение 3.10 следва, че реда на $\varphi(g)$ дели m. □

Лема 6.11

Нека $\varphi : G \to G'$ е хомоморфизъм на групи. Тогава $Ker(\varphi) \trianglelefteq G$ е нормална подгрупа на G.

Доказателство. $Ker(\varphi) \trianglelefteq G$.
От Твърдение 6.10 следва, че $e \in Ker(\varphi) \Rightarrow Ker\varphi \neq \emptyset$.

- $Ker(\varphi) \leq G$
  - Ако $a, b \in Ker(\varphi) \Rightarrow \varphi(ab) = \varphi(a)\varphi(b) = e'.e' = e' \Rightarrow ab \in Ker(\varphi)$.
  - Ако $a \in Ker(\varphi) \Rightarrow \varphi(a^{-1}) = \Big(\varphi(a)\Big)^{-1} = ()e')^{-1} = e' \Rightarrow a^{-1} \in Ker(\varphi)$.
- $Ker(\varphi) \trianglelefteq G \Leftrightarrow \forall g \in G, h \in Ker(\varphi)$ то и $g^{-1}hg \in Ker(\varphi)$.

$$\varphi(g^{-1}hg) = \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g^{-1})e\varphi(g) = e \Rightarrow Ker(\varphi) \trianglelefteq G.$$

□

Дефиниция 6.12: Образ на хомоморфизъм

Нека φ е хомоморфизъм на групата G в G'. Тогава множеството

$$Im(\varphi) = \{\ a' \in G' \mid \exists a \in G : \varphi(a) = a'\ \} = \{\varphi(a) \mid a \in G\} \subseteq G'$$

*наричаме **образ** на хомоморфизма φ.*

Твърдение 6.13

Нека φ е хомоморфизъм на групата G в G'. Тогава образът $Im(\varphi)$ е подгрупа на G', т.е. $Im(\varphi) \leq G'$.

Доказателство. Ако $a', b' \in Im(\varphi)$, то съществуват елементи $a, b \in G$ такива, че $\varphi(a) = a', \varphi(b) = b'$. Тогава

- $a', b' \in Im(\varphi) \Rightarrow a'b' \in Im(\varphi)$, защото

$$\varphi(ab) = \varphi(a)\varphi(b) = a'b' \in Im(\varphi)$$

- $a' \in Im(\varphi) \Rightarrow (a')^{-1} \in Im(\varphi)$, защото

$$\varphi(a^{-1}) = \Big(\varphi(a)\Big)^{-1} = (a')^{-1} \in Im(\varphi).$$

□

ПРИМЕРИ:

-
-
-

Лема 6.14

Ако $H \trianglelefteq G$ е нормална подгрупа на G, то H е ядро на някакъв хомоморфизъм на G (т.е. $H = Ker(\pi)$).

Доказателство. Да дефинираме изображението:

$$\pi : G \to G/H$$
$$\pi : g \to gH, \quad g \in G \text{ (произволен)}$$
$$\pi(g) = gH$$

- π е изображение върху;
- π е хомоморфизъм:

$$\forall a, b \in G, \quad \pi(ab) = (ab)H = (aH)(bH) = \pi(a)\pi(b)$$

- $Ker(\pi) = H$;

$$g \in G \Rightarrow g \in Ker(\pi) \Leftrightarrow \pi(g) = gH = H \Leftrightarrow g \in H.$$

π - естествен хомоморфизъм на G върху G/H.

□

Лема 6.11 и Лема 6.14 водят до следната теорема:

Теорема 6.15

Ядрата на всевъзможните хомоморфизми на дадена група се изчерпват с нейните нормални подгрупи.

Доказателство. Лема 6.11 - $\forall Ker(\varphi) \trianglelefteq G$
Лема 6.14 - $\forall H \trianglelefteq G \Rightarrow H = Ker(\pi)$ на някакъв хомоморфизъм.

□

6.4 Изоморфизъм

Целта ни е да определим кога две групи са всъщност едни и същи. Изоморфните групи имат една и съща структура. Изоморфизмът просто дава нови имена на елементите на групата. Елементите от едната група се изобразяват в елементи на другата.

Теорема 6.16

Изоморфизмът е релация на еквивалентност.

Доказателство.

- **Рефлексивност:** Нека разледаме изображението $\alpha : G \to G$, зададено чрез $\alpha(g) = g, \forall g \in G$. То е изоморфизъм. (защо?)
- **Симетричност.** Нека $\alpha : G \to G'$ е изоморфизъм, то съществува съществува изображение $\beta : G' \to G$, зададено с $\beta(g') = g$, където $\alpha(g) = g'$ и то е биекция. Трябва само да проверим, че е хомоморфизъм. Нека $a, b \in G, \alpha(a) = a', \beta(a') = a, \alpha(b) = b', \beta(b') = b$. Тогава

$$\alpha(ab) = \alpha(a)\alpha(b) = a'b'$$
$$\beta(a'b') = ab = \beta(b')\beta(a')$$

- **Транзитивност.** Нека $\alpha : G \to G'$ и $\beta : G \to G'$ са изоморфизми. Нека $\gamma = \alpha \circ \beta$. γ е биекция. Проверяваме за хомоморфизъм, $a, b \in G$:

$$\gamma(ab) = \beta\Big(\alpha(ab)\Big) = \beta\Big(\alpha(a)\alpha(b)\Big) = \beta\Big(\alpha(a)\Big)\beta\Big(\alpha(b)\Big) = \gamma(a)\gamma(b).$$

□

ПРИМЕРИ:

- Да разледаме множеството $G = \{1, -1, i, -i\}$ (където $i \in \mathbb{C}$) е група относно умножението. Ще покажем, че тя $(G, .)$ е изоморфна на $(\mathbb{Z}_4, +)$. За да докажем това, ще дефинираме изображение: $\varphi : G \to \mathbb{Z}_4$, зададено чрез

$$\varphi(0) = 1,\ \varphi(1) = i,\ \varphi(2) = -1,\ \varphi(3) = -i.$$

Това изображение е биекция и трябва да покажем, че е хомоморфизъм, т.е. че запазва груповата операция.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	3	0	1	2
3	3	0	1	2

.	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	i	1	i	-1

∘	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Таблиците за $\mathbb{Z}_4$ и G са показани на таблица 1 и 2. Но може да се забележи, че те имат таблица 3, като просто елементите са преименувани.

Твърдение 6.17

Ако G е група и $|G| = 2k, k > 1$, то в G има елемент от ред 2.

Доказателство. □

Твърдение 6.18

Ако G е група и всеки нейн елемент има от ред 2. Тогава G е абелева.

Доказателство. □

Както вече видяхме цикличните групи могат да се класифицират с точност до изоморфизъм. Ако G е циклична група и е има безкраен ред, то тя е изоморфна на $(\mathbb{Z}, +)$. Ако има краен ред n, то тя е изоморфна на $(\mathbb{C}_n, .)$. Както и ако имаме група от прост ред p, то тя е изоморфна на $(\mathbb{C}_p, .)$ (защо?).

Дефиниция 6.19

Нека $(G, \star)$ и $(H, \circ)$ са групи. За декартово произведение $G \times H$ дефинираме операция $\diamond$:

$$(g_1, h_1) \diamond (g_2, h_2) = (g_1 \star g_2, h_1 \circ h_2), \forall g_i \in G, h_i \in H, i = 1, 2.$$

*С така въведената операция наричаме $G \times H$ **директно произведение** на G и H.*

Твърдение 6.20

Директното произведение на две групи е група.

Доказателство. □

Теорема 6.21

Нека G е група, която има два различни комутиращи елемента a и b от ред 2. Тогава G има подгрупа изоморфна на $\mathbb{C}_2 \times \mathbb{C}_2$.

Доказателство. Нека $|a| = |b| = 2$. Тогава $H = \{e, a, b, ab\}$ е подгрупа на G (съдържа единица, затворена е относно операцията).

H съдържа 4 различни елемента. Ясно е, че e, a и b са различни. Ако $ab = e = bb \Rightarrow a = b$ и $ab = b = eb \Rightarrow a = e$, което е невъзможно.

Твърдим, че $H \cong \mathbb{C}_2 \times \mathbb{C}_2$. Да разгледаме изображението $\varphi : H \to \mathbb{C}_2 \times \mathbb{C}_2$, дефинирано чрез

$$\varphi(e) = (1, 1),\ \varphi(a) = (-1, 1),\ \varphi(b) = (1, -1) \text{ и } \varphi(ab) = (-1, -1).$$

Това изображение е биекция. Като сравним таблиците им (те еднозначно се попълват) се проверява, че те са еднотипни и изображението е хомоморфизъм.

□

Твърдение 6.22

Всяка група от ред 4 е изоморфна или на $\mathbb{C}_4$ или на $\mathbb{C}_2 \times \mathbb{C}_2$.

Доказателство. В група от ред 4 всеки неединичен елемент има ред 2 или 4.

- Ако има елемент от ред 4 следователно е циклична и изоморфна на $\mathbb{C}_4$.
- В противен случай, всеки неединичен елемент е от ред 2. Но това означава, че групата е абелева и от предната лема следва, че групата има подгрупа изоморфна на $\mathbb{C}_2 \times \mathbb{C}_2$. Но тази подгрупа има ред 4, колкото е реда на групата, следователно съвпадат.

□

Теорема 6.23

Нека G е група и $|G| = 2p$, където p е нечетно просто число. Тогава G е изоморфна или на $\mathbb{C}_{2p}$ или на D_{2p}.

Доказателство. Възможните редове на неединични елементи от G са 2, p и $2p$.

- Ако в G има елемент от ред $2p$, то G е циклична и е изоморфна на $\mathbb{C}_{2p}$.
- Считаме, че всеки неединичен елемент е от ред 2 или p.
  - Ако всеки елемент има ред 2, това означава, че групата е абелева и има подгрупа от ред 4, което е противоречие с теоремата на Лагранж.
  - Следователно $a \in G$ има ред p и нека разгледаме елемента $b \notin \langle a \rangle$. Да допуснем, че $|b| = p$. Тогава $\langle a \rangle \bigcap \langle b \rangle$ е подгрупа и на $\langle a \rangle$ и на $\langle b \rangle$ и от теоремата на Лагранж може да има ред 1 или p. И понеже $b \notin \langle a \rangle$ следва, че сечението има ред 1.

    Да разгледаме множеството:

    $$M = \{a^i b^j \mid 0 \leq i, j \leq p-1\} \subseteq G.$$

    Броят на елементите в M (различните) е най-много p^2. Ако два елемента от M са равни, т.е. $a^i b^j = a^k b^s \Rightarrow a^{i-k} = b^{s-j} \in \langle a \rangle \bigcap \langle b \rangle = \{e\}$, т.е всички елементи са различни и са p^2 на брой и освен това се съдържат в групата G, която има ред p, което е противоречие. Следователно $|b| = 2$.

Подгрупата $\langle a \rangle$ има индекс 2, което означава, че е нормална (защо?). Така, $b^{-1}ab \in \langle a \rangle$ и нека $b^{-1}ab = a^k$. Тогава

$$a = b^{-2}ab^2 = b^{-1}\underbrace{\left(b^{-1}ab\right)}_{a^k} b = b^{-1}a^k b = (b^{-1}ab)^k = (a^k)^k = a^{k^2}.$$

Понеже a има ред p, следователно $p/(k^2-1) = (k-1)(k+1)$. Но p е просто число, а $0 \leq k \leq p-1 \Rightarrow k = \pm 1$. Така $b^{-1}ab = a$ или $b^{-1}ab = a^{-1}$.

Нека $b^{-1}ab = a \Rightarrow ab = ba$, т.е. комутират. Да разгледаме редът на ab. Ако $(ab)^n = e \Rightarrow a^n = b^{-n} \in \langle a \rangle \bigcap \langle b \rangle = \{e\}$. Но a и b имат различни редове, който са прости числа, съответно p и 2. Така p/n и $2/n \Rightarrow 2p/n$. Следователно ab има ред $2p$, но този случай вече го изключихме.

Следователно $b^{-1}ab = a^{-1}$. И знаем всичко за тази група - $\langle a \rangle$ има индекс 2, $b \notin \langle a \rangle$ и елементите на G са a^i и $ba^i, 0 \leq i < p$. Нещо повече, знаем как да намерим произведението на два елемента:

$$a^i a^j = a^{(i+j) \ mod \ p},$$
$$ba^i a^j = ba^{(i+j) \ mod \ p},$$
$$a^i ba^j = b\left(b^{-1}a^i b\right)a^j = b\left(b^{-1}ab\right)^i a^j = b(a^{-1})^i a^j = ba^{j-i},$$
$$ba^i ba^j = b(ba^{j-i}) = a^{j-i}.$$

Готови сме да попълним таблицата за групата и всъщност се оказва, че имаме същата групова структура както и на диедралната група. Наистина нека F е някоя симетрия в D_{2p}, а $R_{\frac{2\pi}{p}}$ е ротация на ъгъл $\frac{2\pi}{p}$. Да разгледаме изображението:

$$\varphi : G \to D_{2p}$$
$$\varphi(a^i) = R_{\frac{2i\pi}{p}}$$
$$\varphi(ba^i) = FR_{\frac{2i\pi}{p}}$$

Изображението е биекция и хомоморфизъм, с което теоремата е доказана.

□

6.5 Теорема за хомоморфизмите.

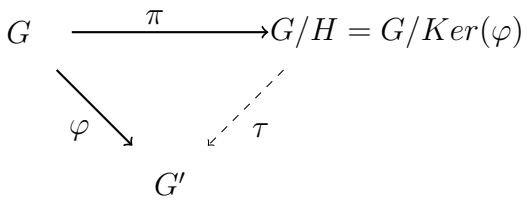
Теорема 6.24

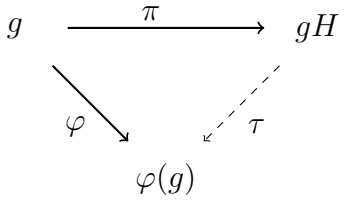
Нека $\varphi : G \to G'$ е хомоморфизъм на групи и $H = Ker(\varphi)$. Тогава

$$H \trianglelefteq G \text{ и } G/H \cong Im(\varphi).$$

Доказателство. Да разгледаме изображението:

$$\tau : G/H \to Im(G)$$
$$\tau : gH \to \varphi(g)$$
$$\tau(gH) = \varphi(g)$$





- τ е коректно дефинирано, т.е. не зависи от избора на представителя g на съседния клас gH. Нека $g_1H = gH \Rightarrow g_1 = gh, h \in H$ (за някой елемент h от H).

  Имаме $\tau(g_1H) = \varphi(g_1) = \varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)e = \varphi(g) = \tau(gH) \Rightarrow \tau$ е коректно дефинирано изображение.

- τ е изоморфизъм на групи
  - τ е изображение на G/H върху $Im(\varphi)$
  - τ е инекция

    Нека $a \neq b$ и да допуснем, че

    $$\tau(aH) = \tau(bH) \Rightarrow$$
    $$\varphi(a) = \varphi(b) \ /.\varphi(b^{-1}) \Rightarrow$$
    $$\varphi(b^{-1})\varphi(a) = e$$
    $$\varphi(b^{-1}a) = e \Rightarrow$$
    $$b^{-1}a \in H \Rightarrow bH = aH \text{ Противоречие!!!}$$
    $$\Rightarrow \tau(aH) \neq \tau(bH)$$

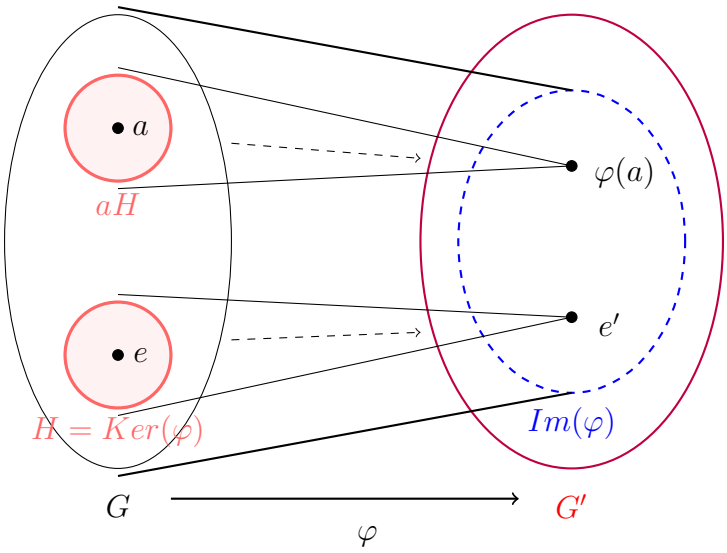
    Следователно τ е биекция.
  - τ е хомоморфизъм

    $$\tau\Big((aH)(bH)\Big) = \tau\Big((ab)H\Big) = \varphi(ab) = \varphi(a)\varphi(b) = \tau(aH)\tau(bH).$$

    τ - хомоморфизъм.

  Следователно τ е изоморфизъм.

□


a
aH
φ(a)
e
e′
H = Ker(φ)
Im(φ)
G
G′
φ

Глава 7

Действие на група върху множество. Орбити и стабилизатори. Формула за класовете на спрегнатост.

Досега разгледахме групите като множество с добре дефинирана бинарна операция. Или като структура, където много от информацията за групата може да се извлече от нейните подструктури (подгрупи), т.е. досега гледахме на групата "отвътре".

Обаче понятието за **действие на група** върху множество ще покаже, че много за групата може да се научи от това как групата си взаимодейства с "външния свят". Свойствата и структурата на групата често стават очевидни когато видим как "действа" групата. Научихме много

- за D_8 от ефекта на нейните елементи върху върховете на квадрата.
- за симетричната група S_n, която беше дефинирана като пермутации на множеството $\{1, 2, \ldots, n\}$.

Използването на действие на група е един от най-важните начини, по-които теория на групите се използва в други области на математиката. Например, теория на графите се интересува как група действа върху графи, топологията - върху повърхнини и възли, а теория на групите се интересува как група действа върху група.

Основната идея е много проста. Имаме действие на група върху множество, така че всеки елемент от групата размества (пермутира) елементите в множеството, но груповата операция се запазва.

ПРИМЕРИ:

- S_n действа върху Ω_n;
- S_n върху геометрични обекти;
- D_8 -групата от симетриите на квадрата действа върху върховете на квадрата.

Дефиниция 7.1: Действие на група върху множество

Нека G е група и Ω е множество. ***Действие на група върху множество*** *е изображение, дефинирано чрез:*

$$\begin{aligned}&\psi : G \times \Omega \to \Omega,\\ &\psi : (g, x) \to g \circ x, \quad \forall g \in G, \forall x \in \Omega\\ &\psi(g, x) = g \circ x, \ \textit{мислим като } g(x)\end{aligned}$$

което има свойствата:

(1) за всяко $x \in \Omega$ и e е единичния елемент на G е изпълнено:

$$\begin{aligned}&\psi(e, x) = x, \ \textit{или}\\ &e \circ x = x\end{aligned}$$

(2) за произволни $h, g \in G$ и $x \in \Omega$ е изпълнено:

$$\begin{aligned}&\psi\Big(h, \psi(g, x)\Big) = \psi(hg, x)\\ &h \circ (g \circ x) = (hg) \circ x.\end{aligned}$$

Ω се нарича G-множество.

ПРИМЕРИ:

- **Естественото действие на S_n върху $\Omega_n = \{1, 2 \ldots, n\}$.**

  Да разгледаме изображението:

  $$\psi(\sigma, i) = \sigma \circ i = \sigma(i), \quad \sigma \in S_n, i \in \Omega_n$$

  Изразът $\sigma(i)$ има смисъл и е елемент от Ω_n.

  (1) $id \in S_n, \forall i \in \Omega_n \Rightarrow id \circ i = id(i) = i \in \Omega_n$.

  (2) $(\sigma\tau) \circ i = (\sigma\tau)(i) = \sigma\Big(\tau(i)\Big) = \sigma \circ (\tau \circ i)$

ПРИМЕРИ:

- **Разширено действие на естественото действие на S_n.**

  $G = S_4$
  $\Omega = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$
  множеството от всички подмножества с дължина 2 на Ω_4

  Дефинираме действието на G върху Ω чрез:

  $$\sigma \circ \{a,b\} = \{\sigma(a),\sigma(b)\},\ \forall \sigma \in G, \{a,b\} \in \Omega.$$

  Така зададеното изображение е действие на група.

- **Действие на D_8 върху диагоналите на квадрата.**

  $G = D_8 = \{e,a,a^2,a^3,b,ba,ba^2,ba^3\} = \{a,b \mid a^4 = b^2 = e, bab = a^{-1} = a^3\}$
  $\Omega = \{d_1,d_2\}$

  $a \circ d_1 = d_2,\ a \circ d_2 = d_1$ и т.н.

Твърдение 7.2

Действията на група върху множество са във взаимно еднозначно съответствие с хомоморфизмите $\Phi : G \to S_M$ на G в симетричната група S_M на M. Така действието на G върху M се свежда до действието на подгрупата $\Phi(G) \leq S_M$ върху M.

7.1 Действие чрез спрягане

Дефиниция 7.3: Действие чрез спрягане

Нека G е група и множеството $\Omega \equiv G$. За $g \in G$ и $x \in \Omega$ дефинираме изображението:

$$g \circ x = gxg^{-1}$$

*Това е действие на G върху Ω и се нарича **действие чрез спрягане**. Елементът gxg^{-1} се нарича **спрегнат** на x и се означава с x^g.*

Наистина е действие:

(1) $e \circ x = exe = x$.

(2) $g \circ (h \circ x) = g \circ (hxh^{-1}) = g\left(hxh^{-1}\right)g^{-1} = ghx(gh)^{-1} = (gh) \circ x.$

Нека G е група, Ω е множество и G действа върху Ω.

Дефиниция 7.4: Стабилизатор

*Нека $x \in \Omega$. **Стабилизатор** на x в групата G наричаме множеството*

$$St_G(x) = \{g \in G \mid |g \circ x = x\}.$$

Твърдение 7.5

Стабилизаторът на всеки елемент $x \in \Omega$ е подгрупа на G, т.е.

$$St_G(x) \leq G, \ \forall x \in \Omega.$$

Доказателство. (1) $g, h \in St_G(x) \Rightarrow (gh) \circ x = g \circ (h \circ x) = g \circ x = x \Rightarrow gh \in St_G(x)$.

(2) $g \in St_G(x) \Rightarrow x = e \circ x = (g^{-1}g) \circ x = g^{-1} \circ (g \circ x) = g^{-1} \circ x \Rightarrow g^{-1} \in St_G(x)$.
$\Rightarrow St_G(x) \leq G$. □

7.2 Орбити

Дефиниция 7.6: G-еквивалентни или еквивалентни

*Нека $x, y \in \Omega$. Казваме, че x и y са **еквивалентни или G-еквивалентни** и пишем $x \sim y$, ако*

$$\exists g \in G : y = g \circ x.$$

Твърдение 7.7

Релацията G-еквививалентни е релация на еквивалентност.

Доказателство.

- Рефлексивност. $x \sim x (x = e \circ x)$
- Симетричност. $x \sim y \Rightarrow y \sim x$ $(y = g \circ x \Rightarrow x = g^{-1} \circ x, \text{ т.е. } y \sim x)$.
- Транзитивност. $x \sim y, y \sim z \Rightarrow x \sim z$

$$y = g \circ x, z = h \circ y \Rightarrow$$
$$(hg) \circ x = h \circ (g \circ x) = h \circ y = z \Rightarrow x \sim z.$$

□

Дефиниция 7.8: Орбити

Орбита на $x \in \Omega$ под действието на G наричаме:

$$O_G(x) = O(x) = G_x = \{y \in \Omega \mid \exists g \in G : g \circ x = y\} = \{g \circ x \mid g \in G\}.$$

Следствие 7.9

Множеството Ω се разбива на непресичащи се класове на еквивалентност, които се наричат G-орбити.

Доказателство. Орбитите са класове на еквивалентност следователно:

$$\Omega = O(x_1) \bigcup O(x_2) \bigcup \dots O(x_k).$$

□

Теорема 7.10

Нека Ω е G-множество. Тогава,

(1) ако $y \in O(x)$ и $y = g \circ x$, то $St_G(y) = gSt_G(x)g^{-1}$.

(2) ако $|G| < \infty$, то

$$|O(x)| = |G : St_G(x)|, \quad |O(x)|/|G|$$
$$|\Omega| = \sum_{i=1}^{k} |\Omega_i| = \sum_{i=1}^{k} |O(x_i)| = \sum_{i=1}^{k} |G : St_G(x_i)|.$$

Доказателство. (1) ако $y \in O(x) \Rightarrow g \in G,\ y = g \circ x$, то $St_G(y) = gSt_G(x)g^{-1}$.

$\subseteq$)

$$\left.\begin{array}{l} y \in O(x) \Rightarrow \exists g \in G : y = g \circ x \\ u \in St_G(y) \Rightarrow y = u \circ y \end{array}\right\} \Rightarrow \begin{array}{c} y = u \circ y = u \circ \underbrace{(g \circ x)}_{y} = (ug) \circ x \\ y = g \circ x \Rightarrow \\ g \circ x = (ug) \circ x \ / \circ g^{-1} \\ x = (g^{-1}ug) \circ x \Rightarrow \\ St_G(y) \subseteq gSt_g(x)g^{-1} \end{array}$$

$\supseteq$)

$$\left.\begin{array}{l} y \in O(x) \Rightarrow \exists g \in G : y = g \circ x \Rightarrow x = g^{-1} \circ y \\ v \in St_G(x) \Rightarrow x = v \circ x \end{array}\right\} \Rightarrow \begin{array}{c} y = g \circ x = g \circ v \circ x = \\ g \circ v \circ g^{-1} \circ y = (gvg^{-1}) \circ y \\ \Rightarrow gvg^{-1} \in St_G(y) \Rightarrow \\ gSt_g(x)g^{-1} \subseteq St_G(y) \end{array}$$

Следователно $St_G(y) = gSt_g(x)g^{-1}$.

(2) Нека $g, h \in G$. Тогава

$$h \circ x = g \circ x \Leftrightarrow (g^{-1}h) \circ x = x \Leftrightarrow g^{-1}h \in St_G(x) \Leftrightarrow gSt_G(x) = hSt_G(x).$$

Следователно броя на различните елементи в $O(x)$ съвпада с този на различните съседни класове, т.е. $|O(x)| = |G : St_G(x)|$ и от Теоремата на Лагранж следва, че $|G| = |St_G(x)||G : St_G(x)| = |St_G(x)||O(x)| \Rightarrow |O(x)|/|G|$.

Множеството Ω се разбива на непресичащи се класове на еквивалентност (G-орбити), т.е.

$$\begin{aligned}\Omega = \Omega_1 \cup \Omega_2 \cdots \cup \Omega_k = \quad & (\Omega_i \cap \Omega_j = \emptyset) \\ = O(x_1) \cup O(x_2) \cdots \cup O(x_k) & \\ = \sum_{i=1}^{k} |G : St_G(x_i)|, &\end{aligned}$$

където $x_1, x_2, \ldots, x_k$ са представители на различните орбити.

□

ПРИМЕРИ:

- $G = D_4$ действа върху $\Omega_4 = \{1,2,3,4\}$. $a = (1\ 2\ 3\ 4)$ е ротация и $b = (14)(23)$ е симетрия.

  Тогава $O(1) = \{1,2,3,4\} \Rightarrow |O(1)| = 4$, а стабилизатора на 1 е $St_G(1) = \{e, ab = (2\ 4)\}$ $|St_G(1)| = 2$.

  Нека разгледаме различни подгрупи на D_8 и да намерим орбитите и стабилизаторите на елементите (тук ще разгледаме само за 1).

  $G_1 = \langle a \rangle \Rightarrow O(1) = \{1,2,3,4\}, St_G(1) = \{e\}$.

  $G_2 = \langle b \rangle \Rightarrow O(1) = \{1,4\}, St_G(1) = \{e\}$.

  $G_3 = \langle (2\ 4) \rangle \Rightarrow O(1) = \{1\}, St_G(1) = \{e, (2\ 4)\}$.

  $G_4 = \langle (1\ 3) \rangle \Rightarrow O(1) = \{1,3\}, St_G(1) = \{e\}$.

- Нека $\Omega = \mathbb{R}^2(O)$, линейното пространство с точките в равнината и с фиксиран нулев вектор т.О и G е групата от ротациите с център т.О. Тогава орбитите $O(x)$ са концентрични окръжности с център т. О и минаващи през т. x.

- $\sigma = (1\ 3\ 5)(2\ 6) \in S_6, H = \langle \sigma \rangle \leq S_6$ действа върху $\Omega = \{1,2,\ldots,6\}$.

  Тогава множеството се разбива на непресичащи се орбити:

  $$O(1) = O(3) = O(5) = \{1,3,5\}, \quad O(2) = O(6) = \{2,6\}, \quad O(4) = \{4\}.$$

  Стабилизатора на 1 е $St_G(1) = \{e, \sigma^3\}$, а на 2 е $St_G(2) = \{e, \sigma^2, \sigma^4\}$. Това е така, σ^3 оставя неподвижен елемента 1 (както и 3 и 5), следователно пермутациите, които оставят неподвижен елемента 1 са от вида σ^{3k}. Редът на σ е 6 (защо?), следователно са само e и σ^3 са от стабилизатора на 1.

- Нека $\sigma = \pi_1 \ldots \pi_k \in S_n, H = \langle \sigma \rangle \leq S_n$ действа върху Ω_n. Ако $\sigma = (i_1\ i_2\ \ldots\ i_s) \ldots (j_1\ j_2\ \ldots\ j_t)$, то следва, че множеството се разбива на съответни орбити $O(i_1) = \{i_1, i_2, \ldots i_s\}$, $O(j_1) = \{j_1, j_2, \ldots j_t\}$ и единични орбити на елементите, които не са записани в произведението на независими цикли с дължина 1.

Дефиниция 7.11

Групата G действа транзитивно върху Ω, ако за всеки два елемента $x, y \in \Omega, \exists g \in G : y = g \circ x$.

Ако G действа транзитивно, следва че $\forall x \in \Omega \Rightarrow O(x) \equiv \Omega$, т.е. има единствена орбита.

ПРИМЕРИ:

- S_n, A_n действат транзитивно върху $\Omega_n = \{1, 2 \ldots, n\}$.

Твърдение 7.12

Ако G действа транзитивно върху $\Omega \Rightarrow |\Omega| / |G|$.

Доказателство. $\Omega = O(x), \forall x \in \Omega \Rightarrow |O(x)| = |\Omega| \Rightarrow |\Omega| / |G|$. □

Дефиниция 7.13

Нека групата G действа върху множеството $\Omega = G$ чрез спрягане и $x \in G$.
***Клас спрегнати елементи с** x наричаме*

$$O(x) = Cl_x = \{gxg^{-1} \mid g \in G\}.$$

***Централизатор** на x в G наричаме*

$$Z(x) = Z_G(x) = St_G(x) = \{g \in G \mid gxg^{-1} = x\}.$$

Тъй като $gxg^{-1} = x \Leftrightarrow gx = xg \Rightarrow Z_G(x) \leq G$ и се състои от всички елементи, които комутират с x.

$$\Rightarrow |G| = \sum_{i=1}^{s} Cl_{x_i} = \sum_{i=1}^{s} |G : Z_G(x_i)|.$$

Дефиниция 7.14: Център на G

***Център на** G наричаме*

$$Z(G) = \{x \in G \mid xg = gx, \forall g \in G\}.$$

Нека $x \in Z(G)$
$\Rightarrow xg = gx, \forall g \in G,$
$\Rightarrow gxg^{-1} = x$
$\Rightarrow Cl_x = \{gxg^{-1} \mid g \in G\} = \{x\},$

т.е. $Z(G)$ се състои от всички елементи $x \in G$, такива, че класа спрегнати елементи с x да се състои само от един елемент x, т.е. $Cl_x = \{x\}$.
Нека $Z(G) = \{x_1, x_2, \ldots, x_t\}$ следователно $|Cl_{x_i}| = 1,\ x_i \in Z(G)$. Тогава

$$|G| = \sum_{i=1}^{t} |Cl_{x_i}| + \sum_{i=t}^{k} |Cl_{x_i}| = |Z(G)| + \sum_{i=t}^{k} |Cl_{x_i}| = |Z(G)| + \sum_{i=t}^{k} |G : Z_G(x_i)| \qquad (1)$$

и се нарича **формула за класовете**.

Твърдение 7.15

Нека p е просто число, $n \in \mathbb{N}$ и $|G| = p^n$. Тогава центърът на групата е нетривиален, т.е. $Z(G) \neq \{e\}$.

Доказателство. От формулата за класовете (1) следва, че:

$$|G : Z(x_i)| \ / \ |G| \ (= p^n)$$
$$|G : Z(x_i)| > 1, \ (x_i \notin Z(G))$$
$$|G| = |Z(G)| + \sum_{i=t}^{k} |G : Z_G(x_i)|$$
$$\Rightarrow p/|Z(G)| \Rightarrow |Z(G)| > 1 \Rightarrow Z(G) \neq \{e\}.$$

□

Следствие 7.16

Ако G е крайна група от ред $|G| = p^2$, където p е просто число, то групата е абелева.

Доказателство. □

ПРИМЕРИ:

- S_3 действа на S_3 чрез спрягане. $S_3 = \{e, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$.

  За всеки елемент $x \in S_3$ трябва да намерим множеството от елементи от групата във вида gxg^{-1}.

  Ако g и x комутират, следва че $gxg^{-1} = x$, т.е. няма какво да пресмятаме. С други думи при действие спрягане елементите от централизатора на x, т.е $Z_G(x)$ не местят x (оставят го неподвижен).

  Единичният елемент остава неподвижен при това действие. Следователно $Cl_e = O(e) = \{e\}$ е един клас спрегнати елементи.

  Нека $x = (1\ 2\ 3)$. За да намерим орбитата на x трябва да пресметнем всички gxg^{-1} за всяко $g \in S_3$. Ясно е, че e, x, x^2 комутират с x, т.е. оставят го неподвижен при това действие. За другите елементи имаме:

  $$(1\ 2)x(1\ 2)^{-1} = (1\ 3\ 2), \quad (1\ 3)x(1\ 3)^{-1} = (1\ 3\ 2), \quad (2\ 3)x(2\ 3)^{-1} = (1\ 3\ 2).$$

  Можем да продължим по този начин и получаваме, че има три класа спрегнати елементи:

  $$\{e\}, \quad \{(1\ 2\ 3), (1\ 3\ 2)\}, \quad \{(1\ 2), (1\ 3), (2\ 3)\}.$$

Теорема 7.17

Броят N на елементите на S_n, които се представят като произведение на a_1 цикли с дължина 1, a_2 цикли с дължина 2, и т.н. a_n цикли с дължина n, се дава с формулата

$$N = \frac{n!}{1^{a_1}2^{a_2}\dots n^{a_n}a_1!a_2!\dots a_n!}.$$

Доказателство. Нека $\pi \in S_n$ е с исканата структура, т. е. с точност до наредба разлагането на π в произведение от независими цикли е следното:

$$\pi = \underbrace{(*)\dots(*)}_{a_1}\ \underbrace{(**)\dots(**)}_{a_2}\ \dots\ \underbrace{(*\dots*)\dots(*\dots*)}_{a_n}.$$

Общият брой на горните записи е $n!$ - толкова колкото са пермутациите на числата от 1 до n. Но всеки цикъл с дължина k има k различни записа (циклични премествания). Следователно за всеки цикъл (те са a_k на брой) с дължина k възможните записи за π се групират по k и всяка група представя една и съща субституция. Следователно $n!$ трябва да разделим на $1^{a_1}2^{a_2}\dots n^{a_n}$. Освен това, ако разместим два цикъла с дължина k субституцията π не се променя. Следователно за да получим различните π трябва да разделим $n!$ и на $a_1!a_2!\dots a_n!$. □

Теорема 7.18: Лема на Коши

Ако G е крайна група, p е просто число и $p/|G|$, то G съдържа елемент от ред p.

Доказателство. • Да разгледаме множеството:

$$M = \{(a_1, a_2, \ldots, a_p) \mid a_1 a_2 \ldots a_p = e\} \subset \underbrace{G \times G \cdots \times G}_{p}$$

Такава p-орка е еднозначно определена от първите $(p-1)$ елемента, а p-тия е обратен на произведението на $a_1 a_2 \ldots a_{p-1}$, т.е $a_p = (a_1 a_2 \ldots a_{p-1})^{-1}$. Вижда се, че тези $p-1$ елемента могат да бъдат избрани свободно от G, така $|M| = |G|^{p-1}$. Понеже $p/|G| \Rightarrow p/|M|$.

- Цикличната група от ред p, т.е. $\mathbb{C}_p$ действа върху множеството M посредством циклична пермутация (преместване надясно) на елементите.

  Нека $\sigma = (1\ 2\ \ldots\ p)$, то $\mathbb{C}_p = \langle\sigma\rangle$.

  С други думи разглеждаме изображението

  $$\psi : \mathbb{C}_p \times M \to M,$$
  $$\psi : (\tau, (a_1, a_2, \ldots, a_p)) \to \tau \circ (a_1, a_2, \ldots, a_p), \quad \forall \tau \in \mathbb{C}_p, \forall (a_1 \ldots a_p) \in M$$
  $$\psi : (\tau, (a_1, a_2, \ldots, a_p)) \to (a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(p)}), \quad \forall \tau \in \mathbb{C}_p, \forall (a_1 \ldots a_p) \in M$$

  Да разгледаме $a_1 \underbrace{(a_2 \ldots a_p)}_{a_1^{-1}} = e \Rightarrow \sigma \circ (a_1, \ldots, a_p) = (a_2, \ldots, a_p, a_1)$, т.е. е изпълнено $\underbrace{(a_2 \ldots a_p)}_{a_1^{-1}} a_1 = e$.

  Или по-общо $\underbrace{(a_1 \ldots a_i)}_{a} \underbrace{(a_{i+1} \ldots a_p)}_{b} = e$

  $\Rightarrow \sigma^i \circ (a_1, \ldots, a_p) = (a_{i+1}, \ldots, a_i)$ и е изпълнено $\underbrace{(a_{i+1} \ldots a_p)}_{b} \underbrace{(a_1 \ldots a_i)}_{a} = e$, т.е. всяка циклична пермутация на компонентите на M дава елемент на M.

  (1) $e \circ (a_1, a_2, \ldots, a_p) = (a_1, a_2, \ldots, a_p)$.

  (2) Трябва да проверим, че $h \circ (g \circ x) = (hg) \circ x$, където $h, g \in \mathbb{C}_p \Rightarrow h = \sigma^i, g = \sigma^j$.

  $$\begin{aligned} \sigma^i \circ (\sigma^j \circ (a_1, a_2, \ldots, a_p)) &= \sigma^i \circ (a_{\sigma^j(1)}, a_{\sigma^j(2)}, \ldots, a_{\sigma^j(p)}) \\ &= (a_{\sigma^i(\sigma^j(1))}, a_{\sigma^i(\sigma^j(2))}, \ldots, a_{\sigma^i(\sigma^j(p))}) \\ &= (a_{\sigma^{i+j}(1)}, a_{\sigma^{i+j}(2)}, \ldots, a_{\sigma^{i+j}(p)}). \end{aligned}$$

С това показахме, че $\mathbb{C}_p$ действа върху M.

- Групата $\mathbb{C}_p$ има ред p.

  За действие на (циклична) група от прост ред p единствените възможни мощности на орбити са 1 и p, което следва от Теорема 7.10 б) следва, че $|O(x)| = |G : St_G(x)| = |G|/|St_G(x)|$ (редът на групата в случая е p).

  Орбитата на един елемент $x \in M$ е с дължина 1, ако

$$\begin{aligned} |O(x)| = 1 \Leftrightarrow \quad & \sigma^i \circ x = x, \forall i \in 0, \ldots, p-1 \Leftrightarrow \\ & (a_1, a_2, \ldots, a_p) = (a_2, a_3, \ldots, a_p, a_1) \Leftrightarrow \\ & a_1 = a_2 = \cdots = a_p = y \Leftrightarrow \\ & y^p = e. \end{aligned}$$

  Знаем, че множеството е обединение на непресичащи се орбити и нека $x_1, \ldots, x_s$ са по един представител от всички орбити, т.е.

$$\begin{aligned} M &= O(x_1) \cup O(x_2) \cdots \cup O(x_s) \\ |M| &= \underbrace{|O(x_1)| + \cdots + |O(x_t)|}_{\text{орбити с дължина 1}} + \underbrace{|O(x_{t+1})| + \cdots + |O(x_s)|}_{\text{орбити с дължина } p}. \end{aligned}$$

$$|M| = |G|^{p-1} = t + (s-t).p$$

  Понеже $p/|M| \Rightarrow p/t$. Освен това $t \geq 1$, защото имаме поне един елемент, чиято орбита е с дължина 1 и това е единичния елемент $E = (e, \ldots, e)$. Следователно има поне още $p-1$ елемента с орбити с дължина 1. Но това са всъщност означава, че има поне $p-1$ елемента g от G, такива, че $g^p = e$, т.е. от ред p.

□

Глава 8

Пръстени – примери и основни свойства. Обратими елементи и делители на нулата. Теорема на Ойлер - Ферма и теорема на Уилсън.

Дефиниция 8.1: Пръстен

Пръстен $(R, +, .)$ *е непразно множество* R*, в което са дефинирани две бинарни операции събиране*

$$R \times R \to R, \quad (a, b) \to a + b$$

и умножение

$$R \times R \to R, \quad (a, b) \to ab,$$

такива че:

(1) $(R, +)$ *е абелева група,*

(2) умножението е асоциативно, т.е.

$$(ab)c = a(bc), \ \forall a, b, c \in R$$

(3) дистрибутивните закони за събиране и умножение са изпълнени:

$$(a + b)c = ac + bc,$$
$$c(a + b) = ca + cb.$$

Дефиниция 8.2

Ако $(R,+,.)$ е пръстен, то

- *$(R,+)$ се нарича **адитивна група** на R.*
- *неутралния елемент на $(R,+)$ се нарича **нула** и се бележи с 0 или 0_R.*
- *за всеки елемент $a \in R$, обратният се нарича **противоположен** на a и се бележи с $-a \in R$.*
- *ако в R има неутрален елемент относно умножението ще го наричаме **единичен елемент** или **единица**, бележим с 1 или 1_G.*
- *ако R е пръстен с единица, то множеството $R^\star$ на обратимите относно умножението елементи на R е група (да се докаже) и се се нарича **мултипликативна група** на R.*
- *и е изпълнено $ab = ba,\ \forall a,b \in R$, то R наричаме **комутативен пръстен**.*

Твърдение 8.3

Ако $(R,+,.)$ е пръстен с 1, то $(R^\star,.)$ е група, относно умножението дефинирано в пръстен а R.

Доказателство. Бинарната операция умножение в пръстена R е асоциативна. R е пръстен с 1, т.е. в $R^\star$ има 1.

Затворено относно умножението, т.е. произведение на обратими елементи е обратим елемент:

$$(ab)(b^{-1}a^{-1}) = 1 \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$$

За всеки елемент $u \in R^\star$ следва, че има u^{-1} и u^{-1} е също обратим $u^{-1} \in R^\star$.

□

ПРИМЕРИ:

- $R^\star$ -мултипликативната група на R.

  $\mathbb{Z}^{star} = \{-1,1\} = \mathbb{C}_2$.

  $M_n(F)^\star = GL_n(F)$ (F - поле)

ПРИМЕРИ:

- Множествата $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ са комутативни пръстени с 1 относно събиране и умножение на числа. Мултипликативната група на $\mathbb{Z}$ е $\mathbb{Z}^\star = \{\pm 1\}$, а на $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ са $\mathbb{Q}^\star = \mathbb{Q} \setminus \{0\}, \mathbb{R}^\star = \mathbb{R} \setminus \{0\}, \mathbb{C}^\star = \mathbb{C} \setminus \{0\}$.
- Множеството $\mathbb{N}$ не е пръстен (защо?).
- Множеството $(n\mathbb{Z}, +, .)$ е комутативен пръстен и при $n > 1$ няма единица.
- $Z_n = \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ - фактор група (остатъците по модул n). Въведохме събиране в това множество чрез

$$\overline{a} + \overline{b} = \overline{a+b}$$

и по подобен начин въвеждаме и умножение:

$$\overline{a}.\overline{b} = \overline{a.b}.$$

Операциите събиране и умножение в $\mathbb{Z}_n$ са коректно дефинирани. $\mathbb{Z}_n$ е комутативен пръстен с единица $\overline{1}$ и се нарича пръстен от класовете остатъци по модул n.

- Нека F е числово поле, а $F[x]$ множеството от всички полиноми на x с коефициенти от F. Тогава $F[x]$ е комутативен пръстен с 1 относно операциите събиране и умножение на полиноми.
- Нека F е числово поле, а $M_n(F)$ са квадратните матрици от ред n с елементи от полето F. Тогава $M_n(F)$ е пръстен относно събиране и умножение на матрици. При $n \geq 2, M_n(F)$ не е комутативен.

Твърдение 8.4

Нека $(R, +, .)$ е пръстен. Тогава

(1) нулевият елемент е единствен.

(2) всеки елемент $a \in R$ има единствен противоположен $-a \in R$.

(3) ако в R има единица, то тя е единствена.

(4) ако R е пръстен с единица и R има повече от два елемента, то $1 \neq 0$.

Доказателство. (1) и (2) Следват от факта, че $(R, +)$ е абелева група.

(3) Ако допуснем, че 1 и e са единици в пръстена R, то следва, че $1 = 1.e = e$.

(4) $1 = 0 \Rightarrow 0 = r.0 = r.1 = r, \ \forall r \in R \Rightarrow R = \{0\}$.

□

Дефиниция 8.5: Тривиален пръстен

Нека R. Това е комутативен пръстен с 1 и се нарича ***тривиален пръстен*** *и $0 = 1$. Но за всички други пръстени с единици, нулата е различна от единицата $0 \neq 1$.*

Твърдение 8.6

Нека $(R, +, .)$ е пръстен. Тогава

(1) $a.0 = 0.a = 0$ *за произволен елемент от R и нулата на пръстена.*

(2) $-(a+b) = (-a) + (-b)$ *и* $-(-a) = a \quad \forall a, b \in R.$

(3) $-(ab) = (-a)b = a(-b) \quad \forall a, b \in R.$

(4) $(a-b)c = ac - bc$ *и* $a(b-c) = ab - ac \quad \forall a, b, c \in R.$

Доказателство. (1) $a \in R$, $a.0 = a(0+0) = a.0 + a.0$/добавяме от двете страни $(-a.0) \Rightarrow a.0 = 0$. Аналогично и $0.a = 0$.

(2) обратния елемент на $a+b$ е $-(a+b) = (-a)+(-b)$ и обратния на $-a$ е $-(-a) = a \quad \forall a, b \in R$. Операцията събиране в R е комутативна

$$(a+b) + \Big((-a) + (-b)\Big) = (b+a) + \Big((-a) + (-b)\Big) = b + \Big(a + (-a)\Big) + (-b)$$
$$= b + 0 + (-b) = b + (-b) = 0.$$

(3) $-(ab) = (-a)b = a(-b) \quad \forall a, b \in R.$

$$0 = 0.b = \Big(a + (-a)\Big).b = ab + (-a)b \Rightarrow (-a)b = -(ab).$$

Аналогично се доказва и $-(ab) = a(-b)$. Вместо $-(ab)$ пишем $-ab$.

(4) $(a-b)c = ac - bc$ и $a(b-c) = ab - ac \quad \forall a, b, c \in R.$

$$(a-b)c = \Big(a + (-b)\Big)c = ac + (-b)c = ac + (-bc) = ac - bc.$$

По-същия начин се доказва и второто равенство.

□

Дефиниция 8.7

Нека $n \in \mathbb{N}$, R е пръстен и $a \in R$. Тогава дефинираме кратно на a

$$n.a = \underbrace{a + a + \cdots + a}_{n \text{ пъти}}, \quad (-n)a = -(na).$$

Дефиниция 8.8

Нека $n \in \mathbb{N}$, R е пръстен и $a \in R$. Тогава дефинираме степен на a

$$a^1 = a, a^n = a.a^{n-1}.$$

Ако R има единица, то дефинираме $a^0 = 1$. Ако елемента a има обратен a^{-1}, то $a^{-n} = (a^{-1})^n$.

Дефиниция 8.9

*Ненулев елемент $0 \neq a \in R$ от пръстена R се нарича **делител на нулата**, ако съществува ненулев елемент $0 \neq b \in R$, такъв че $ab = 0$ или $ba = 0$.*

Дефиниция 8.10

*Комутативен пръстен с единица, в който няма делители на нулата, се нарича **област**.*

В област от $ab = 0$ следва, че или a или b е 0.

ПРИМЕРИ:

- $\mathbb{Z}_6, \overline{2}.\overline{3} = \overline{0}, \overline{3}.\overline{4} = \overline{0}$.
- Делители на нулата в $M_n(F)$ са особените, ненулеви матрици, т.е. матриците с детерминанта 0.
- При пръстени не можем да "съкращаваме", т.е. от $ab = ac$ и $a \neq 0$ не следва, че $b = c$. В $\mathbb{Z}_{12}$ имаме $\overline{3}.\overline{1} = \overline{3}.\overline{5}$, $\overline{3} \neq 0$, $\overline{1} \neq \overline{5}$.

  Както и $\overline{5}.\overline{3} = \overline{3}$, но $\overline{5} \neq \overline{1}$.
- В област може да "съкращаваме", т.е. от $ab = ac$ и $a \neq 0$ следва, че $b = c$. Т.е. $a(b - c) = 0$ и $a \neq 0 \Rightarrow b - c = 0 \Rightarrow b = c$.

Дефиниция 8.11: Тяло

*Пръстен с единица R $(1 \neq 0)$ е **тяло**, ако мултипликативната група $(R^\star, .)$ се състои от всички ненулеви елементи на R, т.е. $(R \setminus \{0\}, .)$ е група.*
С други думи пръстен с единица R е тяло, ако всеки ненулев елемент е обратим.

Дефиниция 8.12: Поле

*Комутативно тяло е **поле**, т.е. пръстен с 1 и $(R \setminus \{0\}, .)$ е абелева група.*
С други думи, поле е комутативен пръстен с 1, в който всеки ненулев елемент е обратим.

Всяко поле е област. F - поле, $0 \neq a \in F$ и $ab = 0 \ /.a^{-1} \Rightarrow b = 0$.

Но не е вярно обратното - всяка област е поле !!! (напр. $\mathbb{Z}$).

Твърдение 8.13

Нека $(R,+,.)$ е пръстен, $a \in R$ и $m,n \in \mathbb{Z}$. Тогава

(1) $ma + na = (m+n)a$,

(2) $m(n(a)) = (mn)a$,

(3) $a^{-1} = a^{-n}$,

(4) $(a^m)^n = a^{mn}$.

В общия случай $(ab)^n \neq a^n b^n$.

Дефиниция 8.14:

Едно непразно подмножество S на пръстена R се нарича подпръстен на R, ако е затворено относно операциите събиране и умножение, т.е.

$$\text{ако } a,b \in S \Rightarrow a \pm b, ab \in S.$$

Ако S е подпръстен на R, то S съдържа нулата ($a \in S \Rightarrow 0 = a - a$), както и заедно с елемента a съдържа и $-a$ ($0, a \in S \Rightarrow 0 - a = -a \in S$).

Подпръстена S е също и пръстен относно операциите събира не и умножение, дефинирани в R. Сечение на подпръстени на R ($\bigcap S_i$) е също подпръстен на R.

Дефиниция 8.15:

Ако R е пръстен, то множеството

$$Z(R) = \{r \in R \mid za = az, \forall a \in R\}$$

се нарича ***център*** *на пръстена R.*

$Z(R)$ е комутатиен подпръстен на R.

$Z(R) = R \Leftrightarrow R$ е комутативен пръстен.

ПРИМЕРИ:

- $\mathbb{Z}_6, A = \{0,3\}, e_A = 3, B = \{0,2,4\}, e_B = 4$.
  $\mathbb{Z}_6^\star = \{1,5\}$ $(1 = e_A + e_B, 5 = 3 + 2)$.
- Поле - всяко числово поле - $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- F - числово поле, а $F(x)$ - множеството от всички рационални функции на x, т.е. частно на два полинома с коефициенти от F.
  $F(x)$ - поле относно $(+,.)$ на рационални функции.

Твърдение 8.16

Ако $n > 1, n \in \mathbb{N}$, то

(1) $|\mathbb{Z}_n^\star| = \varphi(n)$, където $\varphi(n)$ е функцията на Ойлер.

(2) $\mathbb{Z}_n$ е поле, тогава и само тогава n е просто число.

Доказателство. (1) За да докажем исканото твърдението $|\mathbb{Z}_n^\star| = \varphi(n)$ ще покажем, че ако за цялото число $a \in \mathbb{Z}$, то елементът $\overline{a} \in \mathbb{Z}_n$ е обратим тогава и само тогава, когато $(a, n) = 1$.

$\Leftarrow$) Нека $(a, n) = 1 \Rightarrow$

$$\begin{aligned} \exists u, v \in \mathbb{Z}: \quad & au + nv = 1 \\ \text{в } \mathbb{Z}_n \Rightarrow \quad & \overline{a}.\overline{u} + \overline{n}.\overline{v} = \overline{1}, \\ \text{но } \overline{n} = \overline{0} \Rightarrow & \\ \overline{a}.\overline{u} = \overline{1} \Rightarrow & \\ \overline{a} \text{ е обратим, и обратния му е } \overline{u}. & \end{aligned}$$

$\Rightarrow$) Нека $\overline{a}$ е обратим в $\mathbb{Z}_n \Rightarrow \overline{a}.\overline{u} = \overline{1}$ $(u \in \mathbb{Z})$.
Да допуснем, че $(a, n) = d > 1$ и

$$\begin{aligned} & a = a_1 d \\ & n = n_1 d, \quad 0 < n_1 < n \Rightarrow \overline{n_1} \neq \overline{0} \text{ в } \mathbb{Z}_n \\ & \overline{1} = \overline{a}.\overline{u} \ /.\overline{n_1} \\ & \overline{n_1} = \overline{n_1}.\overline{a}.\overline{u} = \overline{n_1 a u} = \overline{n_1 a_1 d u} = \overline{n a_1 u} = \\ & \overline{n}.\overline{a_1 u} = \overline{0}, \text{ Противоречие!} \end{aligned}$$

Следователно $(a, n) = 1$.

(2) $\mathbb{Z}_n$ е поле, тогава и само тогава n е просто число.

$$\begin{aligned} & \mathbb{Z}_n \text{ е поле } \Leftrightarrow \\ & \mathbb{Z}_n^\star = \mathbb{Z}_n \setminus \{0\} \Leftrightarrow \\ & |\mathbb{Z}_n^\star| = n - 1 \Leftrightarrow \\ & \varphi(n) = n - 1 \Leftrightarrow \\ & n - \text{ просто.} \end{aligned}$$

□

Теорема 8.17: Теорема на Ойлер-Ферма

Ако $n \in \mathbb{N}, r \in \mathbb{Z}$ *и* $(r, n) = 1$, *то*

$$r^{\varphi(n)} \equiv 1 \ (mod\ n).$$

В частност, ако p *е просто число и* $p \nmid r$, *то*

$$r^{p-1} \equiv 1 \ (mod\ p).$$

Доказателство. $r^{\varphi(n)} \equiv 1 \ (mod\ n)$ е еквивалентно на $\overline{r}^{\varphi(n)} = \overline{1}$ в $\mathbb{Z}_n$.
$\varphi(n)$ е реда на групата $\mathbb{Z}_n^\star$, т.е. $|\mathbb{Z}_n^\star| = \varphi(n)$. Редът на всеки елемент от групата дели реда на групата (следствие от Теоремата на Лагранж) и $\overline{r}^{\varphi(n)} = \overline{1}$.

□

Твърдение 8.18

Ако p *е просто число и* $a \in \mathbb{Z}$, *то*

$$a^p \equiv a \ (mod\ p).$$

Доказателство.

- $p/a \Rightarrow p/a^p \Rightarrow p/(a^p - a) \Leftrightarrow a^p \equiv a \ (mod\ p)$.
- $p \nmid a \Rightarrow a^{p-1} \equiv 1 \ (mod\ p)$ (от Теоремата на Ойлер-Ферма) и $a \equiv a \ (mod\ p) \Rightarrow a^p \equiv a \ (mod\ p)$.

□

Теорема 8.19: Теорема на Уилсън

Ако p *е просто число, то*

$$(p-1)! \equiv -1 \ (mod\ p).$$

Доказателство.

$$(p-1)! \equiv -1 \ (mod\ p) \Leftrightarrow \overline{1}.\overline{2}\ldots\overline{p-1} = \overline{-1} \text{ в } \mathbb{Z}_p.$$

$\overline{-1} = -\overline{1} = \overline{p-1}$.
Ако $a \in \mathbb{Z}_p$, то $a^{-1} = a \Leftrightarrow a = \overline{1}$ или $a = \overline{-1}$.
Да допуснем, че $a = a^{-1}$ и $a \neq \overline{1}, a \neq -\overline{1}$.

$$\overline{a}.\overline{a^{-1}} = (\overline{a})^2 = \overline{1}, a \neq \pm\overline{1} \Rightarrow$$
$$a^2 \equiv 1(mod\ p) \Rightarrow$$
$$p/(a^2 - 1) \Rightarrow p/(a-1) \text{ или } p/(a+1)$$
$$\text{Но } 0 < a \leq p-1 \Rightarrow a = 1 \text{ или } a = p-1.$$

Произведението $\overline{1}.\overline{2}\ldots\overline{p-1}$ се разбива на двуелементни подмножества от вида $\{a, a^{-1}\}$ и две едно елементни $\{1\}$ и $\{-1\}$. Следователно

$$\overline{1}.\overline{2}\ldots\overline{p-1} = -\overline{1} = \overline{1}.\overline{2}\ldots\overline{p-1} = \overline{-1}.$$

□

Глава 9

Характеристика на поле. Просто поле. Поле от частни.

9.1 Характеристика на поле. Просто поле.

Нека F е поле.

Дефиниция 9.1

Характеристика на поле *е най-малкото естествено число p, за което е изпълнено $p.1 = 0$. Бележим с $char\ F = p$.*
Ако такова число не съществува, то $char\ F = 0$.

ПРИМЕРИ:

- Всяко числово поле е с характеристика 0.
- Ако характеристиката на едно поле е p, то p е редът на адитивната група $(F, +)$.
- $char\mathbb{Z}_p = p$.

Твърдение 9.2

Ако F е поле, то $charF = \begin{cases} 0, \\ p, \quad p - \text{ просто число} . \end{cases}$

Доказателство. Нека F е поле с характеристика p. Да допуснем, че p не е просто

число, следователно

$$p = s.t, \quad 0 < s, t < p$$
$$p.1 = 0 \Rightarrow$$
$$(s.1)(t.1) = 0 \ /.(s.1)^{-1}(t.1)^{-1} \Rightarrow$$
$$s.1 \neq 0 \neq t.1$$
$$\Rightarrow 1 = 0 \quad \text{Противоречие!} \Rightarrow p \text{ е просто число.}$$

□

Дефиниция 9.3

Нека F е поле и K е подмножество на F съдържащо поне 2 елемента. Казваме, че K е ***подполе*** *на F, ако*

$$\forall a, b \in K \Rightarrow a \pm b, \ ab \text{ и } a^{-1}(a \neq 0) \in K.$$

Бележим $K \leq F$ или $K < F$ и казваме, че F е разширение на K.

- K е поле относно операциите дефинирани в F.
- K съдържа 0 и 1.
- $K \leq F \Rightarrow charK = charF$.
- $\bigcap K_i \leq F$, където $K_i \leq F$.

Дефиниция 9.4

Едно подполе P е просто поле, ако няма собствени (т.е. различни от P) подполета.

Твърдение 9.5

Всяко поле съдържа единствено просто подполе.

Доказателство. $\bigcap$ всички подполета на F = единственото му просто подполе. □

Твърдение 9.6

Полетата $\mathbb{Q}$ и $\mathbb{Z}_p$, p - просто число са прости полета.

Доказателство. • Нека P е единственото просто подполе на $\mathbb{Q}$.

$$\begin{aligned}\text{От } 0,1 \in P \Rightarrow & 2 = 1+1 \in P \\ & 3 = 2+1 \in P \\ & -1 = 0-1 \\ & -2 = 0-2 \\ & \dots \\ & \Rightarrow \mathbb{Z} \subseteq P \\ \text{От } m,n(n\neq 0) \in \mathbb{Z} \Rightarrow & \frac{m}{n} \in P \\ & \mathbb{Q} \subseteq P \ (P \text{ е просто поле }) \Rightarrow \mathbb{Q} = P.\end{aligned}$$

• Нека P е единственото просто подполе на $\mathbb{Z}_p$.

$$\begin{aligned}&\overline{1} \in P \Rightarrow \overline{k} = k.\overline{1} \in P \ (0 \leq k \leq p-1) \\ &\Rightarrow \mathbb{Z}_p \leq P \Rightarrow \mathbb{Z}_p \equiv P \Rightarrow \mathbb{Z}_p \text{ е просто поле.}\end{aligned}$$

□

Дефиниция 9.7: Хомоморфизъм на пръстени

Ако R, R' са пръстени и $\varphi : R \to R'$ е изображение, то φ е ***хомоморфизъм на пръстени****, ако $\forall a, b \in R$ следва, че*

$$\begin{aligned}\varphi(a+b) &= \varphi(a) + \varphi(b) \\ \varphi(ab) &= \varphi(a)\varphi(b).\end{aligned}$$

Ако φ е инекция, то φ е ***влагане****. Ако φ е биекция, то φ е* ***изоморфизъм****.*

ПРИМЕРИ:

- $\varphi : \mathbb{Z} \to \mathbb{Q},\ \varphi(z) = z\ (z \in \mathbb{Z})$.
- $\phi : \mathbb{Z} \to \mathbb{Z}_p,\ \phi(z) = \overline{z}\ (z \in \mathbb{Z})$.

Теорема 9.8

Нека P е просто поле. Тогава:

(a) ако $char\ P = 0$, то $P \cong \mathbb{Q}$.

(b) ако $char\ P = p$, то $P \cong \mathbb{Z}_p$.

Доказателство. (a) Ако $char\ P = 0$, то $P \cong \mathbb{Q}$. За всяко $n \in \mathbb{Z}, n \neq 0$, $n.1$ е обратим, защото $n.1 \neq 0$, където 1 е единицата на P.

Нека

$$P_0 = \{(m.1)(n.1)^{-1} \in P | m, n \in \mathbb{Z}\}$$

Изпълнени са следните свойства:

(1) $(m.1)(n.1)^{-1} = (k.1)(s.1)^{-1} \Leftrightarrow (m.1)(s.1) = (k.1)(n.1)$

(2) $(m.1)(n.1)^{-1} \pm (k.1)(s.1)^{-1} = \Big((ms \pm kn).1\Big)(ns.1)^{-1}$

(3) $\Big((m.1)(n.1)^{-1}\Big)\Big((k.1)(s.1)^{-1}\Big) = \Big(mk.1\Big)\Big(ns.1\Big)^{-1}$

(4) $m \neq 0,\ \Big((m.1)(n.1)^{-1}\Big)^{-1} = (n.1)(m.1)^{-1}$

От тези свойства следва:

- $P_0 \leq P$(свойства (2),(3),(4)) $\Rightarrow P_0 = P$ (P е просто поле).
- $\varphi : P_0 = P \to \mathbb{Q},\ \varphi((m.1)(n.1)^{-1}) = \frac{m}{n}$.
  Изображението е коректно дефинирано, т.е. образът на всеки елемент от P е еднозначно определен елемент на $\mathbb{Q}$ (свойство (1)).

$$\begin{aligned}
&(m.1)(n.1)^{-1} = (k.1)(s.1)^{-1} \Leftrightarrow (m.1)(s.1) = (k.1)(n.1)\\
&\varphi((m.1)(n.1)^{-1}) = \varphi((k.1)(s.1)^{-1})\\
&\frac{m}{n} = \frac{k}{s} \Leftrightarrow m.s = k.n
\end{aligned}$$

- φ - хомоморфизъм (свойство (2,3) и правилото за умножение на рационални числа).
- φ - биекция (върху, свойство (1) - различните елементи от P се изобразяват различни от $\mathbb{Q}$)

(b) ако $char\ P = p$, то $P \cong \mathbb{Z}_p$. Нека означим с

$$P_0 = \{0,\ 1,\ 2.1,\ \ldots,\ (p-1).1\} \subseteq P$$

Ако $n \in \mathbb{N}$, то

$$\begin{aligned}
&n = pq + r, \quad 0 \leq r \leq p-1,\\
&\text{то } n.1 = (pq+r).1 = (pq).1 + r.1 = q.\underbrace{(p.1)}_{=0} + r.1 = r.1 \in P_0
\end{aligned}$$

- P_0 е подпръстен на P:
  - $\forall a, b \in P_0 \Rightarrow (a \pm b).1 = r_{a\pm b}.1 \in P_0$
  - $\forall a \in P_0 \ (a \neq 0) \Rightarrow a^{-1} \in P_0$

$$\Rightarrow a^{-1} \in P : a.a^{-1} = 1$$
$$(a, p) = 1 \Rightarrow \exists u, v \in \mathbb{Z} : \ ua + vp = 1$$
$$\Rightarrow (ua + vp).1 = 1 \Rightarrow (u.1)(a.1) = 1.$$

  $\Rightarrow P_0 \leq P$ и P - просто поле следователно $P = P_0$.

- Разглеждаме $\varphi : P_0 = P \to \mathbb{Z}_p, \ \varphi(k.1) = \overline{k}, \ (k = 0, 1, \ldots, p-1)$.

  φ - биекция.

  Операциите събиране и умножение в P се извършват както и в $\mathbb{Z}_p \Rightarrow$ хомоморфизъм и следователно изоморфизъм.

  $\Rightarrow P \cong \mathbb{Z}_p$.

□

Следствие 9.9

(a) Всяко поле с характеристика 0 съдържа единствено подполе изоморфно на $\mathbb{Q}$.

(b) Всяко поле с характеристика $p > 0$ съдържа единствено подполе изоморфно на $\mathbb{Z}_p$.

9.2 Поле от частни

Полето на рационалните числа $\mathbb{Q}$ е изградено от пръстена на цели числа $\mathbb{Z}$. Рационалните числа са частно от цели числа. Можем ли да имитираме този процес и да изградим други полета, започвайки от други пръстени?

Изграждането на Q трябва да бъде малко по-фино, по-прецизно, отколкото просто да се вземе множеството от частните на цели числа. Ако множеството $\mathbb{Q}$ е само набор от частното на цели числа (при условие, че нулата не може да бъде в знаменателя), тогава $\frac{1}{2}$ и $\frac{3}{6}$ биха били два различни елемента на $\mathbb{Q}$. Очевидно, $\mathbb{Q}$ не е само набор от „дроби“ на цели числа.

Този проблем се решава чрез определяне на рационалните числа, не като дроби (частно) на цели числа, а като класове на еквивалентност на частни на цели числа. Множеството

$$\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \ldots$$

ще бъде един елемент от $\mathbb{Q}$ и ние определяме операциите събиране и умножение за тези класове на еквивалентност. Тъй като всеки клас има безкраен брой представители - за да се гарантира, че събирането и умножението на елементи от $\mathbb{Q}$ са добре дефинирани - е необходимо да се докаже, че операциите са независими от избора на представители.

Ще изградим строго рационални числа от целите числа и ще обобщим конструкцията на всички области. С други думи, започвайки с област R, ние искаме да изградим поле Q, наречено поле от частни и искаме това поле да има определени свойства. По-специално Q е поле, което съдържа копие на R, то е най-малкото такова поле и след като го конструираме, всеки елемент от него може да бъде представен като частно на два елемента от R.

Теорема 9.10

За всяка ненулева област Z съществува поле Q, в което P се влага. Всеки елемент на Q се записва във вида ab^{-1}, $b \neq 0$ (считаме, че $Z \subseteq Q$).
Всеки две такива полета са изоморфни.
Полето Q се нарича ***поле от частни*** *на Z.*

(1) Разглеждаме множеството:

$$W = \{(a,b) | a,b \in Z,\ b \neq 0\}$$

и въвеждаме релация в него:

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc.$$

Това е релация на еквивалентност, защото

- рефлексивна: $(a,b) \sim (b,a)$.
- симетрична: $(a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$.
- транзитивна: $(a,b) \sim (c,d)$ и $(c,d) \sim (e,f) \Rightarrow (a,b) \sim (e,f)$.

$$\left.\begin{array}{l} ad = bc\ /.f \\ cf = de\ /.b \end{array}\right\} \Rightarrow \left.\begin{array}{l} adf = bcf \\ bcf = bde \end{array}\right\} \Rightarrow \begin{array}{l} adf = bde/ \text{ съкращаваме на } d, d \neq 0 \\ \Rightarrow af = eb \Rightarrow (a,b) \sim (e,f) \end{array}$$

$\Rightarrow$ " $\sim$" е релация на еквивалентност и всички елементи от W се разбиват на непресичащи се класове на еквивалентност.

(2) Да означим

$$Q = \{ \text{ класовете на еквивалентност на } W\}.$$

Класът съдържащ (a,b) означаваме с $\dfrac{a}{b}$. Релацията $\sim$ означава, че два съседни класа са равни, т.е. $\dfrac{a}{b} = \dfrac{c}{d} \Leftrightarrow ad = bc$.

(3) Въвеждаме операциите събиране и умножение в Q по следния начин:

- $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$
- $\frac{a}{b}.\frac{c}{d}=\frac{ac}{bd}$

Операциите са коректно дефинирани, т.е. не зависят от избора на представител на класа на еквивалентност.
Нека $\frac{a}{b}=\frac{a_1}{b_1}$ и $\frac{c}{d}=\frac{c_1}{d_1}\Rightarrow ab_1=a_1b$ и $cd_1=c_1d$.

- Ще докажем, че $\frac{ad+bc}{bd}=\frac{a_1d_1+b_1c_1}{b_1d_1}$, т.е.
  $(ad+bc)b_1d_1=(a_1d_1+b_1c_1)bd$
  $(ab_1)(dd_1)+(cd_1)(bb_1)=(a_1b)(dd_1)+(c_1d)(bb_1)$.
- $\frac{ac}{bd}=\frac{a_1c_1}{b_1d_1}$

  $\left.\begin{array}{l}ab_1=ab_1\\cd_1=c_1d\end{array}\right\}/.\Rightarrow(ac)(b_1d_1)=(a_1c_1)(bd)\Rightarrow\frac{ac}{bd}=\frac{a_1c_1}{b_1d_1}$.

(4) $(Q,+,.)$ е поле.

- асоциативност на "+"

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{ad+bc}{bd}+\frac{e}{f}=\frac{(ad+bc)f+(bd)e}{(bd)f}=$$
$$\frac{a(df)+b(cf+de)}{b(df)}=\frac{a}{b}+\frac{cf+de}{df}=\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)$$

- комутативност на "+"

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{cb+da}{db}=\frac{c}{d}+\frac{a}{b}$$

- нулев елемент - $\frac{0}{d},\ d\neq 0$ и $\frac{0}{d}=\frac{0}{f}$

$$\frac{a}{b}+\frac{0}{d}=\frac{ad}{bd}=\frac{a}{b}$$

- противоположен елемент, всеки елемент $\frac{a}{b}\in Q$ си има обратен $-\left(\frac{a}{b}\right)=\frac{(-a)}{b}$, защото

$$\frac{a}{b}+\frac{(-a)}{b}=\frac{ab+b(-a)}{b^2}=\frac{ab+(-ab)}{b^2}=\frac{0}{b^2}$$

- асоциативност на "."

$$\left(\frac{a}{b}.\frac{c}{d}\right).\frac{e}{f} = \frac{(ac)e}{(bd)f} = \frac{a(ce)}{b(df)} = \frac{a}{b}.\left(\frac{c}{d}.\frac{e}{f}\right)$$

- комутативност на "."

$$\frac{a}{b}.\frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}.\frac{a}{b}$$

- единичен елемент - $\frac{a}{a} = \frac{b}{b} = \frac{f}{f}$за ненулеви елементи на Q

$$\frac{a}{b}.\frac{f}{f} = \frac{af}{bf} = \frac{a}{b}$$

- обратен елемент на ненулевия елемент $\frac{a}{b} \in Q, a, b \neq 0$ е $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.
- дистрибутивни закони

(5) Нека ε е фиксиран ненулев елемент на пръстена Z. Изображението

$$\varphi : Z \to Q$$
$$\varphi(a) = \frac{a\varepsilon}{\varepsilon},\ \forall a \in Z$$

е влагане.

- φ е хомомрфизъм:

$$\varphi(a) + \varphi(b) = \frac{a\varepsilon}{\varepsilon} + \frac{b\varepsilon}{\varepsilon} = \frac{a\varepsilon^2 + b\varepsilon^2}{\varepsilon^2} = \frac{(a+b)\varepsilon^2}{\varepsilon^2} = \frac{(a+b)\varepsilon}{\varepsilon} = \varphi(a+b)$$
$$\varphi(a)\varphi(b) = \left(\frac{a\varepsilon}{\varepsilon}\right).\left(\frac{b\varepsilon}{\varepsilon}\right) = \frac{ab\varepsilon^2}{\varepsilon^2} = \frac{ab\varepsilon}{\varepsilon} = \varphi(ab)$$

- влагане - различните в различни. Нека $a \neq b$ и да допуснем, че $\varphi(a) = \varphi(b)$, т.е.

$$\frac{a\varepsilon}{\varepsilon} = \frac{b\varepsilon}{\varepsilon} \Rightarrow$$
$$a\varepsilon^2 = b\varepsilon^2\ /: \varepsilon^2$$
$$\Rightarrow a = b -\ \text{противоречие !}$$

Следователно φ е влагане, т.е. Z е изоморфен на подпръстен на Q или $Z \cong Im(\varphi) \leq Q$.

(6) $Q = \{\varphi(a)\varphi(b)^{-1} \mid a, b \in Z, b \neq 0\}$

Всеки елемент от Q е от вида:

$$\frac{a}{b} = \frac{a\varepsilon^2}{b\varepsilon^2} = \left(\frac{a\varepsilon}{\varepsilon}\right).\left(\frac{\varepsilon}{b\varepsilon}\right) = \left(\frac{a\varepsilon}{\varepsilon}\right)\left(\frac{b\varepsilon}{\varepsilon}\right)^{-1} = \varphi(a)\varphi(b)^{-1}$$

Изображението φ не зависи от ε, защото от $\dfrac{a\varepsilon}{\varepsilon} = \dfrac{a\varepsilon_1}{\varepsilon_1}$ следва, че

$$\varphi(a) = \frac{a\varepsilon}{\varepsilon} = \frac{a\varepsilon_1}{\varepsilon_1}.$$

(7) Нека φ и φ_1 на областа Z са влагания, съответно:

$$\varphi : Z \to Q = \{\varphi(a)\varphi(b)^{-1} \mid a, b, b \neq 0\}$$
$$\varphi_1 : Z \to Q_1 = \{\varphi_1(a)\varphi_1(b)^{-1} \mid a, b, b \neq 0\}.$$

Тогава $Q \cong Q_1$. Изображението:

$$\psi : Q \to Q', \quad \psi\left(\frac{a}{b}\right) = \varphi_1(a)\varphi_1(b)^{-1}$$

е изоморфизъм. (Да се провери, че изображението е коректно дефинирано, хомоморфизъм и биекция).

Глава 10

Идеали и факторпръстени. Теорема за хомоморфизмите при пръстени.

10.1 Идеали. Главни идеали.

Идеалите в теорията на пръстените играят съща роля, както и нормалните подгрупи в теорията на групите.

Дефиниция 10.1

Нека R е пръстен и I е непразно подмножество на R. Казваме, че I е ***ляв (десен) идеал****, ако са изпълнени следните условия:*

(1) $a, b \in I \Rightarrow a - b \in I$,

(2) $a \in I, r \in R \Rightarrow ra \in I$ $(ar \in I)$.

Ако I е ляв (десен) идеал, то I издържа умножение умножение отляво (отдясно) с елементи от R. Ако $I \trianglelefteq R \Leftrightarrow ra, ar \in I, \forall a \in I, r \in R$.

Дефиниция 10.2

Ако I е едновременно и ляв и десен идеал, то I е ***двустранен идеал*** *или само* ***идеал*** *на R. Пишем $I \trianglelefteq R$ или $I \triangleleft R$.*

Дефиниция 10.3

Идеалът I на пръстена R се нарича ***нетривиален****, ако $I \neq \{0\}$ и $I \neq R$.*
I е ***тривиален*** *идеал, ако $I = \{0\}$ или $I = R$.*

ПРИМЕРИ:

- $\{0\} \triangleleft R, R \trianglelefteq R$
- $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ $(n \in \mathbb{N})$
- Нека R е комутативен пръстен с 1 и $a \in R$, то множеството

$$(a) = \{ar \mid r \in R\},$$

е идеал на R, съдържащ a.

- F - поле, $R = M_n(F)$.

$$I = \begin{pmatrix} a_1 & 0 & \dots & 0 \\ a_2 & 0 & \dots & 0 \\ & & \dots & \\ a_n & 0 & \dots & 0 \end{pmatrix} \text{ ляв идеал, но не е десен идеал}$$

$$J = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 0 & 0 & \dots & 0 \\ & & \dots & \\ 0 & 0 & \dots & 0 \end{pmatrix} \text{ десен идеал, но не е ляв}$$

- Всеки идеал е подпръстен, но обратното не е вярно.

$$\underbrace{\mathbb{Z} < \mathbb{Q}}_{\text{подпръстен, но не е идеал}} < \mathbb{R} < \mathbb{C}$$

- Идеалите на $\mathbb{Z}_6 = \{0, 1, \dots, 5\}$

$$\begin{aligned} (0) &= \{0\} \\ (1) &= (5) = \mathbb{Z}_6 \\ (2) &= (4) = \{0, 2, 4\} \\ (3) &= \{0, 3\}, \end{aligned}$$

$\Rightarrow \mathbb{Z}_6$ - главен идеал.

Дефиниция 10.4

Нека R е комутативен пръстен с 1 и $a \in R$. Множеството

$$(a) = \{ar \mid r \in R\}$$

е идеал и се нарича ***главен идеал, породен от елемента*** *a ($(1) = R$). Ако $A \subseteq R$, то множеството*

$$(A) = \{\sum_{i=1}^{n} a_i r_i \mid n \in \mathbb{N}, a_i \in A, r_i \in R\}$$

е ***идеал на R, породен от множеството*** *A.*

Свойства:

(1) I -идеал (ляв, десен, двустранен) на R, то $0 \in I$, ако $a, b \in I \Rightarrow -b = 0 - b \in I, a + b = a - (-b) \in I \Rightarrow I$ подгрупа на $(R, +)$. Освен това $ab \in I \Rightarrow I$ е подпръстен на R.

(2) $\bigcap_k I_k \trianglelefteq R$, където $I_k \trianglelefteq R$ са идеали (ляв/ десен /двустранен)

Доказателство. $J = \bigcap I_k$

- $x, y \in J \Rightarrow x, y \in I_k (\forall k) \Rightarrow x - y \in I_k (\forall k) \Rightarrow x - y \in J.$
- $x \in J \Rightarrow x \in I_k (\forall k) \Rightarrow ax \in I_k (\forall k) \Rightarrow ax \in J$

□

(3) Ако R е комутативен пръстен всеки ляв (десен) идеал е двустранен идеал в R.

(4) Сума на идеали $I, J \trianglelefteq R$:

$$I + J = \{i + j \mid i \in I, j \in J\} \trianglelefteq R$$

Доказателство. $r \in R, x, y \in I + J \Rightarrow$

$$\begin{aligned}
&a = x_1 + y_1,\ x_1, x_2 \in I, y_1, y_2 \in J \\
&b = x_2 + y_2 \\
&I, J \trianglelefteq R \Rightarrow \\
&rx_1, rx_2 \in I \text{ и } x_1 - x_2 \in I \\
&ry_1, ry_2 \in J \text{ и } y_1 - y_2 \in J \Rightarrow \\
&x - y = \underbrace{(x_1 - x_2)}_{\in I} + \underbrace{(y_1 - y_2)}_{\in J} \in I + J \\
&ra = \underbrace{rx_1}_{\in I} + \underbrace{ry_1}_{\in J} \in I + J \Rightarrow \\
&I + J \trianglelefteq R.
\end{aligned}$$

□

(5) Произведение:

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \mid x_i \in I, y_i \in J, 1 \leq i \leq n, n \in \mathbb{N} \right\} \trianglelefteq R$$

(6) Частно:

$$I : J = \left\{ r \in R \mid rx \in I, \forall x \in J \right\} \trianglelefteq R$$

(7) Радикал:

$$\sqrt{I} = \left\{ r \in R \mid r^n \in I, \text{ за някое цяло положително } n \right\} \trianglelefteq R$$

Твърдение 10.5

Нека R е комутативен пръстен с 1.
R е поле $\Leftrightarrow$ R няма нетриавиални идеали (т.е. различни от $\{0\}$ и R).

Доказателство. $\Rightarrow$) R - поле, т.е. всеки ненулев елемент е обратим.

$\{0\} \neq I \trianglelefteq R$ и $0 \neq a \in I \Rightarrow 1 = aa^{-1} \in I \Rightarrow R = (1) \subseteq I \Rightarrow R \equiv I$.

$\Leftarrow$) R няма нетриавиални идеали (т.е. различни от $\{0\}$ и R)

$0 \neq a \in R \Rightarrow (a) \neq (0) \Rightarrow (a) = R = (1)$

$\Rightarrow \exists a' \in R : aa'(= a'a) = 1$, т.е. a е обратим $(a^{-1} = a')$.

Следователно всеки ненулев елемент е обратим $\Rightarrow R$ е поле.

□

Твърдение 10.6

В $\mathbb{Z}$ всеки идеал е главен, т.е. $I = n\mathbb{Z}, n \in \mathbb{N}$ или $n = 0$.

Доказателство.

- Идеалите $n\mathbb{Z} \trianglelefteq \mathbb{Z}, n \in \mathbb{N}$ или $n = 0$ са главни $n\mathbb{Z} = (n)$.
- Нека $H \neq \{0\} < (\mathbb{Z}, +)$ (подгрупа).

  $(\mathbb{Z}, +)$ е (безкрайна) адитивна циклична група, следователно подгрупата ѝ H също е циклична (от Теорема 3.15), която се поражда от най-малкото $n, n \in \mathbb{N}, n \in H$, т.е.

  $$H = \langle n \rangle = \{kn \mid k \in \mathbb{Z}\} = \{nk \mid k \in \mathbb{Z}\} = (n).$$

  Следователно всяка подгрупа H на $(\mathbb{Z}, +)$ е главен идеал в $\mathbb{Z}$.

  (Така доказахме, че всяка подгрупа на H на $(\mathbb{Z}, +)$ е главен идеал в $\mathbb{Z}$. Т.е. всички идеали, подпръстени и подгрупи на $\mathbb{Z}$ са главни идеали в $\mathbb{Z}$.)

□

10.2 Прости и максимални идеали

Нека R е комутативен пръстен с 1. Някои от идеалите на комутативен пръстен са доста интересни.

Дефиниция 10.7: Прост идеал

Нека R е комутативен пръстен с 1 и $P \trianglelefteq R$ е идеал в R. Казваме, че P е ***прост идеал****, ако*

(1) $P \neq R$,

(2) и от $ab \in P \Rightarrow a \in P$ *или* $b \in P$.

Твърдение 10.8

Ако p е просто число, то $I = (p)$ е прост идеал в $\mathbb{Z}$.

Доказателство. $I \neq \mathbb{Z}$ и от $ab \in I$, то $p/ab \Rightarrow p/a$ или p/b, т.е. $a \in I$ или $b \in I$. □

Дефиниция 10.9: Максимален идеал

Нека R е комутативен пръстен с 1 и $M \trianglelefteq R$ е идеал в R. Казваме, че M е ***максимален идеал****, ако*

(1) $M \neq R$,

(2) ако $I \trianglelefteq R$ *и* $M \subseteq I \subseteq R$, *то* $I = M$ *или* $I = R$.

Твърдение 10.10

Ако p е просто число, то $I = (p)$ е максимален идеал в $\mathbb{Z}$.

Доказателство.

$$
\begin{aligned}
&J \triangleleft \mathbb{Z} \text{ и } I \subset J, \text{ то} \\
&\exists m \in J : m \notin I, \text{ т.е. } p \nmid m \Rightarrow \\
&(p, m) = 1 \Rightarrow 1 = up + vm \ (u, v \in \mathbb{Z}) \\
&p, m \in J \Rightarrow 1 \in J \Rightarrow J = \mathbb{Z}.
\end{aligned}
$$

□

Твърдение 10.11

Във всяко поле нулевият идеал е максимален.

Доказателство. Нека F е поле. Да допуснем, че $I \triangleleft F : \{0\} \subset I \Rightarrow 0 \neq a \in I$, но $aa^{-1} = 1 \in I \Rightarrow I = (1) = F$. □

Твърдение 10.12

Във всяка област нулевият идеал е прост.

Доказателство. Нека R е област и $I = \{0\} \triangleleft R$ е нулевият идеал. От $ab = 0 \Rightarrow a = 0$ или $b = 0$. Което всъщност означава, че $I \neq R$ и от $ab \in I \Rightarrow a \in I$ или $b \in I$, т.е. е прост идеал. □

Твърдение 10.13

Всеки максимален идеал в комутативен пръстен с единица е прост идеал.

Доказателство. Нека R е комутативен пръстен с единица и $I \triangleleft R$ е максимален идеал в R.

Ако $ab \in I, a \notin I$, то полагаме $J = I + (a)$. За така конструираният идеал J е ясно, че $I \subset J \triangleleft R$ и $I \neq J$, т.к. $a \in J, a \notin I$.

От факта, че I е максимален идеал следва, че $J = R$, т.е. $I + (a) = R$.

$$1 = c + ax \ /.b \quad c \in I, ax \in (a)$$
$$b = bc + abx = b\underbrace{c}_{\in I} + \underbrace{ab}_{\in I}x \ \in I$$
$$b \in I.$$

Следователно максималният идеал I е прост. □

10.3 Факторпръстен

R -пръстен, $I \trianglelefteq R$ R - абелева група относно събирането и I е нормална подгрупа на $(R, +)$. Да разгледаме факторгрупата $(R/I, +)$

$$R/I = \{a + I \mid a \in R\}$$

от съседни класове по нормалната ѝ подгрупа I с операцията "събиране", дефинирана по-следния начин за съседните класове:

$$(a + I) + (b + I) = (a + b) + I.$$

Във факторгрупата $(R/I, +)$ по аналогичен начин въвеждаме операцията "умножение":

$$(a + I).(b + I) = a.b + I.$$

Ще докажем, че с така въведете операции R/I образува пръстен.

Теорема 10.14

Нека R е пръстен и I е идеал в R. Тогава $(R/I, +, .)$ е пръстен относно вече дефинираните операции за събиране и умножение.

Доказателство. • I е нормална подгрупа на $(R,+)$ и относно операцията събиране $(R/I,+)$ е група, наречена факторгрупа (Теорема 6.6).

- Операцията умножение е дефинирана коректно, т.е. не зависи от избора на представител на съседния клас.

  Ако

  $$a+I=a_1+I \Rightarrow a-a_1\in I$$
  $$b+I=b_1+I \Rightarrow b-b_1\in I$$
  $$(a+I)(b+I)=ab+I$$
  $$(a_1+I)(b_1+I)=a_1b_1+I$$
  трябва да докажем, че $ab+I=a_1b_1+I,$ т.е. $ab-a_1b_1\in I$
  $$ab-a_1b_1=ab-a_1b+a1b-a_1b_1=\underbrace{(a-a_1)}_{\in I}b+a_1\underbrace{(b-b_1)}_{\in I}\in I (I\trianglelefteq R)$$

- Операцята умножение е асоциативна:

$$\Big[(a+I)(b+I)\Big](c+I)=(ab+I)(c+I)=(ab)c+I$$
$$(a+I)\Big[(b+I)(c+I)\Big]=(a+I)(bc+I)=a(bc)+I$$

- Дистрибутивните закони са изпълнени:

$$\Big[(a+I)\ +\ (b+I)\Big](c+I)=((a+b)+I)(c+I)=(a+b)c+I$$
$$(a+I)(c+I)+(b+I)(c+I)=(ac+I)+(bc+I)=ac+bc+I$$

  Понеже $(a+b)c=ac+bc$, то и десния дистрибутивен закон е изпълнен. Аналогично се проверява и левия дистрибутивен закон.

□

Дефиниция 10.15: Факторпръстен

Пръстенът $(R/I,+,.)$ се нарича ***факторпръстен*** *на пръстена R по идеала I.*
Ако R е пръстен с 1, то и факторпръстена R/I има единица и тя е $1+I$

$$(a+I)(1+I)=a.1+I=a+I=(1+I)(a+I).$$

Нулевият елемент на R/I е $I=0+I$.

ПРИМЕРИ:

- **Пръстен на класовете остатъци по модул** n.

  $nZ = (n)$ е главен идеал в и факторпръстена $\mathbb{Z}_n = \mathbb{Z}/(n)$ съдържа n елемента, т.е. съседните класове:

  $$0 + (n) = (n),\ 1 + (n),\ \ldots,\ n - 1 + (n).$$

  Като съседният клас $k + (n),\ (0 \leq k \leq n)$ се състои от всички цели числа, които при деление на n дават остатък k.

Нека $\varphi : R \to R'$ е хомоморфизъм на пръстени (виж Дефиниция 9.7). Ще въведем понятията ядро и образ на хомоморфизма, както и при групи.

Дефиниция 10.16

Нека $\varphi : R \to R'$ е хомоморфизъм на пръстена R в пръстена R'. Множеството

$$Ker(\varphi) = \{a \in R \mid \varphi(a) = 0\ \}$$

се нарича ***ядро на хомоморфизма*** *φ, а*

$$Im(\varphi) = \{b \in R' \mid \exists a \in R : \varphi(a) = b\}$$

се нарича ***образ на хомоморфизма*** *φ.*

Лема 10.17

Нека $\varphi : R \to R'$ е хомоморфизъм на пръстени. Тогава $Ker(\varphi) \trianglelefteq R$ е (двустранен) идеал на R.

Доказателство.

- $Ker(\varphi) \neq \emptyset$, защото $\varphi(0) = 0 \Rightarrow 0 \in Ker(\varphi)$.
- Ако

  $$a_1, a_2 \in Ker(\varphi) \Rightarrow \varphi(a_1) = \varphi(a_2) = 0$$
  $$\varphi(a_1 - a_2) = \varphi(a_1) - \varphi(a_2) = 0 \Rightarrow$$
  $$a_1 - a_2 \in I = Ker(\varphi)$$

- $\varphi(xa_1) = \varphi(x)\varphi(a_1) = \varphi(x).0 = 0 \Rightarrow xa_1 \in Ker(\varphi)$
- Аналогично $a_1 x \in Ker(\varphi)$.

Следователно $Ker(\varphi)$ е едновременно ляв и десен идеал, т.е. двустранен идеал на R.

□

Лема 10.18

Ако $I \trianglelefteq R$ е идеал на произволен пръстен R, то I е ядро на някакъв хомоморфизъм на R (т.е. $I = Ker(\pi)$).

Доказателство. Да разгледаме изображението π - естествен хомоморфизъм на R върху R/I. (Ще покажем, че $I = Ker(\pi)$.)

$$\pi : R \to R/I$$
$$\pi : r \to r + I, \quad r \in R \text{ (произволен)}$$
$$\pi(r) = r + I$$

- π е изображение върху;
- π е хомоморфизъм:

$$\forall a, b \in R, \quad \pi(a + b) = (a + b) + I = (a + I) + (b + I) = \pi(a) + \pi(b)$$
$$\forall a, b \in R, \quad \pi(ab) = (ab) + I = (a + I)(b + I) = \pi(a)\pi(b)$$

- $Ker(\pi) = \{a \in R \mid \pi(a) = I\}$, защото нулевият елемент на факторпръстена R/I е I. Но

$$\pi(a) = I \Leftrightarrow a \in I \Rightarrow Ker(\pi) = \{a \in R \mid a \in I\} = R \bigcap I = I.$$

□

Двете леми могат да бъдат обединени в една.

Теорема 10.19

Непразното подмножество I на пръстена R е ядро на някакъв хомоморфизъм на R тогава и само тогава, когато I е идеал на R.

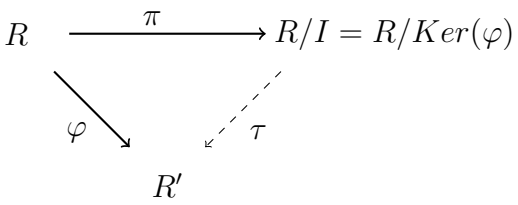
Теорема 10.20: Теорема за хомоморфизмите на пръстени

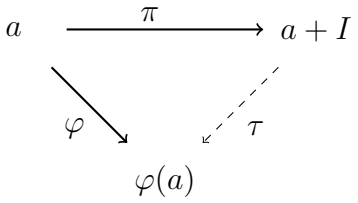
Нека $\varphi : R \to R'$ е хомоморфизъм на пръстени и $I = Ker(\varphi)$. Тогава

$$I \trianglelefteq R \text{ е идеал и } R/I \cong Im(\varphi).$$

Доказателство. От Лема 10.17 следва, че $I = Ker(\varphi)$ е идеал на R.
Да разгледаме изображението:

$$\tau : R/I \to Im(\varphi)$$
$$\tau : a + I \to \varphi(a)$$
$$\tau(a + I) = \varphi(a)$$





- τ е коректно дефинирано и е изоморфизъм на адитивните групи на пръстените R/I и $Im(\varphi)$.
- За да покажем, че τ е хомоморфизъм на пръстени трябва да проверим умножението:

$$\tau\Big((a+I)(b+I)\Big) = \tau(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \tau(a+I)\tau(b+I).$$

- Следователно τ е изоморфизъм, т.е. $R/I \cong Im(\varphi)$.

□

Теорема 10.21

Нека R е комутативен пръстен с 1. Тогава

(a) M е максимален идеал в $R \Leftrightarrow R/M$ е поле.

(b) P е прост идеал в $R \Leftrightarrow R/P$ е област.

Доказателство. (a) M е максимален идеал в $R \Leftrightarrow R/M$ е поле.

$\Leftarrow$) $M \overset{\triangleleft}{max} R$.

R е комутативен пръстен с 1, следователно и R/M е комутативен пръстен с 1. $M \neq R \Rightarrow R/M$ съдържа повече от един съседен клас. (Но $0 = 1$ ако пръстена е нулев). Така, че $0 + M \neq 1 + M$. Остава да докажем, че всеки ненулев елемент от R/M е обратим.

Нека $a + M \neq 0 + M \Rightarrow a \notin M$. Да разгледаме

$$I = M + (a) = \{m + ra \mid m \in M, r \in R\}.$$

I е сума на два идеала на R, следователно е идеал на R.

Ако $r = 0$ забелязваме, че $m \in I$ за всяко $m \in M$, следователно $M \subseteq I$. Елементът $a \in I \setminus M \Rightarrow M \subset I$. Но M е максимален идеал, следователно $I = R$.

R е комутативен пръстен с 1, следователно $1 \in I = R$. Съществуват $m \in M$ и $r \in R$ такива, че $m + ra = 1$. Но тогава

$$(r + M)(a + M) = ra + M = 1 - m + M = 1 + M, \quad (m \in M)$$

което означава, че $(r + M)$ е обратния елемент на $(a + M)$ и R/M е поле.

$\Rightarrow$) Нека R/M е поле. Трябва да покажем, че е максимален идеал.

Ако $M = R$, тогава R/M се състои само от един адитивен ляв съседен клас, но това е противоречие, с факта че в поле има два различни елемента 0 и $1 \Rightarrow M \neq R$.

Да допуснем, че I е идеал на R такъв, че $M \subset I \subset R$. Да разгледаме елемента $a \in I \setminus M$. Понеже $a + M \neq 0 + M$ следователно има обратен елемент - нека да е $b + M$. Тогава

$$(a + M)(b + M) = 1 + M.$$

Т.е. $1 = \underbrace{ab}_{\in I} + \underbrace{m}_{\in M \subset I} \in I$. Това означава, че $I = R$, което е противоречие.

(b) P е прост идеал в $R \Leftrightarrow R/P$ е област.

$\Leftarrow$) Нека P е прост идеал в R. Ще покажем, че R/P е област.

Да допуснем, че $r + P, s + P \in R/P$ и $(r + P)(s + P) = 0 + P$. Тогава

$$(r + P)(s + P) = rs + P = 0 + P \Rightarrow rs \in P.$$

Но P е прост идеал, от $rs \in P$ следва, че или $r \in P$ или $s \in P$. Т.е. или $r + P = 0 + P$ или $s + P = 0 + P$ е нулевия елемент на R/P. Заключаваме, че R/P няма делители на нулата.

От това, че $P \neq R$ следва, че R/P има повече от един елемент, т.е. не е тривиален R/P е област.

$\Rightarrow$) Нека R/P е област. Ще покажем, че P е прост.

Първо, областта има повече от един елемент, така че $P \neq R$.

Нека $ab \in P$ тогава $(a + P)(b + P) = ab + P = 0 + P$ и това означава, че $a + P = 0 + P$ или $b + P = 0 + P$. Следователно $a \in P$ или $b \in P$. Т.е. P е прост идеал.

□

Глава 11

Пръстенът на полиномите на една променлива. Теорема за деление с частно и остатък. Схема на Хорнер. Принцип за сравняване на коефициентите.

Нека A е комутативен пръстен с единица.

Да означим с B множеството :

$$B = \{(a_0, a_1, a_2, \dots) \mid a_i \in A\}$$

от всички безкрайни редици с елементи от A, в които само краен брой членове са различни от нула, наричаме ги **финитни редици**. Въвеждаме операциите събиране и умножение в множеството B по следния начин:

$$f = (a_0, a_1, a_2, \dots) \in B$$
$$g = (b_0, b_1, b_2, \dots) \in B$$
$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$$
$$fg = (c_0, c_1, c_2, \dots)$$
$$c_n = \sum_{i+j=n} a_i b_j \ (n = 0, 1, 2, \dots)$$

Например:

$$c_0 = a_0 b_0$$
$$c_1 = a_0 b_1 + a_1 b_0$$
$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0, \quad \text{и т.н.}$$

Множеството B с така въведени операции събиране и умножение се превръща в комутативен пръстен с единица - $(1, 0, 0, \dots)$.

Асоциативност:

$$f = (a_0, a_1, a_2, \dots) \in B$$
$$g = (b_0, b_1, b_2, \dots) \in B$$
$$h = (e_0, e_1, e_2, \dots) \in B$$
$$fg = (c_0, c_1, c_2, \dots), \quad c_n = \sum_{i+j=n} a_i b_j \ (n = 0, 1, 2, \dots),$$
$$gh = (d_0, d_1, d_2, \dots), \quad d_n = \sum_{i+j=n} b_i e_j \ (n = 0, 1, 2, \dots)$$
$$(fg)h = (s_0, s_1, s_2, \dots)$$
$$f(gh) = (s'_0, s'_1, s'_2, \dots)$$
$$s_m = \sum_{n+k=m} c_n e_k = \sum_{n+k=m} \left(\sum_{i+j=n} a_i b_j \right) e_k = \sum_{i+j+k=m} a_i b_j e_k$$
$$s'_m = \sum_{i+p=m} a_i d_p = \sum_{i+p=m} a_i \left(\sum_{j+k=p} b_j e_k \right) = \sum_{i+j+k=m} a_i b_j e_k$$
$$\Rightarrow s_m = s'_m, \forall m = 0, 1, 2, \dots$$
$$\Rightarrow (fg)h = f(gh).$$

Да означим с A_0 подмножество на B от редици във вида:

$$A_0 = \{(a, 0, 0, \dots) \mid a \in A\}.$$

$A_0 \leq B$ е подпръсен на B, относно операциите събиране и умножение въведени в B. Да разгледаме изображението:

$$\varphi : A \to A_0$$
$$\varphi(a) = (a, 0, 0, \dots)$$
$$\varphi \text{ - биекция}$$
$$\varphi(a + b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \varphi(a)\varphi(b)$$
$$\Rightarrow \varphi(a + b) \text{ - изоморфизъм}$$

И по-този начин считаме, че A е подпръстен на B. Вместо $(a, 0, 0, \dots)$ ще пишем a. Да означим с x редицата $(0, 1, 0, \dots)$ и от дефинираното умножение получаваме:

$$x^2 = (0, 0, 1, 0, \dots)$$
$$x^3 = (0, 0, 0, 1, 0, \dots)$$
$$\dots$$
$$x^n = (\underbrace{0, \dots, 0}_{n}, 1, 0, \dots)$$

$$\text{Ако } a \in A \Rightarrow ax^n = (\underbrace{0, \dots, 0}_{n}, a, 0, \dots)$$

Ако $f = (a_0, a_1, \dots, a_n, 0, \dots)$ е ненулева редица и a_n е последния ненулев член, то

$$f = (a_0, 0, 0 \dots) + (0, a_1, 0, \dots) + \cdots + (0, \dots, 0, a_n, 0, \dots) = \\ = a_0 + a_1 x + \cdots + a_n x^n$$

f се записва по познатия начин, както и операциите събиране и умножение се извършват познатия начин.

Дефиниция 11.1

Пръстена $B = A[x]$ се нарича ***пръстен на полиномите на една променлива x с коефициенти от A*** *или* ***полиномиален пръстен над A****, а елементите* ***полиноми****.*

Нека $f = a_0 + a_1 x + \cdots + a_n x^n$, тогава

- $a_0, a_1, \dots, a_n$ - коефициенти на f,
- a_0 - свободен член,
- a_n - старши член,
- n степен на f и пишем $n = \deg(f)$,
- f -ненулев полином, ако $\deg(f) \in \mathbb{N}$ или 0,
- ако $\deg(f) = 0 \Rightarrow f$ - константи,
- ако $f = 0$ е нулев полином, то $\deg(f) = -\infty$.

Ако f, g - полиноми, то

$$\deg(f + g) \leq max(\deg(f), \deg(g)).$$

Ако A е област, то

$$\deg(fg) = \deg(f) + \deg(g)$$

и $A[x]$ също е област.
Полиномът f ще го записваме по следния начин:

$$f = f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n.$$

Всеки полином f определя функция:

$$f : A \to A$$
$$f : a \to f(a) = a_0 a^n + a_1 a^{n-1} + \cdots + a_{n-1} a + a_n.$$
$f(a)$ - стойност на f при $x = a$.

Ако f, g са полиноми, то

$$(f+g)(a) = f(a) + g(a)$$
$$(fg)(a) = f(a)g(a)$$

Два полинома съвпадат $f = g$, ако определените от тях функции съвпадат. Обратното в общия случай не е вярно.

ПРИМЕРИ:

- $f(x) = x^p \in \mathbb{Z}_p$
  $g(x) = x \in \mathbb{Z}_p$
  $a^p = a,\ \forall a \in \mathbb{Z}_p \Rightarrow f(a) = g(a)$
  $\Rightarrow$ функциите $f : \mathbb{Z}_p \to \mathbb{Z}_p, g : \mathbb{Z}_p \to \mathbb{Z}_p$ съвпадат,
  но полиномите $f(x)$ и $g(x)$ са различни.

- Полиномите $f = x^3 + x + 1$ и $g = x^5 + x^3 + 1$ в $\mathbb{Z}_5$ като функции съвпадат $f(x) = g(x),\ \forall x \in \mathbb{Z}_5$, но всъщност са различни полиноми.

Теорема 11.2: Теорема за деление с остатък

Нека F е поле и $f, g \in F[x]$. Тогава съществува единствена двойка полиноми q и $r \in F[x]$ такива, че

$$f = gq + r \text{ и } \deg(r) < deg(g)$$

(т.е делим f на g с частно q и остатък r).

Доказателство. • (**Съществуване**)

Нека

$$f = a_0x^n + \cdots + a_n$$
$$g = b_0x^m + \cdots + b_n$$

Ако полиномът $g = b_0$ е константа, то е ясно. Считаме, че $\deg(g) = m > 0$. Индукция по n.

- Ако $\deg(g) > \deg(f)$ полагаме $q = 0, r = f$.
- Ако f е константа, то $q = 0, r = f$ (същото).
- Нека $\deg(f) \geq \deg(g)$
  Да разгледаме полинома $a_0b_0^{-1}x^{n-m}g$, старшият му член е a_0x^n. Тогава полиномът
  $$f_1 = f - a_0b_0^{-1}x^{n-m}g$$

е от степен по-малка от n, т.е. $\deg(f_1) < \deg(f)$. Приламе индукционно предположение, т.е. съществуват полиноми $q_1, r_1 \in F[x]$:

$$f_1 = gq_1 + r_1, \quad \deg(r_1) < \deg(g).$$

Следователно

$$\begin{aligned} f &= f_1 + a_0 b_0^{-1} x^{n-m} g = \\ &= gq_1 + r_1 + a_0 b_0^{-1} x^{n-m} g = \\ &= g \underbrace{(q_1 + a_0 b_0^{-1} x^{n-m})}_{q} + \underbrace{r_1}_{r} \\ f &= gq + r, \quad \deg(r) < \deg(g). \end{aligned}$$

- (**Единственост**)

Нека $f = gq + r = gq_1 + r_1, \quad \deg(r), \deg(r_1) < \deg(g)$
$\Rightarrow g(q - q_1) = r_1 - r,$
ако $q \neq q_1 \Rightarrow \deg(g(q - q_1)) = \deg(g) + \deg(q - q_1) \geq \deg(g)$ - противоречие!
$\Rightarrow q = q_1 \Rightarrow r = r_1.$

□

Доказателството на Теорема за деление с чатно и остатък (съществуване) ни дава и практически алгоритъм за намиране на полиномите q и r ($f = gq + r$, $\deg(r) < \deg(g)$).

$$\begin{aligned} & & f_1 &= f - a_0 b_0^{-1} x^{n-m} g = c_0 x^k + \cdots + c_k, \\ \text{ако } & \deg(f_1) \geq \deg(g), & f_2 &= f_1 - c_0 b_0^{-1} x^{k-m} g = d_0 x^k + \cdots + d_k, \\ & & \cdots & \\ & & & \text{и така нататък докато получим} \\ & \deg(f_p) < \deg(g), & r &= f_p, \quad q = a_0 b_0^{-1} x^{n-m} + c_0 b_0^{-1} x^{k-m} + \ldots \end{aligned}$$

Полученият алгоритъм е в сила и ако F не е поле, достатъчно е само b_0 да е обратим в F или 1.
Ако F не е област, то представянето

$$f = gq + r, \ \deg(r) < \deg(g)$$

не е единствено.

ПРИМЕРИ:

$$
\begin{aligned}
f &= \overline{3}x^3 \in \mathbb{Z}_6[x] \\
g &= \overline{3}x^2 - \overline{1} \in \mathbb{Z}_6[x] \\
f = \overline{3}x^3 &= (\overline{3}x^2 - \overline{1})(x + \overline{2}) + \overline{3}x + \overline{3} = g(x + \overline{2}) + \overline{3}x + \overline{3} \\
&= (\overline{3}x^2 - \overline{1})(x + \overline{4}) + x + \overline{4} = g(x + \overline{4}) + x + \overline{4}
\end{aligned}
$$

11.1 Схема на Хорнер

$$
\begin{aligned}
&f = a_0x^n + \cdots + a_n \in F[x] \\
&g = x - \alpha \in F[x] \\
&f = gq + r,\ \deg(r) < \deg(g),\ r \in F \\
&q = b_0x^{n-1} + \cdots + b_{n-1}
\end{aligned}
$$

$$
\begin{aligned}
f &= a_0x^n + \cdots + a_n = (x - \alpha)(b_0x^{n-1} + \cdots + b_{n-1}) + r \\
&= b_0x^n + (b_1 - \alpha b_0)x^{n-1} + (b_2 - \alpha b_1)x^{n-2} \cdots + \\
a_0 &= b_0 \\
b_1 &= a_1 + \alpha b_0 \\
b_2 &= a_2 + \alpha b_1 \\
&\cdots \\
b_{n-1} &= a_{n-2} + \alpha b_{n-2} \\
r &= f(\alpha) = a_n + \alpha b_{n-1}.
\end{aligned}
$$

	a_0	a_1	$\ldots$	a_n
α	$\underbrace{a_0}_{b_0}$	$\underbrace{a_1 + \alpha b_0}_{b_1}$	$\ldots$	$\underbrace{a_n + \alpha b_{n-1}}_{r}$

Пример:

ПРИМЕРИ:

$f = 2x^3 - 6x^2 + 2x - 1, \quad \alpha = 3$

	2	−6	2	1
3	2	0	2	5

$f = (x - 3)(2x^2 + 2) + 5$

Твърдение 11.3

Ако F е поле, то всеки идеал I в пръстена $F[x]$ е главен.

Доказателство.

- Ако $I = \{0\}$, то I е главен идеал.
- Нека $I \neq \{0\}$ и g е ненулев полином с най-ниска степен от I. Ще докажем, че $I = (g)$.
  - $(g) \subseteq I$ - очевидно.
  - Обратното включване. Нека $f \in I$ и $f = gq + r,\ \deg(r) < \deg(g) \Rightarrow r = f - gq \in I$. Ако допуснем, че $r \neq 0$, то стигаме до противоречие с минималната степен на g. Следователно $r = 0 \Rightarrow f = gq \in (g) \Rightarrow I \subseteq (g) \Rightarrow I = (g)$.

□

Твърдение 11.4

Нека K е комутативен пръстен с 1, $f \in K[x]$ и $\alpha \in K$. Тогава

$$f(\alpha) = 0 \Leftrightarrow f = (x - \alpha)q \text{ за някой полином } q \in K[x].$$

Доказателство. Нека $f = (x - \alpha)q + r,\ q, r \in K[x]$ и $\deg(r) < \deg(x - \alpha)$, т.е. $r \in K$. Като заместим x с α получаваме $f(\alpha) = r$.

$$f(\alpha) = 0 \Leftrightarrow r = 0, \text{ т.е. } f = (x - \alpha)q.$$

□

Твърдение 11.5

Нека K е област, $f \in K[x]$. Ако $\deg(f) \leq n$ и съществуват два по два различни елемента $\alpha_1, \ldots, \alpha_{n+1}$, за които $f(\alpha_i) = 0,\ i = 1, \ldots, n+1$, то f е нулевият полином.

Доказателство. Допускаме, че $f \neq 0$.

$f(\alpha_1) = 0 \Rightarrow f = (x - \alpha_1)q_1,\ q_1 \in K[x]$
$f(\alpha_2) = (\alpha_2 - \alpha_1)q_1(\alpha_2)$
тъй като K е област и $\alpha_2 - \alpha_1 \neq 0 \Rightarrow$
$q_1(\alpha_2) = 0 \Rightarrow q_1 = (x - \alpha_2)q_2,\ q_2 \in K[x]$
$\Rightarrow f = (x - \alpha_1)(x - \alpha_2)q_2$
Продължавайки по същия начин получаваме
$f = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_{n+1})q_{n+1},\ q_{n+1} \in K[x]$
но тогава $\deg(f) \geq n + 1$, противоречие ! $\Rightarrow f = 0$.

□

Твърдение 11.6: Принцип за сравняване на коефициентите

Нека K е област и $g_1, g_2 \in K[x]$. Нека $\deg(g_1), \deg(g_2) \leq n$ и съществуват два по два различни елемента $\alpha_1, \ldots, \alpha_{n+1}$, за които $g_1(\alpha_i) = g_2(\alpha_i),\ i = 1, \ldots, n+1$. Тогава $g_1 = g_2$.

Доказателство. Да разгледаме полинома $f = g_1 - g_2$. От условието $\deg(f) \leq n$ и $f(\alpha_i) = 0,\ i = 1, \ldots, n+1$ и от Твърдение 11.5 следва, че $f = 0$, т.е. $g_1 = g_2$. □

ПРИМЕРИ:

- Ако K не е област, Твърдения 11.5 и 11.6 не са верни в общия случай. Полиномът $f = x^2 \in \mathbb{Z}_{16}$ се анулира в $x = \overline{0}, \overline{4}, \overline{8}, \overline{12}$.
- $f = 3x^5 - 4x^2 + 3x + 2$, пресметнете $f(-1)$ и разложете $f(x)$ по степените на $(x+1)$.

	3	0	0	−4	3	2
−1	3	−3	3	−7	10	−8
−1	3	−6	9	−16	26	
−1	3	−9	18	−34		
−1	3	−12	30			
−1	3	−15				
−1	3					

$f(x) = 3(x+1)^5 - 15(x+1)^4 + 30(x+1)^3 - 34(x+1)^2 + 26(x+1) - 8$

Глава 12

Делимост на полиноми над поле. Най-голям общ делител при полиноми.

F - поле, $F[x]$ - полиномиален пръстен

Дефиниция 12.1

*Нека $f, g \in F[x]$ и $g \neq 0$. Казваме, че g **дели** f, g/f, ако $\exists q \in F[x]$ такъв, че*

$$f = g.q.$$

*Това означава, че остатъкът от деление на f с g е 0. Ако g **не дели** f пишем $g \nmid f$.*

СВОЙСТВА:

(1) g/f и $a, b \in F,\ a \neq 0 \Rightarrow ag/bf$

(2) $a, b \in F$ и $a \neq 0 \Rightarrow af/bf$

(3) g/f и $f/g \Rightarrow g = cf, 0 \neq c \in F$ (Ако старшите коефициенти на f и g са равни, то $g = f$)

(4) g/f и $f/h \Rightarrow g/h$

(5) $g/f_1, \ldots f_k$ и $t_1, \ldots, t_k \in F[x] \Rightarrow g/t_1f_1 + \cdots + t_kf_k$

(6) $g/f_1 + f_2$ и $g/f_1 \Rightarrow g/f_2$
($f_1 + f_2 = 0$ и $g/f_1 \Rightarrow g/f_2$)

Дефиниция 12.2: НОД на полиноми

Нека $f, g \in F[x]$ са полиноми и поне единия е ненулев, т.е. $(f,g) \neq (0,0)$. Най-голям общ делител (НОД) на f и g е полинома d, ако изпълнява следните условия:

(1) d/f и d/g,

(2) ако d_1/f и d_1/g, то d_1/d.

Пишем $d = (f,g)$.

Аналогично се дефинира НОД на повече от два полинома $(f_1, \ldots, f_n)$.

Твърдение 12.3

Всеки два полинома $f, g \in F[x] : \ (f,g) \neq (0,0)$ притежават НОД.

Доказателство. Да разгледаме идеалът породен от полиномите f и g:

$$I = (f,g) = \{uf + vg \mid u, v \in F[x]\} \trianglelefteq F[x].$$

$I \neq \{0\}, (f,g) \neq (0,0)$
Е $F[x]$ всеки идеал е главен, следователно $I = (d)$. Ще докажем, че $d = (f,g)$.

(1) $f, g \in (d) \ \Rightarrow \ f = df_1, \ g = dg_1, \ f_1, g_1 \in F[x] \Rightarrow d/f$ и d/g.

(2) $d \in I \Rightarrow \exists u, v \in F[x] : d = uf + vg$. Ако d_1/f и $d_1/g \Rightarrow d_1/d$.

□

- Ако d и d' удовлетворяват определението за НОД следва, че d'/d и $d/d' \Rightarrow d' = ad, \ 0 \neq a \in F$.
- Ако d удовлетворява определението за НОД и $0 \neq a \in F$, то $d' = ad$ също го удовлетворява.
- Следователно НОД на f и g е определен с точност до ненулева константа от полето F.
- Ако старшият член на НОД - d е 1, т.е. полиномът е унитарен, то той е еднозначно определен.

12.1 Алгоритъм на Евклид

Доказателство за съществуване на НОД е и всъщност алгоритъм на Евклид. Той е и правило за намиране му.

Ако $g = 0$ (и $f \neq 0$) $\Rightarrow (f, g) = f$.
Нека $g \neq 0$.

$$\begin{array}{rcl} & f = gq_1 + r_1, & \deg(r_1) < \deg(g) \\ \text{ако } r_1 \neq 0, & g = r_1q_2 + r_2, & \deg(r_2) < \deg(r_1) \\ \text{ако } r_2 \neq 0, & r_1 = r_2q_3 + r_3, & \deg(r_3) < \deg(r_2) \\ & \dots & \\ & \text{всеки получен остатък} & \text{делим на следващият} \\ & \dots & \\ \text{ако } r_{n-1} \neq 0, & r_{n-2} = r_{n-1}q_n + r_n, & \deg(r_n) < \deg(r_{n-1}) \\ \text{ако } r_n \neq 0, & r_{n-1} = r_nq_{n+1} + r_{n+1}, & r_{n+1} = 0 \end{array}$$

Т.к. $\deg(g) > \deg(r_1) > \deg(r_2) > \deg(r_3) > \dots$ процесът е краен, следователно след краен брой стъпки остатъка е равен на нула, т.е. $\Rightarrow r_{n+1} = 0$.
$d = r_n = (f, g)$

(1) $d/r_{n-1} \Rightarrow d/r_{n-2}$ и така нататък $\uparrow\Rightarrow d/f$ и d/g.

(2) Ако d_1/f и $d_1/g \Rightarrow d_1/r_1, d/r_2$ и така $\downarrow d_1/d$.

Дефиниция 12.4

Два полинома са ***взаимно прости****, ако*

$$(f, g) = c, \quad c \neq 0, c \in F.$$

Може да считаме, че $(f, g) = 1$.

От Твърдение 12.3 следва, че ако $(f, g) = d \Rightarrow \exists u, v \in F[x]$:

$$uf + vg = d,$$

и го наричаме **тъждество на Безу**.
Ако $(f, g) = 1 \Rightarrow \exists u, v \in F[x] : uf + vg = 1$. Обратното също е вярно! (защо?)
Но полиномите от тъждеството на Безу не са еднозначно определени от f и g.

Твърдение 12.5

Нека $f_1, f_2, g \in F[x]$. *Ако* g/f_1f_2 *и* $(g, f_1) = 1 \Rightarrow g/f_2$.

Доказателство.

$$\begin{aligned}
&\exists u, v \in F[x] : \\
&ug + vf_1 = 1 \ /.f_2 \\
&ugf_2 + vf_1f_2 = f_2 \\
&g/ugf_2, \quad g/vf_1f_2 \Rightarrow g/f_2.
\end{aligned}$$

□

Твърдение 12.6

Нека $f, g_1, g_2 \in F[x]$. Ако $g_1/f, g_2/f$ и $(g_1, g_2) = 1 \Rightarrow g_1g_2/f$.

Доказателство.

$$\begin{aligned}
&f = g_1f_1 \\
&g_2/g_1f_1 \text{ и } (g_1, g_2) = 1 \Rightarrow g_2/f_1 \\
&\Rightarrow g_1g_2/g_1f_1 = f \\
&\Rightarrow g_1g_2/f.
\end{aligned}$$

□

Дефиниция 12.7: НОК на полиноми

*Нека $f, g \in F[x]$ са два ненулеви полиноми, т.е. $f \neq 0$, $g \neq 0$. **Най-малко общо кратно (НОК)** на f и g е полинома k, ако изпълнява следните условия:*

(1) f/k и g/k,

(2) ако f/k_1 и g/k_1, то k/k_1.

Пишем $k = [f, g]$.

Аналогично се дефинира НОК на повече от два полинома $[f_1, \ldots, f_n]$.

Твърдение 12.8

Ако $f, g \in F[x]$ са полиноми, то е в сила

(a) $(f) + (g) = \Big((f, g)\Big)$,

(b) $(f) \bigcap (g) = \Big([f, g]\Big)$

Доказателство. (a) Нека $d = (f, g) \Rightarrow \exists u, v \in F[x] : uf + vg = d$.

- От d/f и $d/g \Rightarrow (f) \subseteq (d), (g) \subseteq (d) \Rightarrow (f) + (g) \subseteq (d)$.
- От $d = uf + vg \Rightarrow (d) \subseteq (f) + (g)$.

(b) Нека $k = [f, g]$.

- От $h \in (k) \Rightarrow h = kh_1$ и $f/k \Rightarrow h \in (f)$. Аналогично $h \in (g) \Rightarrow h \in (f) \bigcap (g) \Rightarrow (k) \subseteq (f) \bigcap (g)$.
- От $y \in (f) \bigcap (g) \Rightarrow y \in (f)$ и $y \in (g) \Rightarrow f/y$ и $g/y \Rightarrow [f, g]/y \Rightarrow y \in \Big([f, g]\Big) \Rightarrow (f) \bigcap (g) \subseteq \Big([f, g]\Big)$.

□

Глава 13

Неразложими полиноми над поле. Разлагане на полином на неразложими множители.

F - поле, $F[x]$ - полиномиален пръстен

Дефиниция 13.1: Неразложим полином

Нека $f \in F[x]$ и $\deg(f) > 0$. Ще казваме, че полиномът f е ***неразложим над полето*** *F, ако не може да се представи като произведение на два полинома от $F[x]$, чиито степени са по-малки от степента на f, т.е.*

$$\nexists g, h \in F[x],\ \deg(g), \deg(h) < \deg(f) : f = gh.$$

Или единствените делители на f са полиномите от вида a и af, $0 \neq a \in F$. В противен случай f е ***разложим*** *над F.*

ПРИМЕРИ:

- Ако $\deg(f) = 1$, то f е неразложим, т.е. всеки полином от първа степен е неразложим.
- Един полином f може да е разложим над едно поле, а над друго да е разложим! $x^2 - 2$ - неразложим над $\mathbb{Q}$;
  $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ - разложим над $\mathbb{R}$;

Твърдение 13.2

Нека p и $f \in F[x]$ и p е неразложим полином. Тогава $(p, f) = 1 \Leftrightarrow p \nmid f$.

Доказателство. Нека $(f, p) = d = \begin{cases} 1, & p \text{ е неразложим} \\ p, & \end{cases}$.

$\Leftarrow$) Ако $d = p \Rightarrow d = p/f$ - противоречие! $\Rightarrow d = 1$.

$\Rightarrow$) $d = 1 \Rightarrow p \nmid f$.

□

Твърдение 13.3

Нека $f_1, f_2, p \in F[x]$ и p е неразложим полином. Ако p/f_1f_2 и $p \nmid f_1$, то p/f_2.

Доказателство. От твърдение 13.2 и 12.5 (Ако g/f_1f_2 и $(g, f_1) = 1 \Rightarrow g/f_2$.) твърдението следва. □

Теорема 13.4: Теорема за еднозначно разлагане на неразложими множители

Нека $f \in F[x]$ и $\deg(f) > 0$. Тогава $f \in F[x]$ се разлага в произведение на неразложими над F полиноми, т.е.

$$\exists\, p_1, p_2, \ldots, p_k \in F[x],\ \textit{неразложими}\ : f = p_1 \cdots p_k.$$

Ако $f = p_1 \cdots p_k = q_1 \cdots q_s$ са две такива разлагания, то $k = s$ и, след евентуално преномериране на множителите, за всяко $i = 1, \ldots, k$ е изпълнено

$$p_i = a_i q_i, \quad 0 \neq a_i \in F.$$

Доказателство. 1. **Съществуване:** Индукция по $n = \deg(f)$.

Нека $\deg(f) = n > 0$.

Ако f е неразложим полином, то $f = f$, т.е. произведение на един полином.

$\deg(f) = 1$ - като неразложим полином, случаят е същият.

Ако f е разложим, то $f = f_1f_2$, $\deg(f_1), \deg(f_2) < \deg(f)$ (от ИП)
$\Rightarrow f_i = \prod$ (неразложими полиноми), $i = 1, 2 \Rightarrow$ получаваме разлагане за f.

2. **Единственост:**

Нека $f = p_1 \ldots p_k = q_1 \ldots q_s$.

Индукция по k.

- $k = 1 \Rightarrow p_1 = q_1 \ldots q_s$. Ако $s > 1 \Rightarrow p_1$ - разложим (което е противоречие!) $\Rightarrow s = 1$ и $f = p_1 = q_1$.
- ИП, $k > 1$ и твърдението е вярно, ако в едната страна има по-малко от k множителя.
- k

  от $p_1 \ldots p_k = q_1 \ldots q_s \Rightarrow p_1/q_1 \ldots q_s$ от Твърдение 13.3 следва, че p_1 дели някой от $q_1, \ldots, q_s$. Нека p_1/q_1 (q_1 - неразложим) $\Rightarrow p_1 = a_1q_1, 0 \neq a_1 \in$

F. т.к. F-поле следва, че $F[x]$ е област и може да се съкрати на $q_1 \Rightarrow a_1 p_2 \dots p_k = q_2 \dots q_s$.
От ИП следва, че $k-1 = s-1$, т.е. $k = s, p_2 = a_2 q_2, \dots, p_k = a_k q_k,\ 0 \neq a_i \in F, i = 1, \dots k$.

□

Глава 14

Неразложими полиноми над полето на рационалните числа. Лема на Гаус и критерий на Айзенщайн.

$$f = c_0x^n + c_1x^{n-1} + \cdots + c_n = \frac{a_0}{b_0}x^n + \frac{a_1}{b_1}x^{n-1} + \cdots + \frac{a_n}{b_n} \in \mathbb{Q}[x]$$

е полином с рационални коефициенти и $q = \text{НОК}(b_0, b_1, \ldots, b_n) = [b_0, b_1, \ldots, b_n]$. Тогава

$$g = \frac{1}{q}.f.$$

Следователно f и g са едновременно разложими или неразложими над $\mathbb{Q}$. Свеждаме неразложимост на полином с рационални коефициенти над $\mathbb{Q}$ към неразложимост на полином с цели коефициенти над $\mathbb{Q}$.

Нека p е просто число и $\pi_p : \mathbb{Z} \to \mathbb{Z}_p$ е естествения хомоморфизъм на $\mathbb{Z}$ върху $\mathbb{Z}_p$.

$$\pi_p : \mathbb{Z} \to \mathbb{Z}_p$$
$$\pi_p : a \to a + p\mathbb{Z}, \quad a \in \mathbb{Z}, a + p\mathbb{Z} \in \mathbb{Z}_p$$

Твърдение 14.1

Нека R е комутативен пръстен с единица, $I \triangleleft R$ е идеал в R, а

$$\pi : R \to R/I, \quad \pi(a) = a + I$$

е естественият хомоморфизъм и ядрото е $Ker\ \pi = I$, а образа е $Im\ \pi = R/I$. Тогава π индуцира изображение на пръстени Π:

$$\Pi : R[x] \to (R/I)[x], \quad \Pi\left(\sum_{i=0}^{n} a_ix^i\right) = \sum_{i=0}^{n}(a_i + I)x^i$$

и ядрото е $Ker\ \Pi = I[x]$, а образа е $Im\ \Pi = (R/I)[x]$.

Доказателство. • $\Pi : R[x] \to (R/I)[x]$ е хомоморфизъм на пръстени. Нека $f = \sum_{i=0}^{n} a_i x^i$ и $g = \sum_{i=0}^{m} b_i x^i$ са полиноми с коефициенти от R. Тогава

$$\Pi(f+g) = \Pi(f) + \Pi(g)$$
$$\Pi(fg) = \Pi(f)\Pi(g)$$

По-подробно:

$$\begin{aligned}\Pi(f) + \Pi(g) &= \Pi\Big(\sum_{i=0}^{n} a_i x^i\Big) + \Pi\Big(\sum_{j=0}^{m} b_j x^j\Big) = \\ &= \Pi\Big(\sum_{i=0}^{n} (a_i + I)x^i\Big) + \Pi\Big(\sum_{j=0}^{m} (b_j + I)x^j\Big) = \\ &= \sum_{i=0}^{max(n,m)} (a_i + b_i + I)x^i = \\ &= \Pi\Big(\sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j\Big) = \Pi(f+g)\end{aligned}$$

$\Pi(fg) = \Pi(f)\Pi(g)$ - аналогично

- Ядрото на $Ker\ \Pi = I[x]$ е :

$$\begin{aligned}Ker\ \Pi &= \Big\{ f(x) = \sum_{i=0}^{n} a_i x^i \mid \Pi(f) = \sum_{i=0}^{n} (a_i + I)x^i = I \Big\} = \\ &= \Big\{ f(x) = \sum_{i=0}^{n} a_i x^i \mid a_i \in I,\ \forall\ 0 \le i \le n \Big\} = I[x].\end{aligned}$$

- Образът на $Im\ \Pi = (R/I)[x]$, тъй като всеки елемент на $(R/I)[x]$ е от вида:

$$\sum_{i=0}^{n} (a_i + I)x^i = \Pi(\sum_{i=0}^{n} a_i x^i),$$

за някакъв полином на $\sum_{i=0}^{n} a_i x^i \in R[x]$

□

Следствие 14.2

Ако p е просто число, то изображението

$$\Pi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x], \quad \Pi_p\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} (a_i + p\mathbb{Z})x^i$$

е хомоморфизъм на пръстени с ядро $Ker\ \Pi_p = (p\mathbb{Z})[x]$ и образ $Im\ \Pi_p = \mathbb{Z}_p[x]$.

Доказателство. Ако p е просто число, то

$$\pi_p : \mathbb{Z} \to \mathbb{Z}_p, \quad \pi_p(a) = a + p\mathbb{Z}$$

е естественият хомоморфизъм на $\mathbb{Z}$ върху $\mathbb{Z}_p$, нарича се още редукция на целите числа по модул .
Ако $\Pi_p(f) = \overline{f}$, то

$$f = a_0x^n + \cdots + a_n \in \mathbb{Z}[x]$$
$$\overline{f} = \overline{a_0}x^n + \cdots + \overline{a_n} \in \mathbb{Z}_p[x].$$

Ядрото на този хомоморфизъм е:

$$Ker\ \Pi_p = \{f = a_0x^n + \cdots + a_n \in \mathbb{Z}[x] \mid p/a_i, i = 0, \ldots, n, \}$$

□

Дефиниция 14.3

Нека $f = a_0x^n + \cdots + a_n \in \mathbb{Z}[x]$. Наричаме f е ***примитивен полином****, ако коефициентите му са взаимно прости, т.е. $(a_0, \ldots, a_n) = 1$.*

Ако $g \in \mathbb{Q}[x]$, то $g = \frac{r}{q}f$, където $f \in \mathbb{Z}[x]$ е примитивен полином.

Представяме първо $g = \frac{1}{q}f_1$, където q =НОК(знаменателите на коефициентите на g).
После $g = \frac{r}{q}f$, където r =НОД(на коефициентите на f_1).
$f = a_0x^n + \cdots + a_n \in \mathbb{Z}[x]$.
Коефициентите на f са взаимно прости $\Leftrightarrow$ нямат общ прост делител, т.е. когато $\forall p:$ просто число, $\exists\ 0 \le i \le n : p \nmid a_i$.
f - примитивен полином $\Leftrightarrow \forall p:$ просто число, $\overline{f} \neq \overline{0} \in \mathbb{Z}_p$.

Твърдение 14.4

Нека $h \in \mathbb{Z}[x]$ е примитивен полином, $c \in \mathbb{Q}$ и $ch \in \mathbb{Z}[x]$. Тогава $c \in \mathbb{Z}$.

Доказателство. Нека $h = p_0x^k + \cdots + p_k \in \mathbb{Z}[x]$ и $c = \frac{r}{q}, r, q \in \mathbb{Z}$ такива, че $(r, q) = 1$.
От $ch \in \mathbb{Z}[x] \Rightarrow \frac{rp_i}{q} \in \mathbb{Z}$, т.е. q/rp_i.
От $(r, q) = 1 \Rightarrow q/p_i, i = 0, \ldots, k$.
h е примитивен полином $\Rightarrow (p_0, \ldots, p_k) = 1 \Rightarrow q = \pm 1 \Rightarrow c = \pm r \in \mathbb{Z}$.

□

Лема 14.5: Лема на Гаус

Ако f и $g \in \mathbb{Z}[x]$ са примитивни полиноми, то произведението fg е примитивен полином.

Доказателство. Нека $f, g \in \mathbb{Z}[x]$ - примитивни полиноми и p е просто число.
$\Rightarrow \overline{f}, \overline{g} \neq \overline{0} \in \mathbb{Z}_p$.
$\mathbb{Z}_p$ е област и $\overline{f}.\overline{g} = \overline{fg}$, защото $\Pi_p(fg) = \Pi_p(f)\Pi_p(g)$ е хомоморфизъм
$\Rightarrow \overline{fg} \neq \overline{0} \Rightarrow fg$ е примитивен полином. □

Следствие 14.6

Нека $f \in \mathbb{Z}[x]$ е полином с цели коефициенти.

Ако полиномът f е разложим над $\mathbb{Q}$, то f е разложим и над $\mathbb{Z}$.

Т.е. f неразложим над $\mathbb{Q} \Leftrightarrow f$ е неразложим над $\mathbb{Z}$.

Доказателство. Нека $f = f_1f_2,\ f_1, f_2 \in \mathbb{Q}[x]$.

$$f_1 = \frac{p_1}{q_1}h_1,\ h_1 \in \mathbb{Z}[x],\ \text{примитивен полином}$$
$$f_2 = \frac{p_2}{q_2}h_2,\ h_2 \in \mathbb{Z}[x],\ \text{примитивен полином}$$
$$\Rightarrow f = \frac{p_1p_2}{q_1q_2}\underbrace{h_1h_2}_{\text{примитивен}}$$
$$f \in \mathbb{Z}[x] \Rightarrow c = \frac{p_1p_2}{q_1q_2} \in \mathbb{Z} \text{ от Твърдение } 14.4$$
$$f = (ch_1)h_2,\ ch_1, h_2 \in \mathbb{Z}[x].$$

Така въпроса за неразложимост над $\mathbb{Q}$ на полином с рационални коефициенти се свежда до неразложимост над $\mathbb{Z}$ на полином с цели коефициенти. □

Твърдение 14.7: Критерий на Айзенщайн

Нека $f = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$ *е полином с цели коефициенти и съществува просто число* p*, за което*

(1) $p \nmid a_0$,

(2) $p/a_1, \ldots, a_n$,

(3) $p^2 \nmid a_n$.

Тогава f *е неразложим над* $\mathbb{Q}$.

Доказателство. Да допуснем противното $f = gh,\ \deg(g), \deg(h) < \deg(f)$.
Можем да считаме, че (Следствие 14.6), че $g, h \in \mathbb{Z}[x]$. Тогава $\overline{gh} = \overline{g}.\overline{h}$.
От (1) и (2), следва, че $\overline{f} = \overline{a_0}x^n,\ a_0 \neq \overline{0}$.
От теоремата за еднозначно разлагане на неразложими множители следва, че

$$\overline{g} = \overline{b}x^k,$$
$$\overline{h} = \overline{c}x^l,$$
$$\text{където } \overline{b}\overline{c} = \overline{a_0},\ k, l < n \text{ и } k + l = n.$$

Тогава

$$g = bx^k + pg_1,$$
$$h = cx^l + ph_1,$$
$$\text{където } b \text{ и } c \text{ са подходящи праобрази на } \overline{b} \text{ и } \overline{c}$$

Следователно

$$f = a_0x^n + \cdots + a_n = (bx^k + pg_1)(cx^l + ph_1)$$
$$a_n = f(0) = p^2g_1(0)h_1(0),$$
$$\Rightarrow p^2/a_n \text{ противоречие! .}$$

$\Rightarrow f$ е неразложим над $\mathbb{Q}$.

□

Твърдение 14.8

За всяко естествено число n *съществува неразложим полином от* $\mathbb{Q}[x]$ *от степен* n.

Доказателство. От критерия на Айзенщайн, такива са например полиномите $x^n + p$, където p е произволно просто число. □

Дефиниция 14.9

Нека полето K е разширение на полето F, т.е. $F \leq K$ и $\alpha \in K$. Наричаме α е ***корен*** *на f, ако $f(\alpha) = 0$.*

Намирането на корените на полином с рационални коефициенти се свежда до намирането на корените на полином с цели коефициенти. Ако $g \in \mathbb{Q}[x] \Rightarrow g = \frac{1}{q} f,\ f \in \mathbb{Z}[x]$, то f и g имат едни и същи корени.

Твърдение 14.10

Нека $f = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in \mathbb{Z}[x]$ и $\alpha = \frac{u}{v}$ е рационален корен на f, ако $u, v \in \mathbb{Z}, (u, v) = 1$.

Тогава $u/a_n, v/a_0$.

Доказателство.

$$
\begin{aligned}
& f(\alpha) = f\left(\frac{u}{v}\right) = 0 \\
& \Rightarrow a_0 \left(\frac{u}{v}\right)^n + a_1 \left(\frac{u}{v}\right)^{n-1} + \cdots + a_{n-1} \left(\frac{u}{v}\right) + a_n = 0 \ /.v^n \\
& \Rightarrow a_0 u^n + a_1 u^{n-1} v + \cdots + a_{n-1} u v^{n-1} + a_n v^n = 0 \\
& \Rightarrow u / a_n v^n \text{ и } (u, v) = 1 \\
& \Rightarrow u / a_n.
\end{aligned}
$$

Аналогично v/a_0. □

Глава 15

Корени на полиномите. Кратни корени. Поле на разлагане. Формули на Виет.

15.1 Корени на полиномите.

Нека $f \in F[x]$ е полином с коефициенти от дадено поле F. Полиномът може да няма корени в F. Например $x^2 + 1 \in \mathbb{R}[x]$ няма корени в $\mathbb{R}$, но има в $\mathbb{C}$. При това $\mathbb{C}$ е разширение на полето $\mathbb{R}$.

Дали за всеки полином $f, \deg(f) > 1$ със степен по-голяма от 1, може да се намери разширение на полето от коефициентите, в което полиномът да има поне един корен?

Дефиниция 15.1: Корен на полином

*Нека полето K $(F \leq K)$ е разширение на полето F, $\alpha \in K$ и $f \in F[x]$. Наричаме α е **корен** на полинома f, ако $f(\alpha) = 0$.*

Теорема 15.2

Нека F е поле и $f \in F[x]$, $\deg(f) > 0$.
Тогава f е неразложим полином $\Leftrightarrow M = (f)$ е максимален идеал.

Доказателство. Да припомним, че $F[x]$ е област на главни идеали, т.е. ако F е поле, то всеки идеал I в пръстена $F[x]$ е главен, Твърдение 11.3.

$\Rightarrow$) Полиномът f е неразложим, $\deg(f) > 0 \Rightarrow f \neq 1 \Rightarrow M = (f) \neq F[x]$.

Да допуснем, че съществува идеал I такъв, че $M \subseteq I \subseteq F[x]$ и трябва да покажем, че $I = M$ или $I = F[x]$. В $F[x]$ всеки идеал е главен следователно $I = (g)$.

$\Rightarrow (f) \subseteq (g) \Rightarrow f = gh, h \in F[x]$. Но f е неразложим, т.е. или g е от степен 0 или h е от степен 0 (т.е. елемент от F).

Ако $\deg(g) = 0$ тогава g е единица в $F[x]$ и $I = F[x]$.

Ако $\deg(h) = 0 \Rightarrow f = \alpha g, \alpha \in F$ и $g = \alpha^{-1} f \in M \Rightarrow I = M$. Следователно M е максимален идеал.

$\Leftarrow$) Нека M е максимален идеал. Нека $f \neq 0$ и допуснем, че е разложим полином, т.е. $f = gh, 1 \leq \deg(g), \deg(h) < \deg(f)$. И двата полинома имат степени по-големи от 1 (т.е. не са единица в $F[x]$) следователно $(g) \neq M \Rightarrow (g) \subset M$, аналогично за $(h) \subset M$, т.е. са собствени идеали. Тогава собствените идеали (g) и (h) съдържат M. Това противоречи на максималността на M, което се дължи на допуснатото. Следователно f е неразложим.

□

Теорема 15.3

Нека F е поле, $f \in F[x]$, $\deg(f) > 0$ и $M = (f)$.
Тогава $F[x]/M$ е поле $\Leftrightarrow$ f е неразложим полином.

Доказателство. f е неразложим полином $\Leftrightarrow$ $M = (f)$ е максимален идеал (Теорема 15.2) $\Leftrightarrow$ $F[x]/M$ е поле (Теорема 10.21). □

Да разгледаме внимателно структурата на факторпръстена $F[x]/\big(f\big)$, където $f \in F[x]$ е произволен ненулев полином.

$$F[x]/\big(f\big) = \Big\{ g + \big(f\big) \mid g \in F[x] \Big\}$$

с операциите събиране и умножение дефинирани във факторпръстена:

$$(a + \big(f\big)) + (b + \big(f\big)) = a + b + \big(f\big)$$
$$(a + \big(f\big))(b + \big(f\big)) = ab + \big(f\big).$$

Два съседни класа $g + (f)$ и $h + (f)$ са равни, т.е.

$$g + (f) = h + (f) \Leftrightarrow$$
дават един и същи остатък при деление на $f \Leftrightarrow$
$$g - h \in (f) \Leftrightarrow$$
$$f/(g - h) \Leftrightarrow$$
$$g \equiv h (mod\ f).$$

Това е еквивалентно g и h да дават един и същи остатък при деление на f. Така всеки съседен клас $g + (f)$ съдържа единствен представител представител $r \in F[x]$ със свойството $\deg(r) < \deg(f)$, което е всъщност остатъка при деление на g с f.

Процесът на преминаване от g към r се нарича **редукция** по модул f. Единствеността на r следва от факта, че ако съществува $r_1 \in g + \big(f\big)$ такъв, че $\deg(r_1) < \deg(f)$, то $r - r_1$ се дели на f и $deg(r - r_1) < \deg(f)$, което е възможно само, ако $r = r_1$.

Различните съседни класове на факторпръстена $F[x]/(f)$ могат да бъдат описани точно, а именно това са точно съседните класове $r + \big(f\big)$, където r пробягва всички полиноми от $F[x]$ със $\deg(r) < \deg(f)$, т.е. ако $\deg(f) = n$, то

$$\begin{aligned} F[x]/\big(f\big) &= \Big\{ r + \big(f\big) \mid r \in F[x], \deg(r) < \deg(f) \Big\} \\ &= \Big\{ \underbrace{r_0 x^{n-1} + r_1 x^{n-2} + \cdots + r_n}_{r} + \big(f\big) \mid r_i \in F, i = 0, \ldots, n-1 \Big\} \end{aligned}$$

Поле с четири елемента.

Да разгледаме полето $(\mathbb{Z}_2, +, .)$ и полиномите с коефициенти от $\mathbb{Z}_2$, т.е. $\mathbb{Z}_2[x]$. Полиномите от степен две са 4:

$$x^2,\ x^2 + \overline{1},\ x^2 + x,\ x^2 + x + \overline{1}.$$

Проверяваме за неразложимост:

$$\begin{aligned} &x^2 = x.x, \\ &x^2 + \overline{1} = (x + \overline{1})^2, \\ &x^2 + x = x(x + \overline{1}), \\ &x^2 + x + \overline{1} - \text{ - неразложим.} \end{aligned}$$

Нека $f = x^2 + x + \overline{1}$ и $I = (f)$, от Теорема 15.3 следва, че $\mathbb{Z}_2[x]/I$ е поле. Елементите на $\mathbb{Z}_2[x]/I$ са:

$$\mathbb{Z}_2[x]/I = \{a + bx + I \mid a, b \in \mathbb{Z}_2\}.$$

Да означим $\mathbb{Z}_2[x]/I$ с L. Тогава елементите на полето L са 4 на брой:

$$\overline{0} = I, \quad \overline{1} = 1 + I, \quad \overline{x} = x + I, \quad \overline{x+1} = x + 1 + I.$$

Таблиците за събиране и умножение на елементите на L са :

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$.$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

Да отбележим, че $(L, +) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, докато $(L \setminus \{0\}, .) \cong \mathbb{Z}_3$. Всъщност $\overline{x+1} = \overline{x}^2$ и следователно ако означим $\overline{x}$ с α, то можем да напишем:

$$L = \{0, 1, \alpha, \alpha^2\}, \text{ където } \alpha + 1 = \alpha^2 \text{ и } \alpha^3 = 1.$$

Събирането и умножението написани с това означение са:

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$.$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Ако елементите на L са записани като степени на α, то умножението става лесно, но за събирането трябва да се използват допълнителни условия (съотношения).

Да отбележим, че L съдържа подполе, съдържащо елементите $\{0,1\}$. Така това подполе е изоморфно на $\mathbb{Z}_2$. С други думи L е по-голямото поле съдържащо подполе изоморфно на $\mathbb{Z}_2$ или можем да кажем, че L съдържа $\mathbb{Z}_2$. Т.е. L е разширение на $\mathbb{Z}_2$.

Оригиналния полином f е полином от $\mathbb{Z}_2[x]$, но също може да мислим, че е полином от $L[x]$. Обаче в L полиномът f не е неразложим! Всъщност има корен:

$$\alpha^2 + \alpha + 1 = 0.$$

В $L[x]$ имаме:

$$x^2 + x + 1 = (x - \alpha)(x - \alpha^2).$$

Стартирахме с поле с два елемента и неразложим полином (от степен 2) над това поле. Конструирахме разширение на това поле, в което този полином има корен!

Теорема 15.4

Нека $f \in F[x]$ и $\deg(f) > 0$. Тогава съществува разширение K на полето F, в което полиномът f има корен.

Доказателство.

- Ако $f = f_1 \dots f_k$, то ако намерим разширение на F, в което един от тези множители има корен, то той ще бъде корен и на f. Така без ограничение на общността можем да считаме, че f е неразложим над F полином. Нека $\deg(f) = n$ и
$$f = a_0 x^n + a_1 x^{n-1} + \dots + a_n.$$
.

- Нека $I = (f)$ и $K = F[x]/I$. От Теорема 15.3 следва, че K е поле.

  Да разгледаме естествения хомоморфизъм от $F[x]$ върху K:

$$\pi : F[x] \to K = F[x]/I$$
$$\pi(g) = g + I, \quad g \in F[x].$$

  Елементите на $K = F[x]/I$ са:

$$K = F[x]/(f) = \Big\{ r + I \mid r \in F[x], \deg(r) < \deg(f) \Big\}$$

Да означим с

$$F_1 = \left\{ r_0 + I \mid r_0 \in F \right\}.$$

Да означим с $\varphi = \pi_{|F}$ ограничението на π върху F, т.е.

$$\begin{aligned} &\varphi : F \to F_1 \\ &\varphi(a) = a + I, \quad a \in F. \end{aligned}$$

φ е изоморфизъм.

$Ker\varphi = \{0\} \triangleleft F$, но F е поле и единствените му идеали са $\{0\}$ и F. $Ker\varphi \neq F \Rightarrow Ker\varphi = \{0\}$.

$Im\varphi = F_1$ и от теоремата за хомоморфизми $F/\{0\} = F \cong Im\varphi = F_1 \subset K$. Благодарение на този изоморфизъм може да отъждествяваме F и F_1 или полето K е разширение на F.

- Разглеждаме полиномът f като полином с коефициенти от K. Ще докажем, че $\alpha = x + I$ от полето K е корен f.

  $f \in F[x] = F_1[x] \subset K[x]$. Тогава полиномът

  $$f = a_o x^n + a_1 x^{n-1} + \cdots + a_n$$

  ще има представяне

  $$f = (a_0 + I)x^n + (a_1 + I)x^{n-1} + \cdots + (a_n + I),$$

  разглеждан като полином от $K[x]$. Тогава

  $$\begin{aligned} f(\alpha) &= (a_0 + I)(x + I)^n + (a_1 + I)(x + I)^{n-1} + \cdots + (a_n + I) \\ &= (a_0 + I)(x^n + I) + (a_1 + I)(x^{n-1} + I) + \cdots + (a_n + I) \\ &= f(x) + I = I. \end{aligned}$$

  т.е. $f(\alpha)$ съвпада с нулевия елемент I на полето K, а това значи, че α е корен на f.

□

Нека $K \geq F$ е разширение на F. За всеки полином $f = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in F[x]$, дефинираме стойността на f в $x = \alpha$ по-следния начин:

$$f(\alpha) = a_0 \alpha^n + a_1 \alpha^{n-1} + \cdots + a_n.$$

Дефинираме:

$$F[\alpha] = \{ f(\alpha) \mid f(x) \in F[x] \} \subseteq K$$

и

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f(x), g(x) \in F[x] \text{ и } g(\alpha) \neq 0 \right\} \subseteq K.$$

Твърдение 15.5

Нека K е поле, F е подполе на K и $\alpha \in K$. Тогава $F[\alpha]$ е подпръстен на K и е област, а $F(\alpha)$ е подполе на K.

Доказателство. Нека $f(x), g(x) \in F[x] \Rightarrow f(x) \pm g(x),\ f(x).g(x) \in F[x]$. Следователно $f(\alpha) \pm g(\alpha) \in F[\alpha]$ и $f(\alpha).g(\alpha) \in F[\alpha]$. Ясно е, че $1 \in F[\alpha]$. Откъдето следва, че $F[\alpha]$ е подпръстен на K. Но подпръстен на поле всъщност е област.

Аналогично може да се покаже, че $F(\alpha)$ е подполе на K. □

Теорема 15.6

Нека полето K е разширение на полето F и $\alpha \in K$. Нека $f \in F[x]$ е неразложим полином от степен n и $f(\alpha) = 0$.

(1) Тогава $F[\alpha]$ е подполе на K,

$$F[\alpha] = \{a_{n-1} + a_{n-2}\alpha + a_{n-3}\alpha^2 + \cdots + a_0\alpha^{n-1} \mid a_i \in F,\ i = 0, 1, \ldots, n-1\},$$

и всеки елемент от $F[\alpha]$ може да се изрази еднозначно във вида:

$$a_{n-1} + a_{n-2}\alpha + a_{n-3}\alpha^2 + \cdots + a_0\alpha^{n-1},\ \text{където } a_0, a_1, \ldots, a_{n-1} \in F.$$

(2) $F[\alpha] \cong F[x]/(f)$.

(3) $F(\alpha) = F[\alpha]$.

(4) Ако F е крайно поле с q елемента, то $\left|F[\alpha]\right| = q^n$.

Доказателство. (1) $F[\alpha] = \{a_{n-1} + a_{n-2}\alpha + a_{n-3}\alpha^2 + \cdots + a_0\alpha^{n-1} \mid a_i \in F\}$

Включването $\{a_{n-1} + a_{n-2}\alpha + a_{n-3}\alpha^2 + \cdots + a_0\alpha^{n-1} \mid a_i \in F\} \subseteq F[\alpha]$ е очевидно. (Полиномите на α от степен $\leq n-1$ с коефициенти от F се съдържат във всички полиноми на α с коефициенти от F.)

За обратното включване $F[\alpha] \subseteq \{a_{n-1} + a_{n-2}\alpha + a_{n-3}\alpha^2 + \cdots + a_0\alpha^{n-1} \mid a_i \in F\}$ делим произволен полином $g \in F[x]$ на f с частно и остатък $q, r \in F[x]$, т.е.

$$\begin{aligned} &g = fq + r,\ \deg(r) < \deg(f) = n \Rightarrow \\ &g(\alpha) = r(\alpha) \in \{a_{n-1} + a_{n-2}\alpha + a_{n-3}\alpha^2 + \cdots + a_0\alpha^{n-1} \mid a_i \in F\} \\ &f(\alpha) = 0 \end{aligned}$$

Откъдето $F[\alpha] \subseteq \{a_{n-1} + a_{n-2}\alpha + a_{n-3}\alpha^2 + \cdots + a_0\alpha^{n-1} \mid a_i \in F\}$. Всеки елемент от $F[\alpha]$ може да се изрази като линейна комбинация на $1, \alpha, \ldots, \alpha^{n-1}$ с коефициенти от F или като полином на α от степен $\leq n-1$ с коефициенти от F.

Еднозначност на представянето. ($1, \alpha, \ldots, \alpha^{n-1}$ са линейно независими)

Да допуснем, че:

$$h_0\alpha^{n-1} + h_1\alpha^{n-2} + \cdots + h_{n-1} = 0, \text{ където } h_0, \ldots, h_{n-1} \in F.$$

Ако

$$h(x) = h_0x^{n-1} + h_1x^{n-2} + \cdots + h_{n-1} = 0, \text{ то } h(\alpha) = 0.$$

Следователно $(x-\alpha)/h(x)$ и $(x-\alpha)/f(x)$. Следователно $(h, f) \neq 1$. Понеже полиномът f е неразложим, то $(h, f) = f$ и f/h. Но $\deg(h) < \deg(f) = n \Rightarrow h(x) = 0$ и следователно $h_0 = \ldots h_{n-1} = 0$. Откъдето заключаваме, че всеки елемент от $F[\alpha]$ може да бъде изразен еднозначно като полином на α от степен $\leq n-1$ с коефициенти от F.

(2) $F[\alpha] \cong F[x]/(f)$

Да означим $I = (f)$. Да разгледаме изображението:

$\psi : F[x]/I \to F[\alpha]$

$\psi : a_{n-1} + a_{n-2}x + a_{n-3}x^2 + \cdots + a_0x^{n-1} + I \to a_{n-1} + a_{n-2}\alpha + a_{n-3}\alpha^2 + \cdots + a_0\alpha^{n-1}$

Изображението ψ е биекция и запазва операциите събиране и умножение. От теорема 15.3 $F[x]/I$ е поле. Следователно и $F[\alpha]$ е поле и ψ е изоморфизъм.

(3) $F(\alpha) = F[\alpha]$

Включването $F[\alpha] \subseteq F(\alpha)$ е ясно.

Ще докажем и обратното включване. Нека $\dfrac{h(\alpha)}{g(\alpha)}$, където $g(\alpha) \neq 0$.

От $f(\alpha) = 0 \Rightarrow f \nmid g$. Но f е неразложим полином над F, така че $(f, g) = 1$. Тогава съществуват полиноми $u, v \in F[x]$ такива, че

$$u(x)f(x) + v(x)g(x) = 1.$$

Замествайки $x = \alpha$ получаваме $v(\alpha)g(\alpha) = 1$. Тогава

$$\frac{h(\alpha)}{g(\alpha)} = \frac{v(\alpha)h(\alpha)}{v(\alpha)g(\alpha)} = v(\alpha)h(\alpha) \in F[\alpha].$$

Следователно $F(\alpha) \subseteq F[\alpha] \Rightarrow F(\alpha) = F[\alpha]$.

□

ПРИМЕРИ:

- $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\} \cong \mathbb{R}/(x^2+1) \cong \mathbb{R}(i) \cong \mathbb{R}[i]$
- $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\} \cong \mathbb{Q}/(x^2-3)$
- $\mathbb{Q}(\sqrt[3]{7}) = \{a + b\sqrt[3]{7} + c(\sqrt[3]{7}^2) \mid a, b, c \in \mathbb{Q}\} \cong \mathbb{Q}/(x^3-7)$

Следствие 15.7

Нека $f \in F[x]$ и $\deg(f) = n > 0$. Тогава съществува разширение L на полето F такова, че всички корени на f са в това разширение или f се разлага в произведение на линейни множители над L, т.е.

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

Доказателство. Нека $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$. Индукция по степента на полинома $n = \deg(f) \in \mathbb{N}$.

- $n = 1 \Rightarrow f = a_0x + a_1 \in F[x] \Rightarrow$ има корен $-\dfrac{a_1}{a_0} \in F$.
- ИП за полиноми със степен по-малка от n.
- n

  От Теорема 15.4 следва, че съществува разширение $K_1 \geq F$, в което $f(x)$ има корен $\alpha_1 \in K_1$. Тогава

  $$f(x) = (x - \alpha_1)g(x),\ g(x) \in K_1[x],\ \deg(g) = \deg(f) - 1.$$

  Старшият коефициент на g е равен на старшия коефициент на f и е a_0. От ИП съществува разширение K_2, над което g се разлага на линейни множители, т.е.

  $$g = a_0(x - \beta_1)\dots(x - \beta_{n-1}).$$

  Тогава

  $$f(x) = (x - \alpha_1)g(x) = a_0(x - \alpha_1)(x - \beta_1)\dots(x - \beta_{n-1}),$$

  с което твърдението е доказано.

□

Дефиниция 15.8: Поле на разлагане

*Нека $f \in F[x], \deg(f) > 0$. **Поле на разлагане на полинома f над F** е минималното поле, което съдържа F и всички корени на f.*

ПРИМЕРИ:

- Ако $f = x^2 + 1 \in \mathbb{R}[x]$, то полето на разлагане над $\mathbb{R}$ е $\mathbb{C}$.
- Ако $f = x^2 + 1 \in \mathbb{Q}[x]$, то полето на разлагане над $\mathbb{Q}$ е $\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$.
- Ако $f = x^2 - 7 \in \mathbb{Q}[x]$, то полето на разлагане над $\mathbb{Q}$ е $\mathbb{Q}(\sqrt{7})$.
- Ако $f = x^2 + 7 \in \mathbb{Q}[x]$, то полето на разлагане над $\mathbb{Q}$ е $\mathbb{Q}(i\sqrt{7})$.
- Ако $f = x^2 + 7 \in \mathbb{R}[x]$, то полето на разлагане над $\mathbb{R}$ е $\mathbb{C}$.

Теорема 15.9: Теорема за единственост на полето на разлагане

Нека $f \in F[x], \deg(f) > 0$ и L_1 и L_2 са две полета на разлагане на полинома f над полето F. Тогава

$$L_1 \cong L_2.$$

Доказателство. □

15.2 Формули на Виет.

Нека $f = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n \in F[x]$ и $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ са всички корени на f, лежащи в полето K разширение на полето F, т.е.

$$\begin{aligned} f &= a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n && (1)\\ &= a_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) && (2)\end{aligned}$$

Приравнявайки коефициентите пред съответните степени на x получаваме формулите на Виет.

Дефиниция 15.10: Формули на Виет

Връзката между корените на полинома f и коефициентите му се дава с ***формулите на Виет:***

$$\begin{aligned} &\alpha_1 + \alpha_2 + \cdots + \alpha_n = -\frac{a_1}{a_0}\\ &\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n = \frac{a_2}{a_0}\\ &\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n = -\frac{a_3}{a_0}\\ &\ldots\\ &\alpha_1\alpha_2\ldots\alpha_n = (-1)^n\frac{a_n}{a_0}\end{aligned}$$

Дефиниция 15.11: k-кратен корен

Нека $f \in F[x], K$ е разширение на F и $\alpha \in K$. Полиномът f има ***k-кратен корен*** *α, ако*

$$f(x) = (x-\alpha)^k g(x),\ g(x) \in K[x] \text{ и } g(\alpha) \neq 0.$$

При $k = 1$, α наричаме прост корен на f, а при $k > 1$ - кратен корен на f.

Нека $f', f'', \ldots, f^{(n)}$ производните на полинома f ($f^{(0)} = f$).

Теорема 15.12

Нека $charF = 0, f \in F[x], K$ *е разширение на* F *и* $\alpha \in K$. *Тогава*

$$\alpha \text{ е } k\text{-кратен корен на } f \Leftrightarrow f(\alpha) = f'(\alpha) = \cdots = f^{k-1}(\alpha) = 0 \text{ и } f^k(\alpha) \neq 0.$$

Доказателство. $\Rightarrow$) Нека α е k-кратен корен на f. Ще докажем, че $f(\alpha) = f'(\alpha) = \cdots = f^{k-1}(\alpha) = 0$ и $f^k(\alpha) \neq 0$.

Индукция по k.

- $k = 1$ (α е прост корен на f).

$$\begin{aligned} & f(x) = (x-\alpha)g(x),\ g(x) \in K[x],\ g(\alpha) \neq 0 \\ \Rightarrow\ & f'(x) = g(x) + (x-\alpha)g'(x) \\ \Rightarrow\ & f'(\alpha) = g(\alpha) \neq 0 \\ \Rightarrow\ & f(\alpha) = 0,\ f'(\alpha) \neq 0. \end{aligned}$$

- ИП - нека $k > 1$ и твърдението е вярно за числа, по-малки от k.
- k

$$\begin{aligned} & f(x) = (x-\alpha)^k g(x),\ g(x) \in K[x],\ g(\alpha) \neq 0 \\ \Rightarrow\ & f'(x) = k(x-\alpha)^{k-1}g(x) + (x-\alpha)^k g'(x) \\ \Rightarrow\ & f'(x) = (x-\alpha)^{k-1} \underbrace{\Big(kg(x) + (x-\alpha)g'(x)\Big)}_{g_1(x)} \\ \Rightarrow\ & f'(x) = (x-\alpha)^{k-1} g_1(x) \\ \Rightarrow\ & g_1(\alpha) = kg(\alpha) \neq 0 \quad char\ F = 0 \\ \Rightarrow\ & \alpha \text{ е } (k-1) \text{ -кратен корен на полинома } f'(x). \\ \Rightarrow\ & \text{твърдението следва от ИП.} \end{aligned}$$

$\Leftarrow$) Нека $f(\alpha) = f'(\alpha) = \cdots = f^{k-1}(\alpha) = 0$ и $f^k(\alpha) \neq 0$.

Нека α е l-кратен корен на f.

- Ако $l < k$, то $l \leq k-1$ и значи $f^{(l)}(\alpha) = 0$ - противоречие!
- Ако $k < l$, то $k \leq l-1$ и от първата част на теоремата следва $f^{(k)}(\alpha) = 0$ - противоречие!
- Следователно $l = k$, т. е. α е k-кратен корен на f.

□

Твърдение 15.13

Нека $f \in F[x]$, K е разширение на F и $\alpha \in K$. Тогава

$$\alpha \text{ е кратен корен } \Leftrightarrow f(\alpha) = f'(\alpha) = 0.$$

Или един полином $f \in F[x]$ има кратен корен тогава и само тогава, когато има общ корен с производната си.

Доказателство. Нека характеристиката на F е произволна.

$\Rightarrow$) α е k-кратен корен $\Rightarrow$ е поне $(k-1)$-кратен корен на производната му f'.

$\Leftarrow$) Да допуснем, че α е прост корен - противоречие с $f(\alpha) = f'(\alpha) = 0 \Rightarrow$ е кратен корен.

□

Глава 16

Симетрични полиноми над поле. Основна теорема за симетричните полиноми. Формули на Нютон.

Нека A е комутативен пръстен с 1.

Пръстенът $B = A[x]$ на полиномите на променливата x е комутативен пръстен с 1. $B = A[x]$ съдържа A.

Продължаваме по същия начин. Да построим пръстена $C = B[y]$ на полиномите на променливата y с коефициенти от B. C е комутативен пръстен с 1 съдържа B и следователно A. C се нарича пръстен на полиномите на две променливи x и y с коефициенти от A и се бележи с $C = A[x, y]$. $C = A[x, y] = B[y] = A[x][y] \Rightarrow$ всеки елемент на $A[x, y]$ се записва като крайна сума:

$$f(x, y) = \sum_{i,j} a_{ij} x^i y^j, \ a_{ij} \in A.$$

Повтаряйки същата конструкция достигаме до пръстена $A[x_1, \ldots, x_n]$ на полиномите на n променливи с коефициенти от A. $A[x_1, \ldots, x_n]$ е комутативен пръстен с 1 и съдържа A. В сила са равенствата:

$$A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n] = \cdots = A[x_1][x_2] \ldots [x_n]$$

Дефиниция 16.1: Моном, едночлен

Полином от вида $aX^I = ax_1^{i_1} \ldots x_n^{i_n}, \ a \in A$ *се нарича* ***моном*** *или* ***едночлен***.

Ако $f \in A[x_1, \ldots, x_n] \Rightarrow f = f(x_1, \ldots, x_n)$ следователно всеки полином е крайна сума на едночлени, т.е.

$$f(x_1, \ldots, x_n) = \sum_{I=\{i_1,\ldots,i_n\}} a_I x_1^{i_1} \ldots x_n^{i_n}, \ a \in A.$$

Дефиниция 16.2: Подобни едночлени

Два ненулеви едночлена

$$u = aX^I = ax_1^{i_1} \dots x_n^{i_n},\ a \in A$$
$$v = bX^J = bx_1^{j_1} \dots x_n^{j_n},\ b \in A$$

се наричат ***подобни****, ако*

$$i_1 = j_1, \dots, i_n = j_n$$

или всяка променлива участва с една и съща степен в двата едночлена.

Ако $f \in A[x_1, \dots, x_n]$ е представен като сума на неподобни едночлени, то казваме че в f е извършено приведение на подобни едночлени.

Ако A е област, то $A[x_1, \dots, x_n]$ също е област.

Дефиниция 16.3

Нека $u = aX^I = ax_1^{i_1} \dots x_n^{i_n},\ 0 \neq a \in A$ *е едночлен и* $f \in A[x_1, \dots, x_n]$ *е полином на* n *променливи с коефициенти от* A*. Наричаме*

$$i_k = \deg_{x_k} u \text{ - степен на } u \text{ относно } x_k,$$
$$i_1 + \dots + i_n = \deg u \text{ - степен на } u,$$
$$\deg f = \max_{\forall u \in f}\{\deg u\} \text{ - степен на } f,$$
$$\deg_{x_k} f = \max_{\forall u \in f}\{\deg_{x_k} u\} \text{ - степен на } f \text{ относно } x_k,$$
$$f = 0 \quad \Rightarrow \deg f = -\infty.$$

Ще дефинираме старши едночлен на полином с n променливи. За съжаление, ако решим да направим аналогия с полином на една променлива веднага се натъкваме на проблем. Ако $f \in A[x]$, то старшия едночлен е едночлена с максимална степен. При полином на n променливи може да имаме повече от един едночлен с най-висока степен. За целта ще направим **лексикографска наредба на едночлени**.

Лексикографската наредба напомня подреждането на думите в речниците. Наредбата се определя от наредбата на първите букви. Ако те са еднакви разглеждаме вторите и т.н. (Алгебра, Алжир, Беда, Изпит).

Дефиниция 16.4

Нека

$$u = aX^I = ax_1^{i_1} \dots x_n^{i_n},\ a \in A$$
$$v = bX^J = bx_1^{j_1} \dots x_n^{j_n},\ b \in A$$

са два неподобни едночлена. Лексикографски $u > v$, *ако* $\exists k,\ k \in \mathbb{N} : k \leq n$ *такова, че*

$$i_1 = j_1, \dots, i_{k-1} = j_{k-1},\ \text{но } i_k > j_k.$$

ПРИМЕРИ:

- $f(x_1, x_2, x_3) = x_1^5 + x_1x_2x_3 + x_1^2x_2^2x_3^3 \Rightarrow \deg f = 7, \deg_{x_1} f = 5, \deg_{x_2} f = 2, \deg_{x_3} f = 3.$
- $f(x_1, x_2, x_3, x_4) = x_1^2 + x_1x_2^2x_3x_4^5 + x_2^2x_3^5x_4^2 + x_2^2x_3^5x_4$
- $x_1 > x_2^3x_3^4 > x_2^3x_3 > x_2^2x_4^2$

Дефиниция 16.5: Старшия едночлен

Нека $f \in A[x_1, \dots, x_n]$ *и* $f \neq 0$. ***Старши член на*** f *се нарича лексикографски максималния едночлен и се бележи с* $LT(f)$ *(leading term).*

Лема 16.6: Лема за старшия едночлен

Нека A *е област и* $f, g \in A[x_1, \dots, x_n]$ *са два ненулеви полинома на* n *променливи. Тогава*

$$LT(fg) = LT(f)LT(g).$$

Доказателство. Нека

$$u = LT(f) = ax_1^{i_1} \dots x_n^{i_n},\ 0 \neq a \in A$$
$$v = LT(g) = bx_1^{j_1} \dots x_n^{j_n},\ 0 \neq b \in A$$

са старшите едночлени на полиномите f и g. Тогава

$$uv = abx_1^{i_1+j_1} \dots x_n^{i_n+j_n}.$$

Ще докажем, че $LT(fg) = u.v$. Нека

$$u' = a'x_1^{i'_1} \dots x_n^{i'_n},$$
$$v' = b'x_1^{j'_1} \dots x_n^{j'_n}$$

са произволни едночлени на полиномите f и g. Ако не са изпълнени едновременно равенствата $u = u'$ и $v = v'$, то

$$uv > u'v'.$$

- Нека $u \neq u'$ и $v \neq v' \Rightarrow u > u', v > v'$. Тогава $\exists k, s \in \mathbb{N},\ (1 \leq k, s \leq n)$ такива, че:

$$i_1 = i'_1, \ldots, i_{k-1} = i'_{k-1},\ \text{но}\ i_k > i'_k,$$
$$j_1 = j'_1, \ldots, j_{s-1} = j'_{s-1},\ \text{но}\ j_s > j'_s.$$

  Ако $k \leq s$, то

$$i_1 + j_1 = i'_1 + j'_1, \ldots, i_{k-1} + j_{k-1} = i'_{k-1} + j'_{k-1},\ \text{но}\ i_k + j_k > i'_k + j'_k \Rightarrow uv > u'v'.$$

- Аналогично се разглеждат и случаите за $u = u'$ или $v = v'$.

□

16.1 Симетрични полиноми

Дефиниция 16.7

Нека $f \in A[x_1, \ldots, x_n]$ е полином на n променливи. Полиномът f се нарича ***симетричен****, ако за произволна пермутация $\sigma \in S_n$ е в сила равенството:*

$$f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Ако f и g са симетрични полиноми, то

$$f + g,\ f - g \text{ и } fg,\ \text{са симетрични полиноми.}$$

Следователно

$$\left\{ f \in A[x_1, \ldots, x_n] \mid f \text{ е симетричен полином} \right\} \leq A[x_1, \ldots, x_n]$$

е подпръстен на $A[x_1, \ldots, x_n]$.
Нека f е симетричен полином. Тогава от равенството

$$f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

следва, че заедно с едночлена

$$ax_1^{k_1} \ldots x_n^{k_n}$$

полиномът f съдържа всички едночлени от вида

$$ax_{\sigma(1)}^{k_1} \ldots x_{\sigma(n)}^{k_n}.$$

Ако $u = LT(f) = ax_1^{k_1} \ldots x_n^{k_n} \Rightarrow k_1 \geq k_2 \geq \cdots \geq k_n$.

Дефиниция 16.8

Тези полиноми се наричат ***елементарни симетрични полиноми.***

$$\begin{aligned}
\sigma_1 &= \sigma_1(x_1,\dots,x_n) = x_1 + x_2 + \dots + x_n,\\
\sigma_2 &= \sigma_2(x_1,\dots,x_n) = x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n,\\
\sigma_3 &= \sigma_3(x_1,\dots,x_n) = x_1x_2x_3 + x_1x_2x_4 + \dots + x_{n-2}x_{n-1}x_n,\\
&\dots\\
\sigma_n &= \sigma_n(x_1,\dots,x_n) = x_1x_2\dots x_n.
\end{aligned}$$

Нека F е поле, $f = a_0x^n + \dots + a_n \in F[x]$ и $\alpha_1, \alpha_2, \dots, \alpha_n$ са всички корени на f. Тогава формулите на Виет се записват по следния начин:

$$\sigma_k(\alpha_1,\dots,\alpha_n) = (-1)^k\frac{a_k}{a_0},\ k = 1,2,\dots,n.$$

Ако $g(x_1,\dots,x_n) \in A[x_1,\dots,x_n]$ е произволен полином на n променливи, то

$$g\big(\sigma_1,\dots,\sigma_n\big)$$

е симетричен полином на n променливи. (Сума, разлика, произведение на симетрични полиноми е симетричен полином). Вярно е и обратното!

Теорема 16.9: Основна теорема за симетричните полиноми

Нека A е област и $f = f(x_1,\dots,x_n) \in A[x_1,\dots,x_n]$ е симетричен полином. Тогава съществува единствен полином $g \in A[x_1,\dots,x_n]$, такъв че

$$f(x_1,\dots,x_n) = g\big(\sigma_1,\dots,\sigma_n\big).$$

Доказателство. 1. **Съществуване.** Ако

$$u = LT(f) = ax_1^{k_1}\dots x_n^{k_n} \quad \Rightarrow \quad k_1 \geq k_2 \geq \dots \geq k_n.$$

Да разгледаме полинома:

$$\varphi_1 = a\ \sigma_1^{k_1-k_2}\ \sigma_2^{k_2-k_3}\ \dots\ \sigma_{n-1}^{k_{n-1}-k_n}\ \sigma_n^{k_n},$$

т.к. φ_1 е едночлен на симетрични полиноми, следователно φ_1 е симетричен полином на $x_1, x_2, \dots, x_n$.

Да разгледаме старшите едночлени на :

$$\begin{aligned} & LT \\ \sigma_1 \ &\to x_1 \\ \sigma_2 \ &\to x_1x_2 \\ \sigma_3 \ &\to x_1x_2x_3 \\ & \dots \\ \sigma_n \ &\to x_1x_2\dots x_n \end{aligned}$$

От Лема 16.6 следва, че старшия едночлен на φ_1 е произведение на старшите едночлени на $\sigma_1, \dots \sigma_n$, т.е.

$$\begin{aligned} LT(\varphi_1) &= a\ (x_1)^{k_1-k_2}\ (x_1x_2)^{k_2-k_3}\ \dots\ (x_1x_2\dots x_{n-1})^{k_{n-1}-k_n}\ (x_1x_2\dots x_n)^{k_n} \\ &= a\ x_1^{k_1}\ x_2^{k_2}\ \dots\ x_n^{k_n}. \end{aligned}$$

$\Rightarrow f_1 = f - \varphi_1 \in A[x_1, \dots, x_n]$ е симетричен полином и $LT(f_1) < LT(f)$.

Ако $f_1 \neq 0$ продължаваме по същия път, докато не получим нулев полином, т.е.

$$\begin{aligned} f_1 &= f - \varphi_1 \\ f_2 &= f_1 - \varphi_2 \\ &\dots \\ f_{s-1} &= f_{s-2} - \varphi_{s-1} \\ 0 = f_s &= f_{s-1} - \varphi_s \end{aligned} \tag{1}$$

Всички получени полиноми са симетрични на n промеливи и старшия им едночлен на всеки следващ полином е по-малък от предишния. Този процес не може да бъде безкраен. Ако

$$LT(f_k) = bx_1^{l_1} \dots x_n^{l_n} \quad \Rightarrow \quad k_1 \geq l_1 \geq l_2 \geq \dots \geq l_n,$$

за някое k, то броят на всички различни n-орки е ограничен отгоре - $(k_1+1)^n$.

От (1) получаваме, че $f = \varphi_1 + \dots \varphi_s$. Но φ_i са едночлени на $\sigma_1, \dots, \sigma_n$ с коефициенти от $A \Rightarrow f$ е полином на $\sigma_1, \dots, \sigma_n$ с коефициенти от A, т.е.

$$f(x_1, \dots, x_n) = g\big(\sigma_1, \dots, \sigma_n\big).$$

2. **Единственост.**

Нека

$$\begin{aligned} g_1 &= g_1(y_1, \dots, y_n) \in A[y_1, \dots, y_n] \\ g_2 &= g_2(y_1, \dots, y_n) \in A[y_1, \dots, y_n] \\ &\text{са такива, че} \\ f(x_1, \dots, x_n) &= g_1(\sigma_1, \dots, \sigma_n) = g_2(\sigma_1, \dots, \sigma_n). \end{aligned}$$

Да разгледаме полинома:

$$g = g(y_1, \ldots, y_n) = g_1(y_1, \ldots, y_n) - g_2(y_1, \ldots, y_n)$$
$$\Rightarrow g(\sigma_1, \ldots, \sigma_n) = 0.$$

Ще докажем, че $g(y_1, \ldots, y_n) = 0 \Rightarrow g_1(y_1, \ldots, y_n) = g_2(y_1, \ldots, y_n)$.
Индукция по n.

- $n = 1$
$$\sigma_1 = x_1 \Rightarrow g(x_1) = 0 \Rightarrow g(y_1) = 0.$$
- ИП. Нека твърдението е вярно за полином на $n-1$ променливи.
- n

  Да допуснем, че съществува полином на n променливи $g(y_1, \ldots, y_n)$ такъв, че

$$g(\sigma_1, \ldots, \sigma_n) = 0 \text{ като полином на } x_1, \ldots x_n$$
$$g(y_1, \ldots, y_n) \neq 0 \text{ като полином на } y_1, \ldots, y_n.$$

  Измежду всички такива избираме полинома g с най-ниска степен.

$$g \in A[y_1, \ldots, y_n] = A[y_1, \ldots, y_{n-1}][y_n],$$

  $\Rightarrow g$ е полином на y_n с коефициенти от $A[y_1, \ldots, y_{n-1}]$, т.е.

$$g(y_1, \ldots, y_n) = g_0(y_1, \ldots, y_{n-1}) + g_1(y_1, \ldots, y_{n-1})y_n + \cdots + g_k(y_1, \ldots, y_{n-1})y_n^k$$

  (1) $g_0(y_1, \ldots, y_{n-1}) = 0$
  $\Rightarrow g(y_1, \ldots, y_n) = y_n h(y_1, \ldots, y_n)$, т.е. $g = y_n h$, $h \neq 0$, защото $g \neq 0$ и $\deg h = \deg g - 1$.

$$0 = g(\sigma_1, \ldots, \sigma_n) = \sigma_n . h(\sigma_1, \ldots, \sigma_n)$$

  Тъй като $A[x_1, \ldots, x_n]$ е област и $\sigma_n = x_1 \ldots x_n \neq 0$ следва, че

$$h(\sigma_1, \ldots, \sigma_n) = 0.$$

  Но $h(y_1, \ldots, y_n) \neq 0$, $h(\sigma_1, \ldots, \sigma_n) = 0$ и $\deg h < \deg g$ - противоречие с избора на g.

  (2) $g_0(y_1, \ldots, y_{n-1}) \neq 0$

$$0 = g(\sigma_1, \ldots, \sigma_n) = \tag{2}$$
$$= g_0(\sigma_1, \ldots, \sigma_{n-1}) + g_1(\sigma_1, \ldots, \sigma_{n-1})\sigma_n + \cdots + g_k(\sigma_1, \ldots, \sigma_{n-1})\sigma_n^k$$

Да положим $x_n = 0$. Тогава

$$\sigma_n = 0,$$
$$\sigma_i^0 = \sigma_i(x_1, \ldots, x_{n-1}, 0),\ i = 1, \ldots, n-1,$$

това са елементарните симетрични полиноми на $x_1, \ldots x_{n-1}$.

От (2) имаме, че $g_0(\sigma_1^0, \ldots, \sigma_{n-1}^0) = 0$ и от ИП $\Rightarrow g_0(y_1, \ldots, y_{n-1}) = 0$, което е противоречие с допускането, че $g_0(y_1, \ldots, y_{n-1}) \neq 0$.

Следователно допускането, че $g(y_1, \ldots, y_n) \neq 0$ не е вярно.

□

Следствие 16.10

Нека F е поле, $f = a_0x^n + \cdots + a_n \in F[x]$ и $\alpha_1, \ldots, \alpha_n$ са всички корени на f ($\alpha_i \in L \geq F$). Тогава, ако

$$h(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$$

е симетричен полином, то

$$h(\alpha_1, \ldots, \alpha_n) \in F.$$

Доказателство. Нека $g(y_1, \ldots, y_n)$ е полином с коефициенти от F, за който

$$h(x_1, \ldots, x_n) = g\big(\sigma_1, \ldots, \sigma_n\big).$$

Тогава

$$h(\alpha_1, \ldots, \alpha_n) = g\Big(\sigma_1\big(\alpha_1, \ldots, \alpha_n\big), \ldots, \sigma_n\big(\alpha_1, \ldots, \alpha_n\big)\Big).$$

Но

$$\sigma_k\big(\alpha_1, \ldots, \alpha_n\big) = (-1)^k \frac{a_k}{a_0} \in F, k = 1, \ldots, n$$

следователно $h(\alpha_1, \ldots, \alpha_n) \in F$. □

16.2 Формули на Нютон

Нека $ax_1^{i_1}x_2^{i_2} \ldots x_n^{i_n}$ е едночлен на променливите $x_1, x_2, \ldots, x_n$.

Дефиниция 16.11

Симетричната сума

$$S = \sum ax_1^{i_1}x_2^{i_2} \ldots x_n^{i_n}$$

е сумата на всички различни едночлени, които се получават от едночлена $ax_1^{i_1}x_2^{i_2} \ldots x_n^{i_n}$ при прилагането на всевъзможните пермутации на променливите $x_1, x_2, \ldots, x_n$.

Например ($n = 3$):

$$\sum x_1^3 x_2 = x_1^3 x_2 + x_1^3 x_3 + x_2^3 x_1 + x_2^3 x_3 + x_3^3 x_1 + x_3^3 x_2$$

Дефиниция 16.12

Симетричните полиноми

$$S_k = \sum x_1^k = x_1^k + x_2^k + \cdots + x_n^k, \quad k = 0, 1, 2, \ldots$$

степенни сборове. *По определение* $S_0 = n$.

$$\begin{aligned} S_1 &= \sigma_1 \\ S_2 &= \sigma_1^2 - 2\sigma_2 \\ &\Rightarrow S_2 - \sigma_1 S_1 + 2\sigma_2 = 0. \end{aligned}$$

При $3 \leq k \leq n$ имаме:

$$\begin{aligned} \sigma_1 S_{k-1} &= S_k + \sum x_1^{k-1} x_2 \\ \sigma_i S_{k-i} &= \sum x_1^{k-i+1} x_2 \ldots x_i + \sum x_1^{k-i} x_2 \ldots x_i x_{i+1} \text{ при } 1 \leq i \leq k-2 \\ \sigma_{k-1} S_1 &= \sum x_1^2 x_2 \ldots x_{k-1} + k\sigma_k \end{aligned}$$

Като умножим i-тото равенство по $(-1)^i$ $(i = 1, \ldots, k-1)$ и съберем, получаваме равенството

$$S_k - \sigma_1 S_{k-1} + \sigma_2 S_{k-2} + \cdots + (-1)^{k-1} \sigma_{k-1} S_1 + (-1)^k k\sigma_k = 0. \tag{1}$$

Ако положим $\sigma_i = 0$ при $i > n$, то равенството остава в сила. Формулите (1) се наричат **формули на Нютон**.

Нека F е поле, $f = x^n + a_1 x^{n-1} + \cdots + a_n \in F[x]$ и $\alpha_1, \ldots, \alpha_n$ са всички корени на f. От формулите на Виет, можем да запишем формулите на Нютон

$$S_k + a_1 S_{k-1} + a_2 S_{k-2} + \cdots + a_{k-1} S_1 + k a_k = 0.$$

При $i > n$ считаме, че $a_i = 0$.

Глава 17

Теорема на Даламбер (основна теорема на алгебрата)

Дефиниция 17.1: Алгебрически затворено поле

*Едно поле F е **алгебрически затворено**, ако всеки неконстантен полином с коефициенти от F има корен в F.*

Твърдение 17.2

Полето F е алгебрически затворено $\Leftrightarrow$ всеки неконстантен полином $f \in F[x]$ се разлага на линейни множители над F.

Доказателство. $\Leftarrow$) Ако неконстантния полином $f \in F[x]$ се разлага на линейни множители над F, т.е.

$$f = a_0 \prod_{i \in I} (x - \alpha_i),\ a_0, \alpha_i \in F,$$

то f има корен в F и F е алгебрически затворено поле.

$\Rightarrow$) Нека F е алгебрически затворено поле. Индукция по степента на $f \in F[x]$.

- $\deg(f) = 1$ - ясно.
- ИП за $\deg(f) \leq n - 1$
- $\deg(f) = n$. Тогава съществува корен $\alpha \in F$ на $f \Rightarrow \exists g \in F[x],\ \deg(g) = n-1\ :\ f = (x-\alpha)g$. По ИП следва, че g се разлага на линейни множители над F, откъдето следва, че и f се разлага на линейни множители над F.

□

ПРИМЕРИ:

- $\mathbb{Q}$ и $\mathbb{R}$ не са алгебрически затворени. Полиномът x^2+1 няма рационален и реален корен.
- $\mathbb{Z}_p$ не е алгебрически затворено. $f = x^p - x + \overline{1}$ няма корен в $\mathbb{Z}_p$. ($\alpha \in \mathbb{Z}_p \Rightarrow f(\alpha) = \alpha^p - \alpha + \overline{1} = \overline{1} \neq 0$).
- Ако K е крайно поле и $a_1, \ldots, a_n$ са всички елементи на полето K, то полиномът
$$f = \prod_{i=1}^{n}(x - a_i) + 1$$
няма корен в $K \Rightarrow K$ не е алгебрически затворено.

Лема 17.3: Лема на Гаус

Всеки неконстантен полином с реални коефициенти има поне един комплексен корен.

Доказателство. Нека $f = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{R}[x]$, $\deg(f) = n > 0$, $n = 2^k m$, $k \geq 0$ и $m \in \mathbb{N}$ е нечетно число.
Индукция по k - степента на 2 в $\deg(f)$.

- $k = 0 \Rightarrow$ полиномът f е от нечетна степен, т.е. $n = m$. Понеже корените на полиномите f и $\frac{f}{a_0}$ са едни и същи можем да считаме, че $a_0 = LC(f) > 0$. Тогава
$$\lim_{x\to\pm\infty} f = \lim_{x\to\pm\infty}(a_0x^m + a_1x^{m-1} + \cdots + a_m) = \pm\infty$$
От анализа следва, че една непрекъсната функция $f : \mathbb{R} \to \mathbb{R}$ от $-\infty$ до ∞ пресича оста Ox и уравнението $f = 0$ има реален корен.
- ИП - нека $k > 0$ и твърдението е вярно за $k-1$.
- k

  Нека $\deg(f) = n = 2^k m$, L е полето на разлагане на f над $\mathbb{C}$ и $\alpha_1, \ldots, \alpha_n \in L$ са всички корени на полинома f. За произволно фиксирано реално число r да разгледаме
$$\beta_{ij} = \beta_{ij}(r) = \alpha_i\alpha_j + r(\alpha_i + \alpha_j), \quad 1 \leq i < j \leq n. \tag{1}$$
  Да разгледаме полинома
$$g_r(x) = \prod_{1\leq i<j\leq n}(x - \beta_{ij}) \in L[x].$$
  Броят на елементите β_{ij}, както и $\deg(g)$ е равна на
$$n' = \binom{n}{2} = \frac{n(n-1)}{2} = \frac{2^k m(2^k m - 1)}{2} = 2^{k-1}m_0,$$

където m_0 е нечетно число. Нека

$$g_r(x) = x^{n'} + c_1 x^{n'-1} + \cdots + c_0.$$

Ще покажем, че $g_r(x) \in \mathbb{R}[x]$ има реални коефициенти.

От формулите на Виет, коефициентите c_k са с точност до знак елементарните симетрични полиноми на корените $\{\beta_{ij}\}$ на полинома $g_r(x)$, т.е.

$$c_k = (-1)^k \, \sigma_k\big(\beta_{11}, \beta_{12}, \ldots, \beta_{n-1,n}\big).$$

Заместваики β_{ij} чрез $\alpha_1, \ldots, \alpha_n$ от (1) получаваме, че коефициентите на $g_r(x)$ са полиноми на $\alpha_1, \ldots, \alpha_n$,

$$c_k = c_k(\alpha_1, \ldots, \alpha_n) = (-1)^k \, \sigma_k\big(\ldots, \alpha_i\alpha_j + r(\alpha_i + \alpha_j), \ldots\big)$$

и освен това са **симетрични полиноми** на $\alpha_1, \ldots, \alpha_n$ с коефициенти от $\mathbb{R}$. Това е така, защото всяка пермутация $\tau \in S_n$ индуцира пермутация $\overline{\tau}$, действаща върху множеството $\{\beta_{ij}\}$ по следния начин:

$$\overline{\tau}(\beta_{ij}) = \alpha_{\tau(i)}\alpha_{\tau(j)} + r(\alpha_{\tau(i)} + \alpha_{\tau(j)}) = \beta_{\tau(i)\tau(j)}$$

(или $\beta_{\tau(j)\tau(i)}$,ако $\tau(i) > \tau(j)$) и следователно

$$\begin{aligned}
\tau\Big(c_k(\alpha_1, \ldots, \alpha_n)\Big) &= (-1)^k \, \sigma_k\Big(\tau(\beta_{11}), \tau(\beta_{12}), \ldots, \tau(\beta_{n-1,n})\Big) \\
&= (-1)^k \, \sigma_k\Big(\beta_{11}, \beta_{12}, \ldots, \beta_{n-1,n}\Big) \\
&= c_k(\alpha_1, \ldots, \alpha_n) \\
&\quad (\sigma_k \text{ е симетричен полином}).
\end{aligned}$$

Така получихме, че коефициентите c_k на $g_r(x)$ са симетрични полиноми на $\alpha_1, \ldots, \alpha_n$ с коефициенти от $\mathbb{R}$. Припомняме, че $\alpha_1, \ldots, \alpha_n$ са корени на полинома f с реални коефициенти. От основната теорема за симетрични полиноми следва, че симетричния полином $c_k \in \mathbb{R}[\alpha_1, \ldots, \alpha_n]$ е полином на елементарните симетрични полиноми на $\sigma_1, \ldots, \sigma_n$, т.е.

$$c_k(\alpha_1, \ldots, \alpha_n) = h\Big(\sigma_1(\alpha_1, \ldots, \alpha_n), \ldots, \sigma_n(\alpha_1, \ldots, \alpha_n)\Big)$$

и $\sigma_l(\alpha_1, \ldots, \alpha_n) = (-1)^l \dfrac{a_l}{a_0} \in \mathbb{R}$, $l = 1, 2, \ldots, n$. Тогава от Следствие 16.10 имаме, че коефициентите на $g_r(x)$ са реални числа.

Доказахме, че коефициентите на $g_r(x)$ са реални числа, т.е. $g_r(x) \in \mathbb{R}[x]$. Тъй като $\deg(f) = n' = 2^{k-1}m_0$, от от ИП (обърнете внимание - индукция е малко по-странна, по степента на 2 в степента на полинома и въпреки, че $\deg(g_r) > \deg(f), n > 3$, то ИП за g_r важи!!!) следва, че $g_r(x)$ има поне един комплексен корен, който разбира се е един от β_{ij}.

Като меним реалния параметър r ще получаваме полиноми $g_r(x)$ с реални коефициенти. На всеки от тях съответства такава двойка индекси (i,j), $i<j$ (зависеща от r) такава, че елементът

$$\beta_{ij} = \beta_{ij}(r) = \alpha_i\alpha_j + r(\alpha_i+\alpha_j) \in \mathbb{C}.$$

Тъй като различните двойки индекси $i<j$ са само $\binom{n}{2}$, а реалните числа са безбройно много, то може да се намерят две различни реални числа r_1 и r_2, на които да отговаря една съща двойка индекси, за които

$$\begin{aligned}\beta_{ij}(r_1) &= \alpha_i\alpha_j + r_1(\alpha_i+\alpha_j) \quad \in \mathbb{C}\\ \beta_{ij}(r_2) &= \alpha_i\alpha_j + r_2(\alpha_i+\alpha_j) \quad \in \mathbb{C}\end{aligned}$$

са комплексни числа. От където намираме

$$\begin{aligned}\alpha_i+\alpha_j &= \frac{\beta_{ij}(r_1)-\beta_{ij}(r_2)}{r_1-r_2} \quad \in \mathbb{C}\\ \alpha_i\alpha_j &= \beta_{ij}(r_1) - r_1\frac{\beta_{ij}(r_1)-\beta_{ij}(r_2)}{r_1-r_2} \quad \in \mathbb{C}.\end{aligned}$$

Следователно полиномът

$$x^2 - (\alpha_i+\alpha_j)x + \alpha_i\alpha_j \quad \in \mathbb{C}[x]$$

е с комплексни коефициенти и корените му са α_i и α_j. От формулата за корените на квадратно уравнение, следва, че α_i и α_j са комплексни числа. Следователно $f(x)$ има комплексен корен, което трябваше да се докаже.

□

Теорема 17.4: Основна теорема на алгебрата - теорема на Даламбер

Полето на комплексните числа $\mathbb{C}$ е алгебрически затворено.

Доказателство. Нека

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \quad \in \mathbb{C}[x]$$

е неконстантен полином с комплексни коефициенти. Дефинираме комплексно спрегнатия на $f(x)$ полином ппо следния начин

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

Да разгледаме полинома

$$F(x) = f(x)\overline{f(x)} = b_0x^{2n} + b_1x^{2n-1} + \cdots + b_{2n},$$

където

$$b_k = \sum_{i+j=k} a_i \overline{a_j}, \quad (k = 0, 1, \dots 2n).$$

Ще покажем, че $F(x) \in \mathbb{R}[x]$ е полином с реални коефициенти. За целта трябва да докажем, че $F(x) = \overline{F(x)}$ или $b_k = \overline{b_k}$.

$$\overline{b_k} = \overline{\sum_{i+j=k} a_i \overline{a_j}} = \sum_{i+j=k} \overline{a_i \overline{a_j}} = \sum_{i+j=k} \overline{a_i} a_j = b_k.$$

$\Rightarrow b_k \in \mathbb{R}$.

От лемата на Гаус следва, че $F(x) \in \mathbb{R}[x]$ има комплексен корен β и

$$F(\beta) = f(\beta)\overline{f}(\beta) = 0.$$

Следователно $f(\beta) = 0$ или $\overline{f}(\beta) = 0$. Ако $f(\beta) = 0$, то теоремата е доказана.

Нека

$$\overline{f}(\beta) = \overline{a_0}\beta^n + \overline{a_1}\beta^{n-1} + \dots + \overline{a_n} = 0.$$

Да разгледаме комплексно спрегнатото на горното равенство

$$\begin{aligned} 0 = \overline{\overline{f}(\beta)} &= \overline{\overline{a_0}\beta^n + \overline{a_1}\beta^{n-1} + \dots + \overline{a_n}} \\ &= a_0\overline{\beta}^n + a_1\overline{\beta}^{n-1} + \dots + a_n \\ &= f(\overline{\beta}). \end{aligned}$$

Тогава $\overline{\beta}$ е комплексен корен на $f(x)$.

□

Единствените неразложими полиноми над $\mathbb{C}$ са полиномите от първа степен.

От основната теорема на алгебрата следва, че всеки полином f от n-та степен и с комплексни коефициенти може да бъде записан, и то по единствен начин (с точност до разместване на множителите), във вида

$$f(x) = a_0(x - c_1)(x - c_2)\dots(x - c_n),$$

където $a_0 \neq 0$ и $c_1, \dots, c_n$ са комплексни числа.

Ще покажем, че единствените неразложими полиноми с реални коефициенти над $\mathbb{R}$ са полиномите от първа степен и полиномите от 2-ра степен с отрицателна дискриминанта.

Твърдение 17.5

Нека $f(x) \in \mathbb{R}[x]$ и $\deg(f) > 0$. Тогава $f(x)$ се разлага над $\mathbb{R}$ в произведение

$$f(x) = a_0 \prod_{i=1}^{m}(x - \gamma_i) \prod_{j=1}^{l}(x^2 + u_j x + v_j)$$

на линейни множители $(x-\gamma_i) \in \mathbb{R}[x]$ и квадратни тричлени $(x^2+u_jx+v_j) \in \mathbb{R}[x]$ с отрицателна дискриминанта $D(x^2 + u_jx + v_j) < 0$.
Това представяне е (единственото с точност до константа от $\mathbb{R}$) представяне на f като произведение на неразложими над $\mathbb{R}$ полиноми.

Доказателство. Нека

$$f(x) = a_0 \prod_{i=1}^{n}(x - \gamma_i)$$

е разлагането на $f(x)$ на линейни множители над $\mathbb{C}$. Нека $\gamma_1, \dots \gamma_m$ са реалните корени на $f(x)$, а $\gamma_{m+1}, \dots \gamma_n$ са комплексните нереални корени на $f(x)$. Тогава

$$f = \prod_{i=1}^{m}(x - \gamma_i)g,$$

като $g = b_0x^k + \dots + b_k$ е полином с реални коефициенти и g няма реални корени.
Нека $\gamma = a+bi \in \mathbb{C}\, a, b \in \mathbb{R}$ е комплексен корен на $g(x)$ следователно $\overline{\gamma} = \overline{a + bi} = a-bi$ също е комплексен корен на $g(x)$. Да приложим комплексното спрягане

$$\begin{aligned} 0 = \overline{0} = \overline{g(\gamma)} &= \overline{b_0\gamma^k + b_1\gamma^{k-1} + \dots + b_k} \\ &= b_0\overline{\gamma}^k + b_1\overline{\gamma}^{k-1} + \dots + b_k \\ &= g(\overline{\gamma}) \end{aligned}$$

и вземем предвид, че $b_i = \overline{b_i}$, защото са реални числа. Тогава полиномът

$$h(x) = (x - \gamma)(x - \overline{\gamma}) = x^2 - (\gamma + \overline{\gamma})x + \gamma\overline{\gamma} = x^2 - 2ax + (a^2 + b^2)$$

е с реални коефициенти, $h(x)/g(x)$ и дискриминантата му е отрицателна $D = -4b^2 < 0$.
Продължаваме по същия начин:

$$g = hs,\ s \in \mathbb{R}[x].$$

Ако $\deg(s) > 0$ аналогично разъждаваме, докато g се представи като произведение на полиноми от 2-ра степен с отрицателни дискриминанти. □

Глава 18

Крайни полета.

Дефиниция 18.1

Поле с краен брой елементи се нарича ***крайно поле****. Нарича се още и* ***поле на Галоа****.*

Теорема 18.2

Нека F е крайно поле с характеристика $charF = p$.

(a) Всяко крайно поле F има крайна характеристика $p > 0$.

(b) Броят на елементите на полето F е степен на характеристиката, т.е. $|F| = p^n$.

(c) Елементите на F се изчерпват с корените на уравнението $x^q = x$, където $q = |F|$.

Доказателство. (a) Ако $char\, F = 0$, то $n1 \neq m1$ за всеки естествени $n \neq m$, което противоречи на $|F| < \infty$. Следователно $char\, F = p > 0$.

(b) Ако $charF = p$, то F съдържа $\mathbb{Z}_p$ като просто подполе. Може да разглеждаме F като линейно пространство над $\mathbb{Z}_p$. Нека размерността на F над $\mathbb{Z}_p$ е n, т.е. $\dim_{\mathbb{Z}_p} F = n$ и $e_1, \ldots, e_n$ е базис на F над $\mathbb{Z}_p$. Тогава всеки елемент се записва и то по единствен начин като линейна комбинация

$$a = \gamma_1 e_1 + \ldots \gamma_n e_n.$$

Броят на всички такива линейни комбинации е $|F| = p^n$.

(c) Мултипликативната група на полето $F^* = F \setminus \{0\}$ се състои от $p^n - 1$ елемента. Но тогава за всеки елемент $\alpha \in F^\star$ е изпълнено

$$\alpha^{p^n - 1} = 1.$$

Следователно $\alpha^{p^n} = \alpha$, за всяко $\alpha \in F$ (включително нулевия елемент), т.е. елементите на F изчерпват корените на $x^{|F|} = x$.

□

Теорема 18.3

За всяко просто число p и всяко естествено число n съществува единствено с точност до изоморфизъм поле с p^n елемента.

Доказателство. 1. **Съществуване.**

Нека F е полето на разлагане на полинома $f(x) = x^{p^n} - x$ над Z_p. Да разгледаме множеството от корените на полинома $f(x)$ и да го означим с

$$F_0 = \{\alpha \in F \mid f(\alpha) = 0\} = \{\alpha \in F \mid \alpha^{p^n} = \alpha\} \subseteq F.$$

Тогава F_0 е подполе на F. Наистина, ако $\alpha, \beta \in F_0$, т.е. $\alpha^{p^n} = \alpha, \beta^{p^n} = \beta \Rightarrow$

$$(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta,$$

и при $\beta \neq 0 \Rightarrow$

$$(\alpha\beta^{-1})^{p^n} = \alpha^{p^n}\beta^{-p^n} = \alpha\beta^{-1}.$$

Да отбележим, че полиномът $f(x)$ няма кратни корени, т.е. всичките му корени са прости. Това е така, защото $f(x)$ няма общ корен с производната си ($f'(x) = p^n x^{p^n-1} - 1 = -1 \neq 0$). Така F_0 е поле, съдържащо всички корени на $x^{p^n} - x = 0$, откъдето и минималността на полето на разлагане следва, че $F = F_0$. Следователно $|F| = p^n$.

2. **Единственост.**

Нека F_1 и F_2 са две полета с по p^n елемента. Всяко поле с p^n елемента има характеристика p (защо?).

От теорема 18.2 (c) следва, че всеки елемент на поле с p^n елемента е корен на полинома $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Така, че F_1 и F_2 съвпадат с множеството от корените на f ($|F_1| = |F_2| = \deg(f) = p^n$) и съдържат $\mathbb{Z}_p$. Така F_1 и F_2 са полета на разлагане на f над $\mathbb{Z}_p$.

От теоремата за единственост на полето на разлагане всеки две такива полета са изоморфни, т.е. $F_1 \cong F_2$.

□

Така показахме, че единственото с точност до изоморфизъм крайно поле с p^n елемента е полето на Галоа и бележим с $GF(p^n)$ ($GF(p) = \mathbb{Z}_p$).

Лема 18.4

Нека G е група и a, b са елементи на G, с редове съответно r и s и $ab = ba$, т.е. комутират помежду. Тогава:

(a) ако $(r, s) = 1$, то елементът ab има ред rs,

(b) в G има елемент от ред $[r, s]$.

Доказателство. (a) $ab = ba$, $|a| = r, |b| = s$ и $(r, s) = 1$, то $|ab| = rs$. Нека $|ab| = t$.

- От $ab = ba \Rightarrow (ab)^{rs} = a^{rs}b^{rs} = 1 \Rightarrow t \mid rs$.
- От $(ab)^t = 1 \Rightarrow a^t b^t = 1 \Rightarrow a^{ts}b^{ts} = 1 \Rightarrow r \mid ts$, $(r, s) = 1 \Rightarrow r \mid t$. Аналогично $s \mid t$. Понеже $(r, s) = 1 \Rightarrow rs \mid t$.

Така $t = rs$.

(b) Нека

$$r = p_1^{k_1} \dots p_m^{k_m}, \quad k_i \geq 0,\ i = 1, \dots, m$$
$$s = p_1^{l_1} \dots p_m^{l_m}, \quad l_i \geq 0,\ i = 1, \dots, m$$

където $p_1, \dots, p_m$ са различни прости числа.

Ако $u_i = max(k_i, l_i),\ i = 1, \dots, m$, то

$$[r, s] = p_1^{u_1} \dots p_m^{u_m}.$$

В G има елемент от ред $p_i^{u_i}$: $c_i = \begin{cases} a^{p_i^{r/k_i}}, \text{ или} \\ b^{p_i^{s/l_i}}. \end{cases}$ Числата и са две по две взаимно прости. От (a) получаваме, че елементът $c = c_1 \dots c_m$ има ред $[r, s]$.

□

Теорема 18.5

Всяка крайна подгрупа G на мултипликативната група $F^\star$ на едно поле F е циклична.

Доказателство. Нека G е крайна група и $a \in G$ е такъв, че редът му $|a| = r$ е максимален. Нека $b \in G$ е произволен и $|b| = s$. Ще покажем, че $|b| \mid |a|$, т.е. $s \mid r$. Нека $p_1, \dots, p_m$ са различни прости числа

$$r = p_1^{k_1} \dots p_m^{k_m}, \quad k_i \geq 0,\ i = 1, \dots, m$$
$$s = p_1^{l_1} \dots p_m^{l_m}, \quad l_i \geq 0,\ i = 1, \dots, m$$
$$u_i = max(k_i, l_i),\ i = 1, \dots, m$$
$$\Rightarrow \quad [r, s] = p_1^{u_1} \dots p_m^{u_m}.$$

Ако $s \nmid r \Rightarrow [r,s] > r \Rightarrow \exists c \in G \ : \ |c| = [r,s] > r$, което е противоречие с изобра на a. Следователно $s \mid r$.

За всяко $b \in G$ е изпълнено $b^r = 1 \Rightarrow b$ е корен на полинома $x^r - 1$. Броят на корените $x^r - 1$ от F не надминава $r = \deg(x^r - 1)$.

$$\begin{aligned} & \langle a \rangle \subseteq G \subseteq \{\alpha \in F^\star \mid \alpha^r - 1 = 0\} \\ \Rightarrow \quad & r = |\langle a \rangle| \leq |G| \leq \left|\{\alpha \in F^\star \mid \alpha^r - 1 = 0\}\right| = r \\ \Rightarrow \quad & \langle a \rangle = G = \{\alpha \in F^\star \mid \alpha^r - 1 = 0\}. \end{aligned}$$

Което доказва, че G е циклична група от ред r. □

Следствие 18.6

Мултипликативната група $F^\star$ на всяко крайно поле F е циклична.

Доказателство. $G = F^\star$ е крайна група. □

Дефиниция 18.7

Примитивен елемент *на крайното поле F наричаме всеки образуващ на цикличната група $F^\star$.*

Теорема 18.8

Полето $F = GF(p^n)$ съдържа като подполе $K \cong GF(p^m)$ тогава и само тогава, когато $m \mid n$.

Доказателство. $\Rightarrow$) Нека $K \leq F = GF(p^n)$ е подполе на F. Тогава (от теорема 18.2) следва, че

$$\begin{aligned} & |F| = |GF(p^n)| = |K|^t, \quad t \in \mathbb{N} \\ \Rightarrow \quad & p^n = |K|^t \\ \Rightarrow \quad & |K| = p^m, \text{ за някое } m \in \mathbb{N} \\ \Rightarrow \quad & K \cong GF(p^m) \\ \Rightarrow \quad & p^n = p^{mt} \\ \Rightarrow \quad & m \mid n. \end{aligned}$$

$\Leftarrow$) Нека $m \mid n$. Тогава $(p^n - 1) \mid (p^m - 1)$, откъдето получаваме

$$(x^{p^m-1} - 1) \mid (x^{p^n-1} - 1) \quad \text{т. е.} \quad (x^{p^m} - x) \mid (x^{p^n} - x).$$

да разгледаме

$$K = \{\alpha \in F \mid \alpha^{p^m} = \alpha\}.$$

K е поле с p^m елемента и следователно $GF(p^m) \leq F$.

□

Ще построим полето $GF(2^4)$. Съгласно Теорема 18.3

$$GF(2^4) = \left\{ a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \mid a_i \in \mathbb{Z}_2 \right\} \cong \mathbb{Z}_2[x]/\big(m(x)\big),$$

където $m(x)$ е неразложим над $\mathbb{Z}_2$ полином от степен 4 и α е негов корен. Да изберем $m(x) = x^4 + x + 1$. α се явява примитивен елемент на $GF(2^4)$.

Елементите на полето в мултипликативно (като степен на α) и адитивно представяне (отляво е коефициента a_0) са дадени в таблица 18.

Действията при адитивния запис се извършват като с полиноми на α, но по модул $m(x)$, т.е. при условието $\alpha^4 + \alpha + 1 = 0$. Ако разполагаме с мултипликативния и адитивния запис, по-добре е умножението да се извърши чрез събиране на степените по модул 15, а събирането - с двоичните вектори. Например

$$(\alpha^2 + \alpha^3) + (1 + \alpha^2 + \alpha^3) = 1 \text{ или } 0011 + 1011 = 1000,$$

$$(\alpha^2 + \alpha^3).(1 + \alpha^2 + \alpha^3) = \alpha^6\alpha^{13} = \alpha^{19} = \alpha^4 = 1 + \alpha.$$

Степен на α	Полином от α
0	0000
1	1000
α	0100
α^2	0010
α^3	0001
α^4	1100
α^5	0110
α^6	0011
α^7	1101
α^8	1010
α^9	0101
α^{10}	1110
α^{11}	0111
α^{12}	1111
α^{13}	1011
α^{14}	1001

Таблица 18.1: Елементите на полето $GF(16)$.