УДК 512.53

©2012. **О. Г. Ганюшкін, Т. В. Турка**

ПРО ІДЕМПОТЕНТИ НАПІВГРУПИ ВІДПОВІДНОСТЕЙ

Доведено теорему про будову ідемпотентів напівгрупи відповідностей скінченної групи, зокрема, обчислено кількість ідемпотентів напівгруп відповідностей циклічної групи та елементарної абелевої групи.

Ключові слова: *ідемпотент, напівгрупа відповідностей.*

1. Вступ. Нехай G – універсальна алгебра. Якщо підалгебру з $G\times G$ розглядати як бінарне відношення на G, то множина $S(G)$ всіх підалгебр з $G\times G$ є напівгрупою відносно деморганівського добутку відношень. Напівгрупа $S(G)$ називається *напівгрупою відповідностей* алгебри G.

Задачу вивчення напівгруп відповідностей поставив ще в кінці 60-х років минулого століття відомий математик Курош О.Г. (див. [1]).

2. Ідемпотенти напівгрупи відповідностей. У роботі [2] показано, що коли G – група, то елементи напівгрупи $S(G)$ можна ототожнити з п'ятірками вигляду $(H_1, G_1, H_2, G_2, \varphi)$, де $H_1 \le G_1 < G$, $H_2 \le G_2 < G$, а φ – ізоморфізм факторгрупи G_1/H_1 на факторгрупу G_2/H_2. При цьому відповідний елемент напівгрупи $S(G)$ – як підмножина із $G\times G$ – має вигляд

$$(H_1, G_1, H_2, G_2, \varphi) = \bigcup_{a\in G_1} (aH_1 \times \varphi(aH_1)).$$

Множини вигляду $aH_1 \times bH_2$, де $bH_2 = \varphi(aH_1)$, будемо називати блоками елемента $A = (H_1, G_1, H_2, G_2, \varphi)$.

Теорема 1. *Нехай G – група. Елемент $A = (H_1, G_1, H_2, G_2, \varphi)$ напівгрупи відповідностей $S(G)$ буде ідемпотентом тоді і тільки тоді, коли*

$$G_2 \cap H_1 = H_1 \cap H_2 = G_1 \cap H_2,$$

і для класів суміжності G_1 за H_1 та G_2 за H_2 існує спільна система представників, яку ізоморфізм $\varphi : G_1/H_1 \to G_2/H_2$ зберігає (тобто $\varphi(a_iH_1) = a_iH_2$ для $i = 1, \ldots, k$).

Доведення. Необхідність. Нехай $A = (H_1, G_1, H_2, G_2, \varphi)$ – ідемпотент. Нехай

$$\begin{aligned} G_1 &= b'_1H_1 + b'_2H_1 + \ldots + b'_kH_1, \\ G_2 &= b''_1H_2 + b''_2H_2 + \ldots + b''_kH_2. \end{aligned} \tag{1}$$

Можна вважати, що

$$A = (b'_1H_1, b''_1H_2) + (b'_2H_1, b''_2H_2) + \ldots + (b'_kH_1, b''_kH_2). \tag{2}$$

Оскільки $(g_1H_1, g_2H_2) \circ (g_1'H_1, g_2'H_2) \subseteq (g_1H_1, g_2'H_2)$, то з ідемпотентності A випливає, що $(b_i'H_1, b_i''H_2) \circ (b_i'H_1, b_i''H_2) = (b_i'H_1, b_i''H_2)$. Тому $b_i''H_2 \cup b_i'H_1 \neq \varnothing$.

Нехай $a_i \in b_i''H_2 \cap b_i'H_1$. Тоді $b_i''H_2 = a_iH_2$ і $b_i'H_1 = a_iH_1$.

Розклади (1) набувають вигляду

$$G_i = a_1H_i + a_2H_i + \ldots + a_kH_i, \quad i = 1, 2.$$

Таким чином, для класів суміжності G_1 за H_1 і G_2 за H_2 існує спільна система представників $a_1, a_2, \ldots, a_k$. Крім того, розклад (2) набуває вигляду

$$A = (a_1H_1, a_1H_2) + (a_2H_1, a_2H_2) + \ldots + (a_kH_1, a_kH_2),$$

а тому $\varphi(a_iH_1) = a_iH_2$ для всіх $i = 1, 2, \ldots, k$.

Оскільки $A^2 = \bigcup\limits_{i,j=1}^{k} (a_iH_1, a_iH_2) \circ (a_jH_1, a_jH_2)$, то з ідемпотентності A випливає, що при $i \neq j$ має виконуватися рівність $a_iH_2 \cap a_jH_1 = \varnothing$, або, що рівносильно, рівність $H_1 \cap a_j^{-1}a_iH_2 = \varnothing$.

Але $\bigcup\limits_{i \neq j} a_j^{-1}a_iH_2 = G_2 \setminus H_2$. Тому $(G_2 \setminus H_2) \cap H_1 = \varnothing$ і $G_2 \cap H_1 = H_1 \cap H_2$.

Аналогічно доводиться, що $G_1 \cap H_2 = H_1 \cap H_2$.

Достатність. Нехай $A = (H_1, G_1, H_2, G_2, \varphi)$ – такий елемент, що

$$G_i = a_1H_i + a_2H_i + \ldots + a_kH_i, \quad i = 1, 2$$

і $\varphi(a_iH_1) = a_iH_2$. Тоді

$$A = (a_1H_1, a_1H_2) + (a_2H_1, a_2H_2) + \ldots + (a_kH_1, a_kH_2),$$

і $A^2 = \sum\limits_{i,j=1}^{k} (a_iH_1, a_iH_2) \circ (a_jH_1, a_jH_2)$.

Але $a_iH_2 \cap a_jH_1 \neq \varnothing$ тоді і тільки тоді, коли $a_j^{-1}a_iH_2 \cap H_1 \neq \varnothing$. Оскільки $G_2 \cap H_1 = H_2 \cap H_1$, то це буде тоді і тільки тоді, коли $a_j^{-1}a_iH_2 = H_2$, тобто тоді і тільки тоді, коли $i = j$. Тому

$$\sum_{i,j=1}^{k} (a_iH_1, a_iH_2) \circ (a_jH_1, a_jH_2) = \sum_{i=1}^{k} (a_iH_1, a_iH_2) \circ (a_iH_1, a_iH_2) = A$$

Отже, $A^2 = A$. □

3. Випадок циклічної групи.

Теорема 2. *Нехай C_n – циклічна група порядку n. Існує взаємно однозначна відповідність між ідемпотентами напівгрупи $S(C_n)$ і п'ятірками (k, l, m, u, v) натуральних чисел, які задовольняють такі умови:*

1) $k|l$, $l|u$, $u|n$, $k|m$, $m|v$, $v|n$;
2) НСД(m, u) = НСД$(l, v) = k$;
3) $\dfrac{u}{l} = \dfrac{v}{m}$.

Доведення. Нехай C_n – циклічна група порядку n і елемент $A = (H_1, G_1, H_2, G_2, \varphi)$ є ідемпотентом напівгрупи відповідностей $S(C_n)$, де $H_1 \le G_1 \le C_n$, $H_2 \le G_2 \le C_n$ і $G_1/H_1 \simeq G_2/H_2$.

Поставимо елементу A у відповідність такі п'ять чисел:

$$|H_1 \cap H_2| = k, \ \ |H_1| = l, \ \ |H_2| = m, \ \ |G_1| = u, \ \ |G_2| = v.$$

Оскільки $H_1 \cap H_2 \le H_i \le G_i \le C_n, \ \ i = 1, 2$, то

$$k|l, \ \ l|u, \ \ u|n, \quad \text{та} \quad k|m, \ \ m|v, \ \ v|n.$$

Отже, п'ятірка (k, l, m, u, v) задовольняє умову 1).

За теоремою 1 маємо $G_1 \cap H_2 = H_1 \cap G_2 = H_1 \cap H_2$, тому

$$\text{НСД}(m, u) = \text{НСД}(l, v) = k.$$

Отже умова 2) також виконується.

Нарешті з ізоморфності G_1/H_1 і G_2/H_2 випливає, що $\dfrac{u}{l} = \dfrac{v}{m}$. Це доводить умову 3).

Нехай тепер п'ятірка чисел (k, l, m, u, v) задовольняє умови 1) – 3). Оскільки в циклічній групі C_n для кожного дільника d числа n існує рівно одна підгрупа порядку d, то тим самим у групі C_n однозначно визначаються підгрупи G_1, G_2, H_1, H_2 порядків u, v, l, m відповідно, причому $H_1 \le G_1, \ \ H_2 \le G_2$.

Із умов 1) і 2) тоді випливає, що

$$G_2 \cap H_1 = H_1 \cap H_2 = G_1 \cap H_2 \quad \text{і} \quad |H_1 \cap H_2| = k.$$

Із теореми 1 випливає, що для існування такого ізоморфізму $\varphi : G_1/H_1 \to G_2/H_2$, для якого елемент $(H_1, G_1, H_2, G_2, \varphi)$ буде ідемпотентом, досить показати існування спільної системи представників для класів суміжності G_1 за H_1 і G_2 за H_2. Доведення існування такої системи представників розіб'ємо на кілька кроків.

I. Зауважимо, що коли $A = A_1 \times A_2 \times \ldots \times A_q$, де порядки $|A_1|$, $|A_2|$, $\ldots$, $|A_q|$ множників попарно взаємно прості, то кожна підгрупа $B \le A$ має вигляд $B = B_1 \times B_2 \times \ldots \times B_q$, де $B_1 \le A_1$, $B_2 \le A_2$, $\ldots$, $B_q \le A_q$.

II. Якщо існують спільна система представників для A_1 за B_1 і A_2 за B_2 і спільна система представників представників для A_1' за B_1' і A_2' за B_2', то існує спільна система представників для $A_1 \times A_1'$ за $B_1 \times B_1'$ і $A_2 \times A_2'$ за $B_2 \times B_2'$.

Справді, із рівностей

$$A_1 = a_1B_1 + a_2B_1 + \ldots + a_tB_1, \ \ A_2 = a_1B_2 + a_2B_2 + \ldots + a_tB_2$$

і

$$A_1' = b_1B_1' + b_2B_1' + \ldots + b_tB_1', \ \ A_2' = b_1B_2' + b_2B_2' + \ldots + b_tB_2'$$

випливає, що

$$A_1 \times A_1' = \sum_{i,j} (a_i, b_j) B_1 \times B_1',$$

$$A_2 \times A_2' = \sum_{i,j} (a_i, b_j) B_2 \times B_2'.$$

III. Нехай тепер $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_q^{\alpha_q}$. Тоді

$$C_n = C_{p_1^{\alpha_1}} \times C_{p_2^{\alpha_2}} \times \cdots \times C_{p_q^{\alpha_q}}.$$

Позначимо через C_{p^α} довільний множник цього розкладу і нехай

$$G_1^* = G_1 \cap C_{p^\alpha}, \;\; G_2^* = G_2 \cap C_{p^\alpha}, \;\; H_1^* = H_1 \cap C_{p^\alpha}, \;\; H_2^* = H_2 \cap C_{p^\alpha}.$$

Крім того, для підгрупи $(H_1 \cap H_2)^* = (H_1 \cap H_2) \cap C_{p^\alpha}$ маємо $(H_1 \cap H_2)^* = H_1^* \cap H_2^*$. Позначимо

$$|G_1^*| = p^{\beta_1}, \qquad |G_2^*| = p^{\beta_2}, \qquad |H_1^*| = p^{\gamma_1}, \qquad |H_2^*| = p^{\gamma_2}, \qquad |H_1 \cap H_2| = p^{\delta}.$$

Із кроків I і II випливає, що для існування спільної системи представників G_1 за H_1 і G_2 за H_2 досить показати існування спільної системи представників G_1^* за H_1^* і G_2^* за H_2^*. Умови 1) – 3) тепер набувають вигляду:

$1'$) $\delta \le \gamma_1 \le \beta_1 \le \alpha, \quad \delta \le \gamma_2 \le \beta_2 \le \alpha,$

$2'$) $\min(\gamma_2, \beta_1) = \min(\gamma_1, \beta_2) = \delta,$

$3'$) $\beta_1 - \gamma_1 = \beta_2 - \gamma_2.$

Припустимо, що $\delta = \gamma_1$ (випадок $\delta = \gamma_2$ розбирається аналогічно). Якщо при цьому $\delta = \gamma_2$, то із $3'$) випливає, що $\beta_1 = \beta_2$. Але тоді $G_1^* = G_2^*$, $H_1^* = H_2^*$ і існування спільної системи представників очевидна. Якщо ж $\gamma_2 > \delta$, то із $2'$) випливає, що $\beta_1 = \delta$, а після цього із $3'$) випливає, що $\beta_2 = \gamma_2$.

Але тоді $G_1^* = H_1^*$ і $G_2^* = H_2^*$. Отже, маємо лише по одному класу суміжності, і спільним представником можна взяти одиницю e. □

Наслідок 1. *Якщо $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ – канонічний розклад числа n, то кількість ідемпотентів у напівгрупі $S(C_n)$ однозначно визначається мультимножиною $\{k_1, k_2, \ldots, k_t\}$ показників.*

Доведення. Нехай $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ – канонічний розклад числа n, а числа п'ятірки (k, l, m, u, v) мають наступні розклади: $k = p_1^{a_1} \cdots p_t^{a_t}$, $l = p_1^{b_1} \cdots p_t^{b_t}$, $m = p_1^{c_1} \cdots p_t^{c_t}$, $u = p_1^{d_1} \cdots p_t^{d_t}$, $v = p_1^{g_1} \cdots p_t^{g_t}$. Тоді умови теореми 2 будуть залежати лише від показників степенів простих чисел $p_1, p_2, \ldots, p_m$, тобто кількість ідемпотентів однозначно визначається мультимножиною $\{k_1, k_2, \ldots, k_m\}$ показників. □

Теорема 3. *Якщо p – просте число і C_{p^n} – циклічна група порядку p^n, то кількість ідемпотентів у напівгрупі відповідностей $S(C_{p^n})$ буде обчислюватися за формулою*

$$|E(S(C_{p^n}))| = (n+1) \cdot \left(\frac{2+3n}{2} \right).$$

Доведення. Нехай C_{p^n} – циклічна група порядку p^n. Згідно теореми 2 ідемпотенти напівгрупи відповідностей знаходяться у взаємно однозначній відповідності з п'ятірками чисел (k, l, m, u, v), які задовольняють умови 1)-3) теореми 2. Далі замість п'ятірки $(k, l, m, u, v) = (p^{a_1}, p^{a_2}, p^{a_3}, p^{a_4}, p^{a_5})$ зручно розглядати п'ятірку показників $(a_1, a_2, a_3, a_4, a_5)$.

Умову 1) тепер можна переписати у вигляді

$$a_1 = a, \quad a_2 = a + \alpha, \quad a_3 = a + \gamma, \quad a_4 = a + \alpha + \beta, \quad a_5 = a + \gamma + \delta,$$

де $a, \alpha, \beta, \gamma, \delta$ – деякі невід'ємні цілі числа.

Умови 2)-3) тоді набувають вигляду

$$\begin{cases} \min\,(a+\gamma, a+\alpha+\beta) = \min\,(a+\alpha, a+\gamma+\delta) = a, \\ \beta = \delta. \end{cases}$$

Звідси

$$\min\,(a+\gamma, a+\alpha+\beta) = \min\,(a+\alpha, a+\gamma+\beta) = a.$$

Розглянемо два випадки:

1) Нехай $\gamma \neq 0$. Тоді $\alpha + \beta = 0$, звідки $\alpha = \beta = 0$. Після цього у нас лишається лише умова $0 \leq a < a + \gamma \leq n$, а тому параметри (a, γ) можна вибрати $\begin{pmatrix} n+1 \\ 2 \end{pmatrix}$ способами.

2) Нехай тепер $\gamma = 0$. Цей випадок розпадається на 3 підвипадки:

$2'$) $\gamma = \alpha = 0$, $\beta \neq 0$. У цьому випадку все зводиться до нерівності $0 \leq a < a + \beta \leq n$, тому пару (α, β) можна вибрати $\begin{pmatrix} n+1 \\ 2 \end{pmatrix}$ способами.

$2''$) $\gamma = \beta = 0$, $\alpha \neq 0$. Аналогічно попередньому отримуємо нерівність $0 \leq a < a + \alpha \leq n$ і $\begin{pmatrix} n+1 \\ 2 \end{pmatrix}$ способів вибору пари (a, α).

$2'''$) $\gamma = \alpha = \beta = 0$. У цьому випадку лишається лише умова $0 \leq a \leq n$, тому a можна вибрати $n + 1$ способом.

Підсумовуючи все, одержуємо:

$$|E(S(C_{p^n}))| = (n+1) + 3\begin{pmatrix} n+1 \\ 2 \end{pmatrix} = (n+1) \cdot \left(\frac{2+3n}{2}\right). \qquad \square$$

Теорема 4. *Якщо C_n – циклічна група порядку n, де $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ – канонічний розклад числа n, то кількість ідемпотентів у напівгрупі відповідностей $S(C_p)$ обчислюється за формулою*

$$|E(S(C_n))| = \prod_{i=1}^{t} (k_i + 1) \cdot \left(\frac{2+3k_i}{2}\right).$$

Доведення. За теоремою 2 число $|E(S(C_n))|$ дорівнює кількості тих п'ятірок (k, l, m, u, v), які задовольняють умови 1)-3).

Нехай

$$k = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t},\ l = p_1^{b_1} p_2^{b_2} \dots b_t^{b_t},\ m = p_1^{c_1} p_2^{c_2} \dots p_t^{c_t},$$
$$u = p_1^{d_1} p_2^{d_2} \dots p_t^{d_t},\ v = p_1^{g_1} p_2^{g_2} \dots p_t^{g_t}.$$

Умови 1)-3) тоді будуть рівносильні таким:

1) $k|l \iff a_1 \le b_1, \ldots, a_t \le b_t$, $l|u \iff b_1 \le d_1, \ldots, b_t \le d_t$, $u|n \iff d_1 \le k_1, \ldots, d_t \le k_t$,

$k|m \iff a_1 \le c_1, \ldots, a_t \le c_t$, $m|v \iff c_1 \le g_1, \ldots, c_t \le g_t$, $v|n \iff g_1 \le k_1, \ldots, g_t \le k_t$.

2) НСД (u, m) = НСД (l, v) = k тоді і тільки тоді, коли $\min(d_1, c_1) = \min(b_1, g_1) = a_1$, …, $\min(d_t, c_t) = \min(b_t, g_t) = a_t$.

3) $u \cdot m = l \cdot v$ тоді і тільки тоді, коли $c_1 + d_1 = b_1 + g_1$, …, $c_t + d_t = b_t + g_t$.

Таким чином, для кожного i $(1 \le i \le t)$ все зводиться до відповідних умов для циклічної групи $C_{p_i^{k_i}}$, причому для різних i відповідні параметри можна вибирати незалежно. Тому з теореми 3 отримуємо:

$$|E(S(C_n))| = |E(S(C_{p_1^{k_1}}))| \cdot |E(S(C_{p_2^{k_2}}))| \cdot \ldots \cdot |E(S(C_{p_t^{k_t}}))| =$$

$$= \prod_{i=1}^{t} (k_i + 1) \cdot \left(\frac{2 + 3k_i}{2} \right). \qquad \square$$

4. Випадок елементарної абелевої групи. Для довільного числа p позначимо

$$\psi_k(p) = \begin{cases} 1, \text{ якщо } k = 0, \\ (p-1)(p^2-1)\cdots(p^k-1), \text{ якщо } k > 0. \end{cases}$$

Число $\psi_k(p)$ дорівнює кількості способів вибору бази в k-вимірному векторному просторі над полем Z_p.

Крім того, через $\begin{pmatrix} n \\ k \end{pmatrix}_p$ позначається кількість k-вимірних підпросторів n-вимірного простору над простим полем Z_p. Число $\begin{pmatrix} n \\ k \end{pmatrix}_p$ називається коефіцієнтом Гаусса. Як відомо,

$$\begin{pmatrix} n \\ k \end{pmatrix}_p = \frac{1}{p^{k(n-k)}} \cdot \frac{\psi_n(p)}{\psi_k(p)\psi_{n-k}(p)}.$$

Теорема 5. *Кількість ідемпотентів у напівгрупі відповідностей $S(Z_p^n)$ елементарної абелевої групи Z_p^n дорівнює:*

$$|E(S(Z_p^n))| = \sum_{i=0}^{n} \left[\begin{pmatrix} n \\ i \end{pmatrix}_p \cdot \sum_{m_1+m_2=0}^{n-i} \left(p^{m_1 m_2} \begin{pmatrix} n-i \\ m_1+m_2 \end{pmatrix}_p \cdot \begin{pmatrix} m_1+m_2 \\ m_1 \end{pmatrix}_p \times \right.\right.$$

$$\left.\left. \times \left(1 + \sum_{r=1}^{n-i-m_1-m_2} p^{(m_1+m_2-i)r} \cdot \frac{\psi_{n-i-m_1-m_2}(p)}{\psi_r(p)} \right) \right) \right].$$

Доведення. Нехай Z_p^n – елементарна абелева група. Нам буде зручно розглядати Z_p^n як n-вимірний простір над полем Z_p.

Нехай елемент $A = (H_1, G_1, H_2, G_2, \varphi)$ є ідемпотентом напівгрупи відповідностей $S(Z_p^n)$. Позначимо $H = H_1 \cap H_2$ і перейдемо до факторпросторів

$$U = Z_p^n/H,\ \ P_1 = H_1/H,\ \ P_2 = H_2/H,\ \ R_1 = G_1/H,\ \ R_2 = G_2/H.$$

За теоремою 1 існують розклади

$$G_1 = a_1H_1 + a_2H_1 + \ldots + a_tH_1,\ \ G_2 = a_1H_2 + a_2H_2 + \ldots + a_tH_2.$$

Це дає нам розклади

$$R_1 = b_1P_1 + b_2P_1 + \ldots + b_tP_1,\ \ R_2 = b_1P_2 + b_2P_2 + \ldots + b_tP_2,$$

де $b_i = a_i + H$ – відповідний елемент факторпростору U.

Система представників $b_1, \ldots, b_k$ визначена однозначно. Справді, $P_1 \cap P_2 = \{0\}$. Тому з рівностей $b_iP_1 = b_i'P_1$, $b_iP_2 = b_i'P_2$ маємо: $b_i' = b_i + c_1 = b_i + c_2$, де $c_j \in P_i$.

Але тоді $c_1 = c_2$, звідки $c_1 = c_2 = 0$, а тому $b_i' = b_i$.

Це означає, що для довільного i буде $b_iP_1 \cap b_iP_2 = \{b_i\}$. Але тоді з рівностей

$$b_iP_j + b_lP_j = (b_i + b_l)P_j,\ \ j = 1, 2 \quad \text{та} \quad c \cdot (b_iP_j) = cb_i \cdot P_j,\ \ j = 1, 2$$

випливає, що множина $Q = \{b_1, \ldots, b_k\}$ замкнена відносно додавання і множення на скаляри, а тому утворює підпростір простору U.

Із розкладів

$$R_1 = b_1P_1 + b_2P_1 + \ldots + b_tP_1, \quad R_2 = b_1P_2 + b_2P_2 + \ldots + b_tP_2$$

випливає, що

$$R_1 = P_1 \oplus Q, \quad R_2 = P_2 \oplus Q.$$

Таким чином, із кожним ідемпотентом A пов'язується деякий підпростір $H \leq Z_p^n$ і трійка P_1, P_2, Q підпросторів простору $U = Z_p^n/H$, які попарно перетинаються по 0.

Навпаки, нехай H – підпростір Z_p^n і P_1, P_2, Q – трійка підпросторів простору $U = Z_p^n/H$, які попарно перетинаються по 0. Розглянемо $R_1 = P_1 \oplus Q$, $R_2 = P_2 \oplus Q$ і нехай H_1, H_2, G_1, G_2 – прообрази підпросторів P_1, P_2, R_1, R_2 відповідно при канонічному епіморфізмі $Z_p^n \longrightarrow Z_p^n/H$. За спільну систему представників класів суміжності G_1 за H_1 і G_2 за H_2 можна взяти прообрази елементів із Q при цьому епіморфізмі. Тоді відображення $\varphi : G_1/H_1 \to G_2/H_2$, яке зберігає спільні представники, буде, очевидно, ізоморфізмом.

Оскільки побудована таким чином п'ятірка $(H_1, G_1, H_2, G_2, \varphi)$ задовольняє всі умови теореми 1, то відповідний елемент напівгрупи $S(Z_p^n)$ буде ідемпотентом.

Таким чином, кількість ідемпотентів напівгрупи $S(Z_p^n)$ дорівнює кількості наборів (H, P_1, P_2, Q), де H – підпростір із Z_p^n, а P_1, P_2, Q – така трійка підпросторів із Z_p^n/H, які попарно перетинаються по 0.

Для підрахунку таких наборів спочатку вибираємо підпростір $H \leq Z_p^n$. Нехай $\dim H = i$. Тоді H можна вибрати $\left(\begin{array}{c} n \\ i \end{array} \right)_p$ способами.

Нехай $\dim P_1 = m_1$, $\dim P_2 = m_2$. Оскільки $P_1 \cap P_2 = \{0\}$, то об'єднання баз просторів P_1 і P_2 є базою простору $P_1 \oplus P_2$. Базу простору $P_1 \oplus P_2$ можна вибрати

$$(p^{n-i}-1)(p^{n-i}-p)\cdots(p^{n-i}-p^{m_1-1})\cdots(p^{n-i}-p^{m_1+m_2-1}) =$$

$$= \frac{\psi_{n-i}(p)}{p^{(m_1+m_2)(n-i-m_1-m_2)}\psi_{n-i-m_1-m_2}(p)}$$

способами.

Перші m_1 векторів цієї бази дадуть нам базу підпростору P_1, решта m_2 векторів – базу P_2. Оскільки $\psi_{m_1}(p)$ різних баз підпростору P_1 будуть давати один і той підпростір P_1 (і аналогічно для підпростору P_2), то загальна кількість пар (P_1, P_2) дорівнює

$$\frac{\psi_{n-i}(p)}{p^{(m_1+m_2)(n-i-m_1-m_2)}\psi_{n-i-m_1-m_2}(p)\psi_{m_1}(p)\psi_{m_2}(p)} =$$

$$= p^{m_1 m_2}\left(\begin{array}{c} n-i \\ m_1+m_2 \end{array} \right)_p \left(\begin{array}{c} m_1+m_2 \\ m_1 \end{array} \right)_p.$$

Позначимо через $S(m_1, m_2, k)$ кількість тих k-вимірних підпросторів простору $P_1 \oplus P_2$, які мають нульовий перетин, як із P_1, так і з P_2.

Нехай $\overline{Q}$ – один із таких підпросторів, $a_1 + b_1$, $a_2 + b_2$, …, $a_k + b_k$ – база $\overline{Q}$, де $a_1, a_2, \ldots, a_k \in P_1$, $b_1, b_2, \ldots, b_k \in P_2$. Легко зрозуміти, що вектори $a_1, a_2, \ldots, a_k$ – лінійно незалежні. Справді, нехай $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k = 0$. Тоді

$$\alpha_1(a_1+b_1) + \alpha_2(a_2+b_2) + \ldots + \alpha_k(a_k+b_k) = \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_k b_k \in P_2.$$

З іншого боку, $\alpha_1(a_1+b_1)+\alpha_2(a_2+b_2)+\ldots+\alpha_k(a_k+b_k) \in \overline{Q}$. Оскільки $P_2 \cap \overline{Q} = \{0\}$, то $\alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_k b_k = 0$, звідки $\alpha_1 = \alpha_2 = \ldots = \alpha_k$.

Навпаки, нехай $a_1, a_2, \ldots, a_k$ – лінійно незалежні вектори з P_1, а $b_1, b_2, \ldots, b_k$ – лінійно незалежні вектори з P_2. Тоді вектори $a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k$ – також лінійно незалежні. Справді, якщо

$$\alpha_1(a_1+b_1) + \alpha_2(a_2+b_2) + \ldots + \alpha_k(a_k+b_k) = 0,$$

то

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k = -(\alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_k b_k).$$

Але

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k \in P_1, \qquad \alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_k b_k \in P_2$$

і $P_1 \cap P_2 = \{0\}$. Тому $\alpha_1 = \alpha_2 = \ldots = \alpha_k = 0$.

Підпростір $\overline{Q} = \langle a_1+b_1, a_2+b_2, \ldots, a_k+b_k\rangle$ буде мати нульовий перетин із кожним із просторів P_1 і P_2. Справді, нехай

$$\alpha_1(a_1+b_1)+\alpha_2(a_2+b_2)+\ldots+\alpha_k(a_k+b_k)=v\in P_1.$$

Тоді

$$\alpha_1a_1+\alpha_2a_2+\ldots+\alpha_ka_k=v-(\alpha_1b_1+\alpha_2b_2+\ldots+\alpha_kb_k)\in P_1,$$

а оскільки $\alpha_1b_1+\alpha_2b_2+\ldots+\alpha_kb_k\in P_2$і $P_1\cap P_2=\{0\}$, то

$$\alpha_1b_1+\alpha_2b_2+\ldots+\alpha_kb_k=0 \ \text{ і } \ \alpha_1=\alpha_2=\ldots=\alpha_k=0.$$

Аналогічно доводиться, що $\overline{Q}\cap P_2=\{0\}$.

Тому всі k-вимірні підпростори із $P_1\oplus P_2$, які мають нульовий перетин із кожним із P_1 та P_2, можна одержати таким чином: вибираємо довільні лінійно незалежні вектори $a_1, a_2, \ldots, a_k$ в P_1 і лінійно незалежні вектори $b_1, b_2, \ldots, b_k$ в P_2 і кладемо $\overline{Q}=\langle a_1+b_1, a_2+b_2, \ldots, a_k+b_k\rangle$. При цьому кожен простір $\overline{Q}$ буде отримуватися з такою кратністю, скількома способами в ньому можна вибрати базу. Тому

$$S(m_1,m_2,k)=\frac{1}{\psi_k(p)}\cdot\frac{\psi_{m_1}(p)}{p^{k(m_1-k)}\cdot\psi_{m_1-k}(p)}\cdot\frac{\psi_{m_2}(p)}{p^{k(m_2-k)}\cdot\psi_{m_2-k}(p)}=$$

$$=\frac{1}{p^{k(m_1+m_2-2k)}}\cdot\frac{\psi_{m_1}(p)\psi_{m_2}(p)}{\psi_k(p)\psi_{m_1-k}(p)\psi_{m_2-k}(p)}.$$

Але простір $\overline{Q}=Q\cap(P_1\oplus P_2)$ треба "роздути" до Q. При $r>0$ k-вимірний простір $Q\cap(P_1\oplus P_2)$ можна "роздути" до $(k+r)$-вимірного простору Q

$$\frac{(p^{n-i}-p^{m_1+m_2})(p^{n-i}-p^{m_1+m_2+1})\ldots(p^{n-i}-p^{m_1+m_2+r-1})}{(p^{r+k}-p^k)(p^{r+k}-p^{k+1})\ldots(p^{r+k}-p^{r+k-1})}=$$

$$=p^{(m_1+m_2-k)r}\cdot\frac{\psi_{n-i-m_1-m_2}(p)}{\psi_r(p)}$$

способами. Тому загальна кількість $B(m_1,m_2,i)$ способів "роздути" $Q\cap(P_1\oplus P_2)$ до простору Q дорівнює:

$$B(m_1,m_2,i)=1+\sum_{r=1}^{n-i-m_1-m_2}p^{(m_1+m_2-i)r}\cdot\frac{\psi_{n-i-m_1-m_2}(p)}{\psi_r(p)}.$$

Отже, кількість ідемпотентів напівгрупи $S(Z_p^n)$ дорівнює

$$|E(S(Z_p^n))|=\sum_{i=0}^{n}\left[\begin{pmatrix}n\\i\end{pmatrix}_p\cdot\sum_{m_1+m_2=0}^{n-i}\left(p^{m_1m_2}\begin{pmatrix}n-i\\m_1+m_2\end{pmatrix}_p\cdot\begin{pmatrix}m_1+m_2\\m_1\end{pmatrix}_p\times\right.\right.$$

$$\left.\left.\times\left(1+\sum_{r=1}^{n-i-m_1-m_2}p^{(m_1+m_2-i)r}\cdot\frac{\psi_{n-i-m_1-m_2}(p)}{\psi_r(p)}\right)\right)\right]. \qquad \square$$

1. *Курош А.Г.* Общая алгебра (лекции 1969-70 учебного года). – М.: Наука, 1974. – 160 с.
2. *Ганюшкін О.Г., Турка Т.В.* Порядок напівгрупи відповідностей скінченної групи // Вісник Київського університету. – 2009. – Вып. 3. Серія: фіз.-мат. науки. – С. 9-13.

O. G. Ganyushkin, T. V. Turka

The idempotents of semigroup of correspondences.

The theorem about of the structure of idempotents of semigroups of correspondence of the finite group has been proved and the amount of idempotents of semigroups of correspondence cyclic and elementary abelian groups has been calculated.

Keywords: *idempotent, the semigroup of correspondences.*

О. Г. Ганюшкин, Т. В. Турка

Об идемпотентах полугруппы соответствий.

Доказана теорема о строении идемпотентов полугруппы соответствий конечной группы, в частности, вычислено количество идемпотентов полугрупп соответствий циклической группы и элементарной абелевой группы.

Ключевые слова: *идемпотент, полугруппа соответствий.*

Київський національний ун-т ім. Шевченка
Слов'янський державний педагогічний ун-т
ganiyshk@univ.kiev.ua
tvturka@mail.ru

Получено 07.05.12