Упражнение за циклични групи, нормални групи и фактор групи. Първа теорема за хомоморфизмите

Иво Стратев

14 ноември 2020 г.

Съдържание

1 Подгрупи на циклични групи **3**
1.1 Подгрупи на групата на целите числа 3
1.2 Подгрупи на групата на n-тите корени на единицата . . . 4

2 Съседни класове. Теорема на Лагранж. Нормални подгрупи. Фактор групи **5**
2.1 Мултипликативен запис: 6
2.2 Адитивен запис: 6
2.3 Важни свойства ще ги напишем в мултипликативен запис и само за левите съседни класове (за десните е аналогично) 6
2.4 Теорема на Лагранж 7
2.5 Примери 7
2.5.1 $\mathbb{R}^*$ и $\mathbb{R}^+$ 7
2.5.2 $\mathbb{Z}$ и $6\mathbb{Z}$ 7
2.5.3 $\mathbb{C}_8$ и $\mathbb{C}_4$ 8
2.6 Нормални групи 9
2.6.1 Важни неща 9
2.7 Фактор група 9
2.8 Примери 10
2.8.1 $\mathbb{R}^*$ и $\mathbb{R}^+$ 10
2.8.2 $\mathbb{C}_8$ и $\mathbb{C}_4$ 10
2.8.3 $\mathbb{Z}$ и $6\mathbb{Z}$ 11

3 Една класика от Информатика **11**
3.1 Решение 11

4 Първа теорема за хомоморфизмите **12**

5 Схема за задачите ползващи първата теорема за хомоморфизмите **13**

6 Първа порция примери **14**
6.1 Решение: 14

7 Още един пример **17**
7.1 Решение: 17

8 Още един пример **18**
8.1 Решение: 18

9 Последна задача за хомоморфизми **20**
9.1 Решение: 20

10 Задача от теория на числата **23**
10.1 Решение: 23

1 Подгрупи на циклични групи

Нека си припомним каква ни беше дефиницията за подгрупа на дадена група.

Нека $< G, e, *, ()^{-1} >$ е група. Нека $H \subseteq G$. Казваме, че H образува подгрупа на $< G, e, *, ()^{-1} >$, ако

1. $e \in H$
2. $(\forall a \in H)(\forall b \in H)(a * b \in H)$
3. $(\forall a \in H)(a^{-1} \in H)$

Сега очевидно ако $\mathcal{A} =< A, e_{\mathcal{A}}, *_{\mathcal{A}}, inv_{\mathcal{A}} >$ и $\mathcal{B} =< B, e_{\mathcal{B}}, *_{\mathcal{B}}, inv_{\mathcal{B}} >$ са групи, за които е в сила

1. $e_{\mathcal{A}} = e_{\mathcal{B}}$
2. $(\forall b \in B)(\forall c \in B)(b *_{\mathcal{B}} c = b *_{\mathcal{A}} c)$
3. $(\forall b \in B)(inv_{\mathcal{B}}(b) = inv_{\mathcal{A}}(b))$

То $\mathcal{B}$ е подгрупа на $\mathcal{A}$ тогава и само тогава когато $B \subseteq A$.

Така нека сега дадем дефиниция за циклична група. Нека $< G, e, *, ()^{-1} >$ е група. Казваме, че тя е циклична, ако се поражда от един елемент. Тоест $(\exists g \in G)(G =< g >= \{g^z \mid z \in \mathbb{Z}\})$.

От лекции знаем, че $< \mathbb{Z}, 0, +, - >$ е циклична група, защото $< 1 > = 1\mathbb{Z} = \{z.1 \mid z \in \mathbb{Z}\} = \mathbb{Z}$. Също така, знаем, че с точност до изоморфизъм това е единствената циклична група от безкраен ред. Както и ако $n \in \mathbb{N}^+$, то групата на n-тите корени на единицата $< \mathbb{C}_n, 1, ., ()^{-1} >$ е циклична група (поражда се от елемента ω_n^1) и с точност до изоморфизъм е единствената циклична от ред n.

1.1 Подгрупи на групата на целите числа

Така нека $n \in \mathbb{N}$. Тогава $< n >= \{z.n \mid z \in \mathbb{Z}\} = n\mathbb{Z}$. Това са всички цели числа кратни на n. Очевидно $< -n >=< n >$. Ето няколко примера

1. $< 0 > = 0\mathbb{Z} = \{0\}$
2. $< 1 > = 1\mathbb{Z} = \mathbb{Z}$
3. $< 2 > = \{z.2 \mid z \in \mathbb{Z}\} = \{z \in \mathbb{Z} \mid z \equiv 0 \pmod 2\} = 2\mathbb{Z}$
4. $< 6 > = \{z.6 \mid z \in \mathbb{Z}\} = \{z \in \mathbb{Z} \mid z \equiv 0 \pmod 6\} = 6\mathbb{Z}$

Е оказва се, че всяка подгрупа на целите числа е от вида $n\mathbb{Z}$ за някое естествено n. Това се доказва изключително лесно. Ето едно бързо доказателство. Първо нека $n \in \mathbb{N}$ и да видим, че $< n\mathbb{Z}, 0, +, - >$ е група.

1. $0.n = 0$ това е празната сума, по друг начин $0 = n + (-n)$, тоест всеки случай $0 \in n\mathbb{Z}$.
2. $a.n + b.n = (a + b).n \in n\mathbb{Z}$ тоест имаме затвореност относно събирането понеже сума от кратни на n е кратно на n.
3. $-(a.n) = -a.n$ (очевидно)

Значи $n\mathbb{Z}$ образува подгрупа на $< \mathbb{Z}, 0, +, - >$.

Задача за любознателните:
Нека M е множество такова, че $\{0\} \subset M \subset \mathbb{Z}$, което образува подгрупа на $< \mathbb{Z}, 0, +, - >$. Покажете, че $(\exists n \in \mathbb{N} \setminus \{0, 1\})(M = n\mathbb{Z})$.

Сега на въпроса каква е връзката между подгрупите на $< \mathbb{Z}, 0, +, - >$. Нека $n \in \mathbb{N}$ и $m \in \mathbb{N}$. Както видяхме $n\mathbb{Z}$ и $m\mathbb{Z}$ образуват подгрупи на $< \mathbb{Z}, 0, +, - >$. Очевидно $n\mathbb{Z}$ е подгрупа на $m\mathbb{Z}$ ТСТК $n\mathbb{Z} \subseteq m\mathbb{Z}$ понеже и двете са подгрупи на $< \mathbb{Z}, 0, +, - >$. От друга страна $n\mathbb{Z} \subseteq m\mathbb{Z} \longleftrightarrow (\forall z \in \mathbb{Z})(m \mid z.n)$. В частност при $z = 1$ получаваме $m \mid n$, тоест

$$n\mathbb{Z} \leq m\mathbb{Z} \longleftrightarrow m \mid n$$

1.2 Подгрупи на групата на n-тите корени на единицата

Нека си припомним, че $\mathbb{C}_n = \{\omega_n^k \mid k \in \{0, 1, \ldots, n-1\}\}$. Сега на готово ще използваме твърдението от лекции, че всяка подгрупа на циклична група е циклична. Тогава подгрупите на $\mathbb{C}_n$ са точно цикличните групи

породени от някой елемент на $\mathbb{C}_n$. Тоест това са групите $< \omega_n^k >$, за някое $k \in \{0, 1, \ldots, n-1\}$. Така сега използвайки следните две твърдения

1. $ord(\omega_n^k) = \dfrac{ord(\omega_n^1)}{gcd(ord(\omega_n^1), k)} = \dfrac{n}{gcd(n,k)}$
2. $| < \omega_n^k > | = ord(\omega_n^k)$

и имайки предвид, че $< \omega_n^k >$ е циклична група от краен ред. Получаваме $< \omega_n^k >= \mathbb{C}_{\frac{n}{gcd(n,k)}}$. Възможни са два случая

1. $gcd(n,k) = 1$ тогава $< \omega_n^k >= \mathbb{C}_n$.
2. $d = gcd(n,k) > 1$ тогава $d \mid n$ и значи $< \omega_n^k >= \mathbb{C}_{\frac{n}{d}}$ обаче щом $d \mid n$, то $\dfrac{n}{d} \mid n$

Значи всички подгрупи на $< \mathbb{C}_n, 1, ., ()^{-1} >$ са $< \mathbb{C}_d, 1, ., ()^{-1} >$, където $d \mid n$. Сега въпросът е кога $\mathbb{C}_k$ е подгрупа на $\mathbb{C}_d$, това очевидно е ТСТК $\mathbb{C}_k \subseteq \mathbb{C}_d$. Използвайки, че ако $z \in \mathbb{C}$, то $z \in \mathbb{C}_d \longleftrightarrow z^d = 1$. Получаваме $\mathbb{C}_k \subseteq \mathbb{C}_d$ ТСТК $(\forall s \in \{0, 1, \ldots, k-1\})((\omega_k^s)^d = 1)$. В частност трябва да е изпълнено и за $s = 1$, тоест $(\omega_k^1)^d = \omega_k^d = 1$ е това се случва ТСТК $k \mid d$. Така $\mathbb{C}_k \leq \mathbb{C}_d \longleftrightarrow k \mid d$.

2 Съседни класове. Теорема на Лагранж. Нормални подгрупи. Фактор групи

Нека $< G, e, op, inv >$ е група. По естествен начин операцията
$op : G \times G \to G$ може да бъде разширена до операция
$OP_{left} : G \times \mathcal{P}(G) \to \mathcal{P}(G)$. По следния начин
$OP_{left}(g, S) = \{op(g, s) \mid s \in S\}$. Аналогично можем да дефинираме $OP_{right} : \mathcal{P}(G) \times G \to \mathcal{P}(G)$. По следния начин
$OP_{right}(S, g) = \{op(s, g) \mid s \in S\}$. Сега ако H образува подгрупа на $< G, e, op, inv >$. То множеството $OP_{left}(g, H)$ се нарича ляв съседен клас на H по g, а множеството $OP_{right}(H, g)$ се нарича десен съседен клас на H по g.

2.1 Мултипликативен запис:

Ако $< G, 1, ., ()^{-1} >$ е мултипликативно записана група. И H образува нейна подгрупа, то

1. $gH = \{gh \mid h \in H\}$ е левия съседен клас на H по g.
2. $Hg = \{hg \mid h \in H\}$ е десния съседен клас на H по g.

2.2 Адитивен запис:

Ако $< G, 0, +, - >$ е адитивно записана група. И H образува нейна подгрупа, то

1. $g + H = \{g + h \mid h \in H\}$ е левия съседен клас на H по g.
2. $H + g = \{h + g \mid h \in H\}$ е десния съседен клас на H по g.

2.3 Важни свойства ще ги напишем в мултипликативен запис и само за левите съседни класове (за десните е аналогично)

Нека $< G, e, ., ()^{-1} >$ е група и H образува нейна подгрупа. Нека $g \in G$ е произволен. Дефинираме релацията $\sim$ в G. Така $a \sim b \longleftrightarrow aH = bH$. Тогава

1. $\sim$ е релация на еквивалетност
2. $[a]_{\sim} = aH$
3. $\{gH \mid g \in G\}$ е разбиване на G
4. $a \sim b \longleftrightarrow b \in aH$
5. $a \sim b \longleftrightarrow ab^{-1} \in H$
6. gH образува подгрупа на $< G, e, ., ()^{-1} >$ ТСТК $g = e$, тоест единствения съседен клас, който е група е самото H $(H = eH)$
7. gH и H са равномощни ($h \mapsto gh$ е биекция)

С $G : H$ бележим множеството на левите съседни класове тоест $G : H = \{gH \mid g \in G\}$). Мощността на множеството $G : H$ се нарича индекс на групата образувана от H в $< G, e, ., ()^{-1} >$. Тоест индексът на групата образувана от H е $|G : H|$.

2.4 Теорема на Лагранж

Нека $< G, e, ., ()^{-1} >$ е крайна група и H образува нейна подгрупа. Тогава $|G| = |H|.|G : H|$. Следствие $|G : H| = \dfrac{|G|}{|H|}$.

2.5 Примери

2.5.1 $\mathbb{R}^*$ и $\mathbb{R}^+$

Да си припомним, че $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ и $< \mathbb{R}^*, 1, ., ()^{-1} >$ е група. Също така $\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$ и $\mathbb{R}^- = \{r \in \mathbb{R} \mid r < 0\}$. Понеже произведение на положителни е положително и обратен на положително е положително, то $\mathbb{R}^+$ образува подгрупа на $< \mathbb{R}^*, 1, ., ()^{-1} >$. Нека намерим кои са съседните класове и на колко е равен индексът на $\mathbb{R}^+$. Нека $a \in \mathbb{R}^*$. Тогава са възможни два случая

1. $a > 0$. Тогава $a\mathbb{R}^+ = \{ar \mid a \in \mathbb{R}^+\} = \mathbb{R}^+$
2. $a < 0$. Тогава $a\mathbb{R}^+ = \{ar \mid a \in \mathbb{R}^+\} = \mathbb{R}^-$

Ползвахме, че $x \mapsto ax$ е биекция в $\mathbb{R}$. От друга страна
$a\mathbb{R}^+ = b\mathbb{R}^+ \longleftrightarrow \dfrac{a}{b} \in \mathbb{R}^+ \longleftrightarrow \dfrac{a}{b} > 0 \longleftrightarrow sign(a) = sign(b) \longleftrightarrow$
$(a \in \mathbb{R}^+ \ \& \ b \in \mathbb{R}^+) \ \vee \ (a \in \mathbb{R}^- \ \& \ b \in \mathbb{R}^-)$.
Значи $\mathbb{R}^* : \mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\}$. Така $|\mathbb{R}^* : \mathbb{R}^+| = 2$.

2.5.2 $\mathbb{Z}$ и $6\mathbb{Z}$

Нека $a \in \mathbb{Z}$. Да разделим a с частно и остатък на 6. Тоест $a = 6s + r$ и $0 \leq r < 6$. Тогава $a + 6\mathbb{Z} = \{a + 6z \mid z \in \mathbb{Z}\} = \{6s + r + 6z \mid z \in \mathbb{Z}\} = \{r + 6(z + s) \mid z \in \mathbb{Z}\} = \{r + 6z \mid z \in \mathbb{Z}\} = r + 6\mathbb{Z}$. Ползвахме, че $z \mapsto z + s$ е биекция в $\mathbb{Z}$. От друга страна
$a + 6\mathbb{Z} = b + 6\mathbb{Z} \longleftrightarrow a - b \in 6\mathbb{Z} \longleftrightarrow 6 \mid a - b \longleftrightarrow a \equiv b \pmod 6$. Ясно е, че класовете на еквивалетност са

1. $6\mathbb{Z}$
2. $1 + 6\mathbb{Z}$
3. $2 + 6\mathbb{Z}$
4. $3 + 6\mathbb{Z}$
5. $4 + 6\mathbb{Z}$
6. $5 + 6\mathbb{Z}$

Така $|\mathbb{Z} : 6\mathbb{Z}| = 6$.

2.5.3 $\mathbb{C}_8$ и $\mathbb{C}_4$

Понеже $4 \mid 8$, то $\mathbb{C}_4$ образува подгрупа на $< \mathbb{C}_8, 1, ., ()^{-1} >$. Така че можем да говорим за съседни класове и индекс. Ето един трик

$$\omega_4^k = \cos\left(\frac{2k\pi}{4}\right) + i\sin\left(\frac{2k\pi}{4}\right) = \cos\left(\frac{2(2k)\pi}{8}\right) + i\sin\left(\frac{2(2k)\pi}{8}\right) = \omega_8^{2k}$$

Нека си припомним с пример, че $\omega_8^{21} = \omega_8^{16+5} = \omega_8^{2.8}.\omega_8^5 = 1^2.\omega_8^5 = \omega_8^5$. Тоест можем да редуцираме степента до остатък на 8. Сега смятаме

1. $\omega_8^0\mathbb{C}_4 = 1\mathbb{C}_4 = \mathbb{C}_4 = \{1, \omega_8^2, \omega_8^4, \omega_8^6\} = \{\omega_8^0, \omega_8^2, \omega_8^4, \omega_8^6\}$
2. $\omega_8^1\mathbb{C}_4 = \omega_8^1\{1, \omega_8^2, \omega_8^4, \omega_8^6\} = \{\omega_8^{1+0}, \omega_8^{1+2}, \omega_8^{1+4}, \omega_8^{1+6}\} = \{\omega_8^1, \omega_8^3, \omega_8^5, \omega_8^7\}$
3. $\omega_8^2\mathbb{C}_4 = \omega_8^2\{1, \omega_8^2, \omega_8^4, \omega_8^6\} = \{\omega_8^{2+0}, \omega_8^{2+2}, \omega_8^{2+4}, \omega_8^{2+6}\} = \{\omega_8^2, \omega_8^4, \omega_8^6, \omega_8^0\}$
4. $\omega_8^3\mathbb{C}_4 = \omega_8^3\{1, \omega_8^2, \omega_8^4, \omega_8^6\} = \{\omega_8^{3+0}, \omega_8^{3+2}, \omega_8^{3+4}, \omega_8^{3+6}\} = \{\omega_8^3, \omega_8^5, \omega_8^7, \omega_8^1\}$
5. $\omega_8^4\mathbb{C}_4 = \omega_8^4\{1, \omega_8^2, \omega_8^4, \omega_8^6\} = \{\omega_8^{4+0}, \omega_8^{4+2}, \omega_8^{4+4}, \omega_8^{4+6}\} = \{\omega_8^4, \omega_8^6, \omega_8^0, \omega_8^2\}$
6. $\omega_8^5\mathbb{C}_4 = \omega_8^5\{1, \omega_8^2, \omega_8^4, \omega_8^6\} = \{\omega_8^{5+0}, \omega_8^{5+2}, \omega_8^{5+4}, \omega_8^{5+6}\} = \{\omega_8^5, \omega_8^7, \omega_8^1, \omega_8^3\}$
7. $\omega_8^6\mathbb{C}_4 = \omega_8^6\{1, \omega_8^2, \omega_8^4, \omega_8^6\} = \{\omega_8^{6+0}, \omega_8^{6+2}, \omega_8^{6+4}, \omega_8^{6+6}\} = \{\omega_8^6, \omega_8^0, \omega_8^2, \omega_8^4\}$
8. $\omega_8^7\mathbb{C}_4 = \omega_8^7\{1, \omega_8^2, \omega_8^4, \omega_8^6\} = \{\omega_8^{7+0}, \omega_8^{7+2}, \omega_8^{7+4}, \omega_8^{7+6}\} = \{\omega_8^7, \omega_8^1, \omega_8^3, \omega_8^5\}$

Тоест $\mathbb{C}_8 : \mathbb{C}_4 = \{\{\omega_8^0, \omega_8^2, \omega_8^4, \omega_8^6\}, \{\omega_8^1, \omega_8^3, \omega_8^5, \omega_8^7\}\}$. Така $|\mathbb{C}_8 : \mathbb{C}_4| = 2 = \frac{8}{4} = \frac{|\mathbb{C}_8|}{|\mathbb{C}_4|}$ (Лагранж). Това което забелязваме е, че разглеждайки съседният клас на $\mathbb{C}_4$ по ω_8^k. Ако k е четно, то резултата е множеството от тези на четна степен, съответно ако k е нечетно, то резултата е множеството от тези на нечетна степен.

2.6 Нормални групи

Нека $< G, e, ., ()^{-1} >$ е група и H образува нейна подгрупа. Казваме, че подгрупата образувана от H на групата $< G, e, ., ()^{-1} >$ е нормална, ако $(\forall g \in G)(gH = Hg)$.

2.6.1 Важни неща

1. H образува нормална подгрупа на $< G, e, ., ()^{-1} >$ ТСТК $(\forall g \in G)(\forall h \in H)(g^{-1}hg \in H)$.
2. Ако $< G, e, ., ()^{-1} >$ е абелева група, то всяка нейна подгрупа е нормална.
3. Ако $|G : H| = 2$, то H образува нормална подгрупа на $< G, e, ., ()^{-1} >$.

2.7 Фактор група

Нека $< G, e, ., ()^{-1} >$ е група и H образува нейна нормална подгрупа. Тогава в множеството $G : H = \{gH \mid g \in G\}$ можем да въведем групова операция. Това, че H е нормална подгрупа ни позволява да го направим, иначе нямаше да е групова операция ... Та дефинираме следната операция

$$aH * bH = (a.b)H \quad ([a]_{\sim_H} * [b]_{\sim_H} = [a.b]_{\sim_H})$$

Така казахме, че $*$ е групова операция. Нека видим, че наистина получаваме група:

1. $(aH*bH)*cH = (a.b)H*cH = ((a.b).c)H = (a.(b.c))H = aH*(b.c)H = aH * (bH * cH)$
2. $aH*H = aH*eH = (a.e)H = aH$ и $H*aH = eH*aH = (e.a)H = aH$
3. $aH*a^{-1}H = (a.a^{-1})H = eH = H$ и $a^{-1}H*aH = (a^{-1}.a)H = eH = H$

Значи можем преспокойно да твърдим, че относно новата операция $*$ $(aH)^{-1} = a^{-1}H$. Така групата $< G : H, H, *, ()^{-1} >$ се нарича фактор група на $< G, e, ., ()^{-1} >$ по нормалната ѝ подгрупа образувана от H и се бележи с G/H.

Четири вметвания:

1. Ако $< G, e, ., ()^{-1} >$ е абелева група, то всяка нейна фактор група е абелева.

2. Ако $< G, e, ., ()^{-1} >$ е циклична група, то всяка нейна фактор група е циклична.

3. Ако $< G, e, ., ()^{-1} >$ е крайна група, то всяка нейна фактор група е крайна.

4. Редът на една фактор група G/H съвпада с индексът на H в G.

2.8 Примери

2.8.1 $\mathbb{R}^*$ и $\mathbb{R}^+$

Понеже $< \mathbb{R}^*, 1, ., ()^{-1} >$ е абелева, то и $< \mathbb{R}^+, e, ., ()^{-1} >$ е абелева, а значи и нормална подгрупа. Значи е коректно да разгледаме фактор групата $\mathbb{R}^*/\mathbb{R}^+$. Както видяхме $\mathbb{R}^* : \mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\}$. Да видим как се смята в тази фактор група, тя е абелева, така че

1. $\mathbb{R}^+ * \mathbb{R}^+ = 1\mathbb{R}^+ * 1\mathbb{R}^+ = (1.1)\mathbb{R}^+ = \mathbb{R}^+$

2. $\mathbb{R}^+ * \mathbb{R}^- = 1\mathbb{R}^+ * (-1)\mathbb{R}^+ = (1.(-1))\mathbb{R}^+ = (-1)\mathbb{R}^+ = \mathbb{R}^-$

3. $\mathbb{R}^- * \mathbb{R}^- = (-1)\mathbb{R}^+ * (-1) * \mathbb{R}^+ = (-1.-1)\mathbb{R}^+ = 1\mathbb{R}^+ = \mathbb{R}^+$

Тоест очевидно нещата се случват точно както се случват в подгрупата $< \{1, -1\}, 1, ., ()^{-1} >$ на $< \mathbb{R}^*, 1, ., ()^{-1} >$, която е циклична, защото $\{1, -1\} =< -1 >$.

2.8.2 $\mathbb{C}_8$ и $\mathbb{C}_4$

Както видяхме $\mathbb{C}_8 : \mathbb{C}_4 = \{\{\omega_8^0, \omega_8^2, \omega_8^4, \omega_8^6\}, \{\omega_8^1, \omega_8^3, \omega_8^5, \omega_8^7\}\}$. Нека означим

1. $A = \{\omega_8^0, \omega_8^2, \omega_8^4, \omega_8^6\} = \mathbb{C}_4 = 1\mathbb{C}_4$

2. $B = \{\omega_8^1, \omega_8^3, \omega_8^5, \omega_8^7\} = \omega_8^1\mathbb{C}_4$

Понеже $< \mathbb{C}_8, 1, ., ()^{-1} >$ е циклична, в частност е и абелева. То $< \mathbb{C}_4, 1, ., ()^{-1} >$ е нормална и факторът $\mathbb{C}_8/\mathbb{C}_4$ е циклична от ред 2, тоест е изоморфна на $\mathbb{C}_2$. Като сметки

1. $A * A = 1\mathbb{C}_4 * 1\mathbb{C}_4 = (1.1)\mathbb{C}_4 = \mathbb{C}_4 = A$

2. $A * B = 1\mathbb{C}_4 * \omega_8^1\mathbb{C}_4 = (1.\omega_8^1)\mathbb{C}_4 = \omega_8^1\mathbb{C}_4 = B$

3. $B * B = \omega_8^1\mathbb{C}_4 * \omega_8^1\mathbb{C}_4 = \omega_8^2\mathbb{C}_4 = 1\mathbb{C}_4 = A$

2.8.3 $\mathbb{Z}$ и $6\mathbb{Z}$

Понеже алгебриците са пестеливи от към запис, то $r+6\mathbb{Z}$ означаваме още с $\overline{r}$. Така $\mathbb{Z} : 6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. Също така множеството $\mathbb{Z} : 6\mathbb{Z}$ бележим с $\mathbb{Z}_6$. Действието тук се случва по модул остатък на 6. Например ако групата запишем така $< \mathbb{Z}_6, \overline{0}, \oplus, \ominus >$, то

1. $\overline{2} \oplus \overline{3} = \overline{2+3} = \overline{5}$

2. $\overline{4} \oplus \overline{3} = \overline{4+3} = \overline{7} = \overline{1}$

3. $\ominus\overline{4} = \overline{-4} = \overline{6-4} = \overline{2}$

3 Една класика от Информатика

Нека $\alpha = \cos\left(\frac{\pi}{33}\right) + i\sin\left(\frac{\pi}{33}\right)$. Нека $\beta = \alpha^{28}$. Нека $G = < \alpha >$. Нека $H = < \beta >$.

а) Намерете редовете на α, β, G и H.

б) Да се намерят всички подгрупи на $< G, 1, ., ()^{-1} >$ и да се направи схема на включванията между тях.

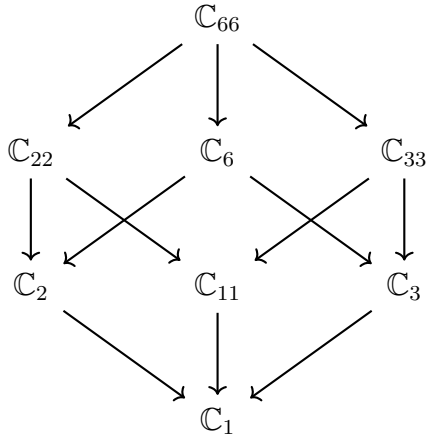
в) Да се реши уравнението $G/H \cong \mathbb{Z}_t$.

г) Да се реши уравнението $G/ < \alpha^s > \cong H$.

3.1 Решение

а) Човек трябва да е много съобразителен и да забележи, че липсва една 2-ка в числителя ... Ей това е нещото, което наказва невнимателните млади Информатици ... Така $\alpha = \cos\left(\frac{2\pi}{66}\right) + i\sin\left(\frac{2\pi}{66}\right) = \omega_{66}^1$. Тогава $G = < \alpha > = < \omega_{66}^1 > = \mathbb{C}_{66}$. Така $ord(\alpha) = |G| = |\mathbb{C}_{66}| = 66$. За β имаме $\beta = \alpha^{28} = (\omega_{66}^1)^{28} = \omega_{66}^{28} = \omega_{2.3.11}^{2.2.7} = \omega_{33}^{14}$. Използвайки, че $gcd(33, 14) = 1$ получаваме, че $H = < \beta > = < \omega_{33}^{14} > = \mathbb{C}_{33}$ и значи $ord(\beta) = |H| = |\mathbb{C}_{33}| = 33$.

б) От предната $G = \mathbb{C}_{66}$.
Естествените делители на 66 са $\{1, 2, 3, 6, 11, 22, 33, 66\}$. Тогава подгрупите са тези образувани от $\mathbb{C}_d$ за $d \in \{1, 2, 3, 6, 11, 22, 33, 66\}$.



в) $G/H = \mathbb{C}_{66}/\mathbb{C}_{33} \cong \mathbb{C}_2 \cong \mathbb{Z}_2$ Значи $t = 2$.

г) Искаме да решим уравнението $\mathbb{C}_{66}/ < \alpha^s > \cong \mathbb{C}_{33}$, което свеждаме до $< \alpha^s >= \mathbb{C}_2$. Тоест искаме $| < \alpha^s > | = 2$, но $| < \alpha^s > | = ord(\alpha^s)$. От друга страна $ord(\alpha^s) = \dfrac{ord(\alpha)}{gcd(ord(\alpha), s)} = \dfrac{66}{gcd(66, s)}$. Значи търсим s, такова че $\dfrac{66}{gcd(66, s)} = 2$, тоест $\dfrac{1}{gcd(66, s)} = \dfrac{2}{66} = \dfrac{1}{33}$. Значи $gcd(66, s) = 33$. Очевидно това се случва когато $s \equiv 33 \pmod{66}$. Понеже $gcd(66, 66z + 33) = gcd(66, 33) = 33$.

4 Първа теорема за хомоморфизмите

Нека $\mathcal{A} =< A, e_{\mathcal{A}}, *_{\mathcal{A}}, inv_{\mathcal{A}} >$ и $\mathcal{B} =< B, e_{\mathcal{B}}, *_{\mathcal{B}}, inv_{\mathcal{B}} >$ са групи. Нека $\varphi : A \to B$ е хомоморфизъм от $\mathcal{A}$ към $\mathcal{B}$. Тоест

$$(\forall x \in A)(\forall y \in A)(\varphi(x *_{\mathcal{A}} y) = \varphi(x) *_{\mathcal{B}} \varphi(y))$$

. Тогава

1. $\mathrm{Ker}(\varphi) = \{a \in A \mid \varphi(a) = e_{\mathcal{B}}\}$ образува **нормална** подгрупа на $\mathcal{A}$.
2. $\mathrm{Im}(\varphi) = \varphi[A] = \{\varphi(a) \mid a \in A\}$ образува подгрупа на $\mathcal{B}$.
3. $A/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$

5 Схема за задачите ползващи първата теорема за хомоморфизмите

Нека $\mathcal{A} =< A, e_{\mathcal{A}}, *_{\mathcal{A}}, inv_{\mathcal{A}} >$ и $\mathcal{B} =< B, e_{\mathcal{B}}, *_{\mathcal{B}}, inv_{\mathcal{B}} >$. Нека $C \subseteq A$. Искаме да докажем, че

1. C образува нормална подгрупа на $\mathcal{A}$.
2. $A/C \cong B$.

За тази цел трябва да измислим подходящо изображение $\varphi : A \to B$, което да е такова, че

1. φ е хомоморфизъм от $\mathcal{A}$ към $\mathcal{B}$.
2. φ е сюрективно, което ще ни подсигури $\mathrm{Im}(\varphi) = B$.
3. $\mathrm{Ker}(\varphi) = C$

Ако имаме такова изображение по първата теорема за хомоморфизмите заключаваме, че C образува нормална подгрупа на $\mathcal{A}$ и $A/C \cong B$. И така за да решим задачата трябва кажем как точно ще разсъждаваме, че да измислим изображението, което търсим. Идеята е да тръгнем от зад на пред ... Да предположим, че имаме изображение $\varphi : A \to B$, което е хомоморфизъм, ще видим как трябва да действа φ, така че $\mathrm{Ker}(\varphi) = C$. Нека $x, y \in A$ са такива, че $\varphi(x) = \varphi(y)$. Тогава

$$\begin{aligned}
\varphi(x) = \varphi(y) &\longleftrightarrow \\
\varphi(x) *_{\mathcal{B}} inv_{\mathcal{B}}(\varphi(y)) = e_{\mathcal{B}} &\longleftrightarrow \\
\varphi(x) *_{\mathcal{B}} \varphi(inv_{\mathcal{A}}(y)) = e_{\mathcal{B}} &\longleftrightarrow \\
\varphi(x *_{\mathcal{A}} inv_{\mathcal{A}}(y)) = e_{\mathcal{B}} &\longleftrightarrow \\
x *_{\mathcal{A}} inv_{\mathcal{A}}(y) \in \mathrm{Ker}(\varphi) &\longleftrightarrow \\
x *_{\mathcal{A}} inv_{\mathcal{A}}(y) \in C &
\end{aligned}$$

Значи искаме x и y да имат един и същ образ ТСТК $x *_{\mathcal{A}} inv_{\mathcal{A}}(y) \in C$. Сега ако $\mathrm{Ker}(\varphi) = C$, то C образува нормална подгрупа на $\mathcal{A}$ и тогава $x *_{\mathcal{A}} inv_{\mathcal{A}}(y) \in C$ е еквивалетно с $x *_{\mathcal{A}} C = y *_{\mathcal{A}} C$. Това е просто вметка, която цели да ни каже, че същност искаме двете релации $\varphi(x) = \varphi(y)$ и $x *_{\mathcal{A}} C = y *_{\mathcal{A}} C$ да съвпадат! Та ако имаме хубав критерий (под хубав имаме предвид такъв, който включва равенство!) за принадлежност

към множеството C сравнително лесно можем да се досетим какво да е изображението вземайки предвид, че образите искаме да са елементите на B! Нека видим няколко примера :)

6 Първа порция примери

Нека $\mathcal{C} =< \mathbb{C}^*, 1, ., ()^{-1} >$. Да се докаже, че M образува нормална подгрупа на $\mathcal{C}$ и $\mathbb{C}^*/M \cong S$, където

а) $M = \mathbb{U}$ и $S = \mathbb{R}^+$

б) $M = \mathbb{R}^+$ и $S = \mathbb{U}$

в) $M = \mathbb{R}^*$ и $S = \mathbb{U}$

6.1 Решение:

Първо това, че M образува нормална подгрупа на $\mathcal{C}$, можем да решим генерално в тази порция примери така: И в трите примера знаем или лесно можем да съобразим, че M образува подгрупа на $\mathcal{C}$. Тоест $< M, 1, ., ()^{-1} >$ е подгрупа на $< \mathbb{C}^*, 1, ., ()^{-1} >$, която е абелева. Следователно M образува нормална подгрупа на $\mathcal{C}$. (Като можем лесно да се измъкнем е хубаво да го направим!)

а) Търсим изображение $\varphi : \mathbb{C}^* \to \mathbb{R}^+$, което е сюрективен хомоморфизъм и $\mathrm{Ker}(\varphi) = \mathbb{U}$. Така нека първо разгледаме трите множества, които имаме и да сме сигурни, че имаме хубав (такъв с равенство) критерий за принадлежност към $\mathbb{U}$.

   1. Понеже $\mathbb{C}$ образува поле, то $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Имаме $x \in \mathbb{C}^* \iff x \in \mathbb{C}$ & $x \neq 0$.
   2. $\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$. Имаме $x \in \mathbb{R}^+ \iff x \in \mathbb{R}$ & $x > 0$.
   3. $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$. Имаме $x \in \mathbb{U} \iff x \in \mathbb{C}^*$ & $|x| = 1$.

   Искаме

$$\varphi(x) = \varphi(y) \longleftrightarrow \frac{x}{y} \in \mathbb{U} \longleftrightarrow \left|\frac{x}{y}\right| = 1 \longleftrightarrow \frac{|x|}{|y|} = 1 \longleftrightarrow |x| = |y|$$

От друга страна ако $x \in \mathbb{C}^*$, то $|x| > 0$ понеже $|x| = 0 \iff x = 0$ и $|x| \geq 0$. Значи ако $x \in \mathbb{C}^*$, то $|x| \in \mathbb{R}^+$. Нека тогава пробваме с изображението $\varphi(x) = |x|$ и да проверим, че то ни върши работа.

1. $\varphi(x.y) = |x.y| = |x|.|y| = \varphi(x).\varphi(y)$ Значи φ е ХММ.
2. Нека $r \in \mathbb{R}^+$. В частност $r \in \mathbb{C}^*$. Но $r = |r| = \varphi(r)$. Значи φ е сюрекция.
3. $x \in \mathbb{U} \iff x \in \mathbb{C}^* \ \& \ |x| = 1 \iff x \in \mathbb{C}^* \ \& \ \varphi(x) = 1 \iff x \in \mathrm{Ker}(\varphi)$. Значи $\mathrm{Ker}(\varphi) = \mathbb{U}$.

От първата теорема за ХММ имаме $\mathbb{C}^*/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$, тоест $\mathbb{C}^*/\mathbb{U} \cong \mathbb{R}^+$.

б) Търсим изображение $\varphi : \mathbb{C}^* \to \mathbb{U}$, което е сюректив хомоморфизъм и $\mathrm{Ker}(\varphi) = \mathbb{R}^+$. Така търсим критерий за принадлежност към $\mathbb{R}^+$, в който да участва равенство. Ами ние вече използвахме едно свойство на елементите включващо равенство. Именно $x \in \mathbb{R}^+ \iff x \in \mathbb{C}^* \ \& \ x = |x|$. Нека пробваме с него. Искаме

$$\varphi(x) = \varphi(y) \longleftrightarrow \frac{x}{y} \in \mathbb{R}^+ \longleftrightarrow \frac{x}{y} = \left|\frac{x}{y}\right| \longleftrightarrow \frac{x}{y} = \frac{|x|}{|y|} \longleftrightarrow \frac{x}{|x|} = \frac{y}{|y|}$$

Получихме $\varphi(x) = \varphi(y) \longleftrightarrow \dfrac{x}{|x|} = \dfrac{y}{|y|}$. Забележете, че от двете страни на равенствата x и y са разделени. Това ни помага да усетим каква информация искаме нашият хомоморфизъм да прехвърли от едната група към другата! След това всичко опира до правилния пренос на информацията ... Така ние искаме $\varphi(x) \in \mathbb{U}$, тоест $\varphi(x) \in \mathbb{C}^* \ \& \ |\varphi(x)| = 1$. Човек лесно съобразява, че ако $x \in \mathbb{C}^*$, то $|x| \in \mathbb{R}^+$ и значи $\dfrac{x}{|x|} \in \mathbb{C}^*$. Я дайте да сметнем модула на $\dfrac{x}{|x|}$, на колко ли е равен ?

$$\left|\frac{x}{|x|}\right| = \frac{|x|}{||x||} = \frac{|x|}{|x|} = 1$$

Значи излезе, че ако $x \in \mathbb{C}^*$, то $\dfrac{x}{|x|} \in \mathbb{U}$. Много неочаквано ... Дали пък няхме специален термин когато разделяхме един вектор на дължината му ? Да веее имаме нормираност му викахме на това с

идеята, че дължината на нормиран вектор винаги е 1-ца. Спомени от 1-ви курс :) Така значи пробваме с изображението $\varphi(x) = \frac{x}{|x|}$.

1. $\varphi(x.y) = \frac{x.y}{|x.y|} = \frac{x.y}{|x|.|y|} = \frac{x}{|x|}.\frac{y}{|y|} = \varphi(x).\varphi(y)$ Значи φ е ХММ.
2. Нека $z \in \mathbb{U}$. В частност $z \in \mathbb{C}^*$. Но тогава $\varphi(z) = \frac{z}{|z|} = \frac{z}{1} = z$. Значи φ е сюрекция.
3. $x \in \mathbb{R}^+ \iff x \in \mathbb{C}^* \ \& \ x = |x| \iff x \in \mathbb{C}^* \ \& \ \varphi(x) = \frac{x}{|x|} = \frac{x}{x} = 1 \iff x \in \mathrm{Ker}(\varphi)$. Значи $\mathrm{Ker}(\varphi) = \mathbb{R}^+$.

От първата теорема за ХММ имаме $\mathbb{C}^*/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$, тоест $\mathbb{C}^*/\mathbb{R}^+ \cong \mathbb{U}$.

в) Търсим изображение $\varphi : \mathbb{C}^* \to \mathbb{U}$, което е сюрективен хомоморфизъм и $\mathrm{Ker}(\varphi) = \mathbb{R}^*$. За целта първо търсим критерий с равенство за принадлежност към $\mathbb{R}^*$. Понеже $\mathbb{R}^* \subset \mathbb{C}^*$, то дайте да видим какво значи едно ненулево комплексно число да е ненулево реално. Нека $z = a + ib$ и $(a, b) \neq (0, 0)$. Ако се случи, че $b \neq 0$, то $z \notin \mathbb{R}^*$. Значи ако, $z \in \mathbb{R}^*$, то $z = a + i0$. Но тогава комплексно спрегнатото на z е $a - i0$, което е z. Тоест $z \in \mathbb{R}^*$, то $z = \overline{z}$. Е ясно е и обратното включване. Та значи ето го критерия за принадлежност към $\mathbb{R}^*$. $x \in \mathbb{R}^* \iff x \in \mathbb{C}^* \ \& \ x = \overline{x}$. Нека пробваме с него. Искаме

$$\varphi(x) = \varphi(y) \longleftrightarrow \frac{x}{y} \in \mathbb{R}^* \longleftrightarrow \frac{x}{y} = \overline{\left(\frac{x}{y}\right)} \longleftrightarrow \frac{x}{y} = \frac{\overline{x}}{\overline{y}} \longleftrightarrow \frac{x}{\overline{x}} = \frac{y}{\overline{y}}$$

Получихме $\varphi(x) = \varphi(y) \longleftrightarrow \frac{x}{\overline{x}} = \frac{y}{\overline{y}}$. Забележете, че променливите пак се разделиха, значи това е информацията, която искаме да прехвърлим. Сега остава човек да съобрази, че ако $x \in \mathbb{C}^*$, то $\frac{x}{\overline{x}} \in \mathbb{U}$. Първо ако $x \in \mathbb{C}^*$, то е ясно, че $\frac{x}{\overline{x}} \in \mathbb{C}^*$. Сега ако $x \in \mathbb{C}^*$, то $\left|\frac{x}{\overline{x}}\right| = \frac{|x|}{|\overline{x}|} = \frac{|x|}{|x|} = 1$. Значи $\varphi : \mathbb{C}^* \to \mathbb{U}$ и $\varphi(x) = \frac{x}{\overline{x}}$ е коректно дефинирано. Да видим, че ни върши работа.

1. $\varphi(x.y) = \frac{x.y}{\overline{x.y}} = \frac{x.y}{\overline{x}.\overline{y}} = \frac{x}{\overline{x}}.\frac{y}{\overline{y}} = \varphi(x).\varphi(y)$ Значи φ е ХММ.

2. Нека $z \in \mathbb{U}$. В частност $z \in \mathbb{C}^*$. Но тогава $\varphi(z) = \frac{z}{\overline{z}} = \frac{z.z}{\overline{z}.z} = \frac{z^2}{|z|^2} = \frac{z^2}{1^2} = z^2$. Значи нека $s = \sqrt{z}$. Тогава $|s| = \sqrt{|z|} = \sqrt{1} = 1$ Значи $s \in \mathbb{U}$ и $\varphi(s) = s^2 = (\sqrt{z})^2 = z$. Значи φ е сюрекция.
3. $x \in \mathbb{R}^* \iff x \in \mathbb{C}^* \ \& \ x = \overline{x} \iff x \in \mathbb{C}^* \ \& \ \varphi(x) = \frac{x}{\overline{x}} = \frac{x}{x} = 1 \iff x \in \mathrm{Ker}(\varphi)$. Значи $\mathrm{Ker}(\varphi) = \mathbb{R}^*$.

От първата теорема за ХММ имаме $\mathbb{C}^*/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$, тоест $\mathbb{C}^*/\mathbb{R}^* \cong \mathbb{U}$.

7 Още един пример

Да се докаже, че $\mathbb{U}/\mathbb{C}_n \cong \mathbb{U}$.

7.1 Решение:

Първо защо $\mathbb{C}_n$ образува подгрупа на $< \mathbb{U}, 1, ., ()^{-1} >$? Ами нека $z \in \mathbb{C}_n$. Тогава $z = |z| (\cos(Arg(z)) + i \sin(Arg(z)))$. Тогава от Моавър 1 имаме $z^n = |z|^n (\cos(n.Arg(z)) + i \sin(n.Arg(z))) = 1$. Значи $|z|^n = 1$. Понеже $|z| \geq 0$, то $|z| = 1$ и значи $z \in \mathbb{U}$. Така $\mathbb{C}_n \subseteq \mathbb{U}$. Обаче $< \mathbb{C}_n, 1, ., ()^{-1} >$ е група. Значи $< \mathbb{C}_n, 1, ., ()^{-1} >$ е подгрупа на $< \mathbb{U}, 1, ., ()^{-1} >$. Даже е и нормална понеже е абелева. Имаме директен критерий за принадлежност към $\mathbb{C}_n$, в който участва равенство. $x \in \mathbb{C}_n \iff x \in \mathbb{U} \ \& \ x^n = 1$. Търсим изображение $\varphi : \mathbb{U} \to \mathbb{U}$, което е сюрективен хомоморфизъм и $\mathrm{Ker}(\varphi) = \mathbb{C}_n$. Искаме

$$\varphi(x) = \varphi(y) \longleftrightarrow \frac{x}{y} \in \mathbb{C}_n \longleftrightarrow \left(\frac{x}{y}\right)^n = 1 \longleftrightarrow \frac{x^n}{y^n} = 1 \longleftrightarrow x^n = y^n$$

Получихме $\varphi(x) = \varphi(y) \longleftrightarrow x^n = y^n$. Така въпросът е дали ако $x \in \mathbb{U}$, то $x^n \in \mathbb{U}$? Ами ако $x \in \mathbb{U}$, то $|x| = 1$ и $|x^n| = |x|^n = 1^n = 1$. Значи да ако, $x \in \mathbb{U}$, то $x^n \in \mathbb{U}$. Значи $\varphi(x) = x^n$ е коректно изображение от $\mathbb{U}$ към $\mathbb{U}$. Да проверим че ни върши работа.

1. $\varphi(x.y) = (x.y)^n = x^n.y^n = \varphi(x).\varphi(y)$. Значи φ е ХММ.
2. Нека $z \in \mathbb{U}$. Имаме, че $\varphi(z) = z^n$. Нека $s = \sqrt[n]{z}$. Тогава $|s| = \sqrt[n]{|z|} = \sqrt[n]{1} = 1$. Значи $s \in \mathbb{U}$. От друга страна $\varphi(s) = s^n = (\sqrt[n]{z})^n = z$. Значи φ е сюрекция.

3. Имаме $x \in \mathbb{C}_n \iff x \in \mathbb{U}\ \&\ x^n = 1 \iff x \in \mathbb{U}\ \&\ \varphi(x) = 1 \iff x \in \mathrm{Ker}(\varphi)$. Значи $\mathrm{Ker}(\varphi) = \mathbb{C}_n$.

От първата теорема за ХММ имаме $\mathbb{U}/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$, тоест $\mathbb{U}/\mathbb{C}_n \cong \mathbb{U}$.

8 Още един пример

Нека $H_n = \{z \in \mathbb{C}^* \mid (\exists r \in \mathbb{R}^+)(\exists s \in \mathbb{C}_n)(z = r.s)\}$. Да се докаже, че

а) $< H_n, 1, ., ()^{-1} >$ е група.

б) $H_n = \{z \in \mathbb{C}^* \mid z^n = |z|^n\}$.

в) H_n образува нормална подгрупа на $< H_{n^2}, 1, ., ()^{-1} >$.

г) $H_{n^2}/H_n \cong \mathbb{C}_n$.

8.1 Решение:

а) Очевидно $H_n \subset \mathbb{C}^*$ и $1 \in H_n$. Ще покажем, че е затворено относно умножението и относно обратен елемент. Нека $a \in H_n$ и нека $b \in H_n$. Тогава нека $r_a \in \mathbb{R}^+$, $r_b \in \mathbb{R}^+$, $s_a \in \mathbb{C}_n$ и $s_b \in \mathbb{C}_n$. Тогава $a.b = (r_a.s_a).(r_b.s_b) = (r_a.r_b)(s_a.s_b)$. Понеже $\mathbb{R}^+$ и $\mathbb{C}_n$ образуват подгрупи на $< \mathbb{C}^*, 1, ., ()^{-1} >$, то $a.b \in H_n$. Също така $a^{-1} = (r_a.s_a)^{-1} = s_a^{-1}.r_a^{-1} = r_a^{-1}.s_a^{-1}$ и значи $a^{-1} \in H_n$. Следователно $< H_n, 1, ., ()^{-1} >$ е подгрупа на $< \mathbb{C}^*, 1, ., ()^{-1} >$. В частност е и група.

б) Нека $z \in \mathbb{C}^*$ е такова, че $z^n = |z|^n$. Нека тригонометричния вид на z е $|z|(\cos(\alpha) + i\sin(\alpha))$. Тогава $z^n = |z|^n(\cos(n\alpha) + i\sin(n\alpha)) = |z|^n$. Значи $\cos(n\alpha) + i\sin(n\alpha) = 1 = 1 + i0$. Значи $\cos(n\alpha) = 1$ и $\sin(n\alpha) = 0$. Решенията на тази система са $n\alpha = 2k\pi$ за $k \in \mathbb{Z}$. Обаче тогава $\alpha = \dfrac{2k\pi}{n}$ и както знаем от първи курс решенията с точност до кратност на 2π са само n за $k \in \{0, 1, \ldots, n-1\}$. Но тогава $z = |z|\omega_n^k$ за $k \in \{0, 1, \ldots, n-1\}$. Значи $\{z \in \mathbb{C}^* \mid z^n = |z|^n\} \subseteq H_n$. Обратното включване е директно от тригонометричния вид на всяко комплексно (получава се $z^n = r^n$ ...)

в) От а) имаме, че $< H_n, 1, ., ()^{-1} >$ е абелева група. Единственото, което трябва да видим е, че $H_n \subseteq H_{n^2}$, което е доста лесно. Нека

$z \in H_n$. Тогава от б) $z^n = |z|^n$. Тогава $z^{n^2} = z^{n.n} = (z^n)^n = (|z|^n)^n = |z|^{n.n} = |z|^{n^2}$. Значи $z \in H_{n^2}$. Следователно $H_n \subseteq H_{n^2}$. Вземайки предвид, че $< H_n, 1, ., ()^{-1} >$ е абелева група получаваме, че е нормална подгрупа на $< H_{n^2}, 1, ., ()^{-1} >$.

г) Вече имаме и критерий за принадлежност към H_n с равенство. Така, че търсим изображение $\varphi : H_{n^2} \to \mathbb{C}_n$, което е сюрективен хомоморфизъм и $\mathrm{Ker}(\varphi) = H_n$. Искаме

$$\varphi(x) = \varphi(y) \longleftrightarrow \frac{x}{y} \in H_n \longleftrightarrow \left(\frac{x}{y}\right)^n = \left|\frac{x}{y}\right|^n \longleftrightarrow$$
$$\frac{x^n}{y^n} = \frac{|x|^n}{|y|^n} \longleftrightarrow \frac{x^n}{|x|^n} = \frac{y^n}{|y|^n}$$

Получихме $\varphi(x) = \varphi(y) \longleftrightarrow \frac{x^n}{|x|^n} = \frac{y^n}{|y|^n}$. Така въпросът е дали ако $x \in H_{n^2}$, то $\frac{x^n}{|x|^n} \in \mathbb{C}_n$? Ами ако $x \in H_{n^2}$, то $x^{n^2} = |x|^{n^2}$. Сега за да видим, че $\frac{x^n}{|x|^n} \in \mathbb{C}_n$ трябва да видим, че на повдигнат на n-та степен дава 1. Тогава ако $x \in H_{n^2}$, то $\left(\frac{x^n}{|x|^n}\right)^n = \frac{x^{n^2}}{|x|^{n^2}} = \frac{|x|^{n^2}}{|x|^{n^2}} = 1$. Значи да ако, $x \in H_{n^2}$, то $\frac{x^n}{|x|^n} \in \mathbb{C}_n$. Значи $\varphi(x) = \frac{x^n}{|x|^n}$ е коректно изображение от H_{n^2} към $\mathbb{C}_n$. Да проверим, че ни върши работа.

(а) $\varphi(x.y) = \frac{(x.y)^n}{|x.y|^n} = \frac{x^n.y^n}{|x|^n.|y|^n} = \frac{x^n}{|x|^n}.\frac{y^n}{|y|^n} = \varphi(x).\varphi(y)$. Значи φ е ХММ.

(б) Искаме да видим, че φ е сюрекция. Нека тогава вземем произволен елемент на $\mathbb{C}_n$. Нека това $z = \omega_n^k$ за някое $k \in \{0, 1, \ldots, n-1\}$. Искаме да намерим $x \in H_{n^2}$, такова че $\varphi(x) = z$. Ами човек ако погледа така двете множества и му дойдат някакви спомени от 1-ви курс ще се усети кой е директния кандидат. Хубаво е той да има модул 1 понеже $|z| = |\omega_n^k| = 1$. Нека пробваме с $\omega_{n^2}^k$. $\varphi(\omega_{n^2}^k) = \frac{(\omega_{n^2}^k)^n}{1^n} = (\omega_{n^2}^n)^k = (\omega_n^1)^k = \omega_n^k = z$. Сега остава да се убедим, че $\omega_{n^2}^k \in H_{n^2}$. Имаме $|\omega_{n^2}^k| = 1$ и $(\omega_{n^2}^k)^{n^2} = 1$. Значи $(\omega_{n^2}^k)^{n^2} = 1 = |\omega_{n^2}^k|^{n^2}$. Така $\omega_{n^2}^k \in H_{n^2}$ и $\varphi(\omega_{n^2}^k) = \omega_n^k = z$. Следователно φ е сюрекция.

(в) Имаме $x \in H_n \iff x \in H_{n^2}$ & $x^n = |x|^n \iff x \in H_{n^2}$ & $\dfrac{x^n}{|x|^n} = 1 \iff x \in H_{n^2}$ & $\varphi(x) = 1 \iff x \in \mathrm{Ker}(\varphi)$. Значи $\mathrm{Ker}(\varphi) = H_n$.

От първата теорема за ХММ имаме $H_{n^2}/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$, тоест $H_{n^2}/H_n \cong \mathbb{C}_n$.

9 Последна задача за хомоморфизми

Нека

1. $G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{Q}^* \;\&\; b \in \mathbb{Q} \right\}$
2. $M = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{Q}^* \right\}$
3. $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{Q} \right\}$

Да се докаже, че

а) G образува група относно операцията умножение на квадратни матрици с рационални коефициенти.

б) M образува подгрупа на групата образувана от G и тя е изоморфна на $< \mathbb{Q}^*, 1, ., ()^{-1} >$.

в) H образува нормална подгрупа на групата образувана от G и $G/H \cong < \mathbb{Q}^*, 1, ., ()^{-1} >$.

9.1 Решение:

а) Следкато искаме да докажем, че G образува група относно операцията умножение на квадратни матрици с рационални коефициенти. То логично е проверим, че $G \subseteq GL_2(\mathbb{Q})$. Нека $a \in \mathbb{Q}^*$ и $b \in \mathbb{Q}$ и нека $m = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. Тогава $\det(m) = a \neq 0$. Значи m е неособена матрица с рационални коефициенти, знаем че рационалните числа

образуват поле, значи m е обратима. Тоест $m \in GL_2(\mathbb{Q})$. Следователно $G \subseteq GL_2(\mathbb{Q})$. Знаем, че $< GL_2(\mathbb{Q}), E_2, ., ()^{-1} >$ образува група, така че ще покажем, че G образува нейна подгрупа. Нека $a \in \mathbb{Q}^*$ и $b \in \mathbb{Q}$ и нека $m = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. Нека $c \in \mathbb{Q}^*$ и $d \in \mathbb{Q}$ и нека $t = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$. Тогава $m.t = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} . \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix}$. Сега понеже $a \in \mathbb{Q}^*$ и $c \in \mathbb{Q}^*$. То $ac\mathbb{Q}^*$. Очевидно $ad + b \in \mathbb{Q}$. Значи $m.t \in G$. Значи G е затворено отнсно умножение на матрици. Понеже $1 \in \mathbb{Q}^*$ и $0 \in \mathbb{Q}$, то $E_2 \in G$. Ако се сетим за практическото правило за намиране на обратна матрица от ред 2. Което беше по главния диагонал разменяме местата, а във вторични сменяме знаците и делим на детерминантата. То $m^{-1} = \frac{1}{\det(m)} \begin{pmatrix} 1 & -b \\ -0 & a \end{pmatrix} = \frac{1}{a} \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} a^{-1} & -b.a^{-1} \\ -0 & 1 \end{pmatrix}$ и очевидно $m^{-1} \in G$. Значи G образува подгрупа на $< GL_2(\mathbb{Q}), E_2, ., ()^{-1} >$.

б) Ще докажем, че $< M, E_2, ., ()^{-1} > \cong < \mathbb{Q}^*, 1, ., ()^{-1} >$ и тогава по изоморфизъм $< M, E_2, ., ()^{-1} >$ ще е група, понеже $< \mathbb{Q}^*, 1, ., ()^{-1} >$ е група. Поглеждайки множеството M смятам, че е задължително студент във ФМИ втори семестър не зависимо кой курс да съобрази, кое изображение е очевидна биекция от M към $\mathbb{Q}^*$. Именно $\varphi\left(\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}\right) = q$. След като, това че $\varphi : M \to \mathbb{Q}^*$ е очевидно, че е биекция остава да видим, че φ запазва бинарната операция. Нека $x \in \mathbb{Q}^*$ и нека $y \in \mathbb{Q}^*$. Тогава $\varphi\left(\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} . \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} x.y & 0 \\ 0 & 1 \end{pmatrix}\right) = x.y = \varphi\left(\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}\right) . \varphi\left(\begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}\right)$. Значи φ е биективен хомоморфизъм, тоест изоморфизъм. Следователно $< M, E_2, ., ()^{-1} >$ е група. Това, че е подгрупа на $< G, E_2, ., ()^{-1} >$ е очевидно, защото е очевидно, че $M \subseteq G$.

в) Използвайки първата теорема за хомоморфизмите ще докажем $G/H \cong < \mathbb{Q}^*, 1, ., ()^{-1} >$, с което "безплатно"ще получим, че H образува нормална подгрупа на $< G, E_2, ., ()^{-1} >$. Първо ни трябва критерий за принадлежност към H, който да отделя от елементите на G със свойство, което е изразимо с равенство. Ами поглеждайки, че $H =$

$\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix} \;\middle|\; b \in \mathbb{Q}\right\}$. То очевидно $H = \left\{\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix} \in G \;\middle|\; a = 1\right\}$. Значи пробваме с този критерий. Като търсим изображение $\psi : G \to \mathbb{Q}^*$, което е сюрективен хомоморфизъм и $\mathrm{Ker}(\psi) = H$.

$$\psi\left(\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}\right) = \psi\left(\begin{pmatrix}c & d\\ 0 & 1\end{pmatrix}\right) \longleftrightarrow \begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}.\begin{pmatrix}c & d\\ 0 & 1\end{pmatrix}^{-1} \in H \longleftrightarrow$$
$$\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}.\begin{pmatrix}c^{-1} & -d.c^{-1}\\ 0 & 1\end{pmatrix} \in H \longleftrightarrow \begin{pmatrix}ac^{-1} & b - adc^{-1}\\ 0 & 1\end{pmatrix} \in H \longleftrightarrow$$
$$ac^{-1} = 1 \longrightarrow a = c$$

Значи

$$\psi\left(\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}\right) = \psi\left(\begin{pmatrix}c & d\\ 0 & 1\end{pmatrix}\right) \longleftrightarrow a = c$$

Значи информацията, която искаме да прехвърляме е каква е стойността на елемента на първи ред и първи стълб. Ако $\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix} \in G$, то $a \in \mathbb{Q}^*$. Значи $\psi\left(\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}\right) = a$ е коректно дефинирано изображение от G към $\mathbb{Q}^*$. Ще покажем, че то ни върши работа.

1. $\psi\left(\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}.\begin{pmatrix}c & d\\ 0 & 1\end{pmatrix}\right) = \psi\left(\begin{pmatrix}ac & ad+b\\ 0 & 1\end{pmatrix}\right) =$
   $a.c = \psi\left(\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix}\right).\psi\left(\begin{pmatrix}c & d\\ 0 & 1\end{pmatrix}\right)$. Значи ψ е хомоморфизъм.
2. Искаме да видим, че ψ е сюрекция. Нека $q \in \mathbb{Q}^*$.
   Тогава $\begin{pmatrix}q & 0\\ 0 & 1\end{pmatrix} \in G$ и $\psi\left(\begin{pmatrix}q & 0\\ 0 & 1\end{pmatrix}\right) = q$. Значи ψ е сюрекция.
3. Както видяхме $H = \left\{\begin{pmatrix}a & b\\ 0 & 1\end{pmatrix} \in G \;\middle|\; a = 1\right\}$.
   Очевидно $H = \{g \in G \mid \psi(g) = 1\} = \mathrm{Ker}(\psi)$.

Така от първата теорема за хомоморфизмите $G/H \cong < \mathbb{Q}^*, 1, ., ()^{-1} >$ и H образува нормална подгрупа на $< G, E_2, ., ()^{-1} >$.

10 Задача от теория на числата

Нека $a, b \in \mathbb{Z}$ са такива, че $gcd(a, b) = 5$. Да се намери на колко може да е равно $gcd(13a + 36b, 2a + 5b)$?

10.1 Решение:

Нека $d = gcd(13a + 36b, 2a + 5b)$. Тогава

$$d = gcd(13a + 36b, 2a + 5b) = gcd(12a + a + 30b + 6b, 2a + 5b) =$$
$$gcd(6(2a + 5b) + a + 6b, 2a + 5b) = gcd(a + 6b, 2a + 5b) =$$
$$gcd(2a - a + 5b + b, 2a + 5b) = gcd(b - a, 2a + 5b).$$

Тогава $d \mid 5(b-a) + (-1)(2a+5b)$ значи $d \mid 7a$. Но $d \mid 2(b-a) + 1(2a+5b)$ значи $d \mid 7b$. Щом $d \mid 7a$ и $d \mid 7b$, то по дефиниция $d \mid gcd(7a, 7b)$. Но $gcd(7a, 7b) = 7.gcd(a, b) = 7.5$. Значи $d \mid 7.5$. Тогава $d \in \{1, 5, 7, 35\}$. Видяхме $d = gcd(b-a, 2a+5b)$. Но $5 \mid b-a$ и $5 \mid 2a+5b$ следователно $5 \mid d$. Значи остава $d \in \{5, 35\}$. Сега остава да проверим, кои от тези случай могат да се реализират. Търсим конкретни a и b така, че $gcd(a, b) = 5$ и $d = 5$. Да пробваме с $b = 5$ и $a = 0$. Първо ясно е, че $gcd(5, 0) = 5$. $gcd(5 - 0, 2.0 + 5.5) = gcd(5, 25) = 5$. Значи $d = 5$ при $b = 5$ и $a = 0$. Търсим конкретни a и b така, че $gcd(a, b) = 5$ и $d = 35$. Да пробваме с $b = 5$ и $a = 5$. Първо ясно е, че $gcd(5, 5) = 5$. $gcd(5 - 5, 2.5 + 5.5) = gcd(0, 7.5) = 7.5 = 35$. Значи $d = 35$ при $b = 5$ и $a = 5$.

Отговор: 5 и 35