Тепер застосуємо критерій Банаха, за яким з умови, що простір $X \subset S$ буде m_1 – скелетоїдом в просторі $S \approx S \times S$, випливає гомеоморфність пар. Теорему 3 доведено.

Three theorems about geometric properties of iterated functors are proved.

1. Атаманюк Б.В. Нескінченні ітерації досконало метризованих функторів. Некомпактний випадок // Вісник Прикарпатського університету.Серія природничо-математичних наук –1996. -В.2.- С.42- 46.
2. Атаманюк Б.В. Поповнення нескінченної ітерації досконало метризованого функтора та пари нескінченних ітерацій // Вісник Прикарпатського університету. Серія природничо-математичних наук. – 1995.- В.1.- С.36-40.
3. Атаманюк Б.В. Функторы итерированного суперрасширения // Вестник МГУ. Серия Механика, Математика. – 1989.-с.95- 96.
4. Атаманюк Б.В. Представление $\sum \times S$ в виде бесконечного итерированного гиперпространства польских пространств // Общая топология: пространства и отображения. Изд-во МГУ.-1989.- С.119-124.
5. Федорчук В.В. Тройки бесконечных итераций совершенно метризуемых функторов // Известия АН СССР. Серия математическая. -1990. –Т.54. - №2.- С.396-417.

Н. М. Дяків, В. М. Пилипів

НІЛЬПОТЕНТНІ ТА ІДЕМПОТЕНТНІ ЕЛЕМЕНТИ В КІЛЬЦІ КЛАСІВ ЛИШКІВ, ЇХ ОБЧИСЛЕННЯ

В роботі розроблено методи обчислення ідемпотентних та нільпотентних елементів у кільці класів лишків $Z/_m$ для довільного модуля m.

Розглянемо теореми, які стосуються кількості та обчислення нільпотентних елементів у кільці класів лишків $Z/_m$.

Якщо m – просте число, то $Z/_m$ є полем, отже, в ньому не існує дільників нуля, а тому єдиним нільпотентним елементом є нульовий.

Теорема 1. Нехай $m = p_1 p_2 ... p_n$, де всі p_i – прості. Тоді в кільці $Z/_m$ нуль є нільпотентом, причому єдиним.

Доведення. Нуль дійсно є нільпотентом, бо вже при $k = 1$ $0^k = 0$.

Нехай в кільці $Z/_m$ існує ще один нільпотент l, такий, що $l \in \{1, 2, ..., m\}$ і $\exists k \in N: l^k = 0$, тобто $l^k \equiv 0 (\bmod m)$, але $m = p_1 p_2 ... p_n$, тобто остання конгруенція рівносильна системі конгруенцій за простими модулями

$$\begin{cases} l^k \equiv 0(\mathrm{mod}\, p_1), \\ l^k \equiv 0(\mathrm{mod}\, p_2), \\ \dots\dots\dots \\ l^k \equiv 0(\mathrm{mod}\, p_n), \end{cases}$$

тобто l є нільпотентом в Z/p_1, Z/p_2, ... Z/p_n, де всі p_i – прості, а при простому p нільпотентом є лише нуль. Тому l дорівнює нулю.

Теорема 2. Якщо $m = p^n$, p – просте число, $n \in N$, то в кільці $Z/_m$ є рівно p^{n-1} нільпотентів, причому кожен з них можна подати як елемент множини $A = \{l = ip,\ i \in \{1, 2, \dots, p^{n-1}\}\}$.

Доведення.

1) Нехай $l = ip$, доведемо, що l – нільпотент, тобто що існує $k \in N:\ l^k \equiv 0\ (\mathrm{mod}\, p^n)$, тобто $l^k = (ip)^k \equiv 0(\mathrm{mod}\ p^n)$. Очевидним k, при якому це виконується, є $k = n$ (хоча може існувати $k_1 < n:\ l^{k_1} \equiv 0(\mathrm{mod}\, p^n))$.

2) Доведемо, що всі числа з множини A неконгруентні між собою. Припустимо протилежне: нехай $ip \equiv jp(\mathrm{mod}\, p^n)$, $ip, jp \in A$. Тоді $i - j \equiv 0(\mathrm{mod}\ p^{n-1})$, тобто $i - j = tp^{n-1}$, але $0 < i \le p^{n-1}, 0 < j \le p^{n-1}$. Тоді $-p^{n-1} < i - j < p^{n-1}$, що можливо тільки при $t = 0$, $i = j$. Отже, множина A складається з p^{n-1} неконгруентних між собою елементів, кожен з яких є нільпотентом в $Z/_m$.

3) Доведемо, що кожен нільпотент з повної системи лишків рівний деякому елементу з множини A.

Нехай l є нільпотентом в $Z/_m$, тобто існує $k \in N : l^k \equiv 0\,(\mathrm{mod}\, p^n)$, $l \in \{1, 2, \dots, p^n\}$. Доведемо, що існує $i \in \{1, 2, \dots, p^{n-1}\}$, таке, що $l = ip$.

Якщо $l = p^n$, то $l \equiv 0(\mathrm{mod}\ m)$ і l можна подати як $l = p^{n-1} \cdot p$, тобто $i = p^{n-1}$.

Нехай $1 \le l \le p^{n-1}$. Тоді $l^k \equiv 0(\mathrm{mod}\ p^n)$ рівносильно тому, що l^k кратне p, p за умовою просте, тоді l кратне p. Дійсно, l^k кратне p, тоді $l^k = ap$, $l = m_1^{\alpha_1} m_2^{\alpha_2} \dots m_j^{\alpha_j}$ – канонічний розклад числа l. Тоді $l^k = m_1^{k\alpha_1} m_2^{k\alpha_2} \dots m_j^{k\alpha_j} = ap$, отже, $\exists\, 1 \le s \le j$, таке, що $m_s^{k\alpha_s}$ кратне p; оскільки m_s і p – прості, тому $m_s = p, 1 \le s \le j$. Тоді l кратне p.

Запишемо через рівність: $l = ap$, $1 \le l \le p^n$, звідси $1 \le a < p^{n-1}$, тобто, поклавши $i = a$, отримаємо, що l можна подати як елемент множини A.

Отже, між множиною нільпотентів в $Z/_m$ та елементами множини A існує взаємнооднозначна відповідність.

Теорема 3. Якщо $m = p_1^k p_2 ... p_n$ – канонічний розклад числа m, то в кільці $Z/_m$ є рівно p_1^{k-1} нільпотентів. Кожен з них є елементом множини $A = \{l = ip_1 p_2 ... p_n,\ i = 1, 2, ..., p_1^{k-1}\}$. (1)

Доведення. Доведення проведемо в кілька етапів.

Всі елементи множини A є нільпотентами, оскільки $\exists\ s = k \in N$:

$l^s = (ip_1 p_2 ... p_n)^k = (p_1^k p_2 ... p_n)(ip_2^{k-1} ... p_n^{k-1}) \equiv 0 (\mathrm{mod}\ m)$.

2) Покажемо, що всі елементи множини A неконгруентні між собою. Дійсно, припустимо, що

$$ip_1 p_2 ... p_n \equiv jp_1 p_2 ... p_n\ (\mathrm{mod}\ p_1^k p_2 ... p_n).$$

Тоді $i \equiv j (\mathrm{mod}\ p_1^{k-1})$, але $-p^{n-1} < i - j < p^{n-1}$, тому $i = j$.

Покажемо, що кожен нільпотент $l \in \{1, 2, ..., p_1^k p_2 ... p_n\}$ є елементом множини A, тобто може бути представлений у вигляді (1).

Оскільки l – нільпотент, то $\exists\ s \in N : l^s \equiv 0\ (\mathrm{mod}\ p_1^k p_2 ... p_n)$. Всі p_j, $j = 1, 2, ..., n$ взаємнопрості, тоді

$$\begin{cases} l^s \equiv 0 (\mathrm{mod}\ p_1^k), \\ l^s \equiv 0 (\mathrm{mod}\ p_2), \\ \cdots \\ l^s \equiv 0 (\mathrm{mod}\ p_n), \end{cases} \Rightarrow \begin{cases} l = ap_1\ (\text{згідно теореми 2}), \\ l\ \text{кратне}\ p_2\ (\text{згідно теореми 2}), \\ \cdots \\ l\ \text{кратне}\ p_n, \end{cases} \Rightarrow l = ip_1 p_2 ... p_n$$

За умовою, $1 \le l \le p_1^k p_2 ... p_n$, тоді $1 \le i \le p_1^{k-1}$, тобто $l \in A$.

Аналогічну теорему можна сформулювати і для випадку довільного модуля m.

Теорема 4. Нехай $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$. Тоді в кільці $Z/_m$ є рівно $p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} ... p_n^{\alpha_n - 1}$ нільпотентів. Кожен з них можна подати у вигляді:

$l = ip_1 p_2 ... p_n$, де $i \in \{1, 2, ..., p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} ... p_n^{\alpha_n - 1}\}$.

Перейдемо до розгляду теорем, які стосуються обчислення ідемпотентних елементів в кільці класів лишків $Z/_m$. У роботі [2] показано, що коли до розкладу модуля m входить k різних простих чисел, то в кільці $Z/_m$ існує 2^k різних ідемпотентів.

При великих m безпосереднє обчислення ідемпотентів за означенням стає практично неможливим, тому їх потрібно шукати, спираючись на властивості ідемпотентів. Доведемо спочатку наступні теореми.

Теорема 5. При $m = p^s$, де s – просте, Z/m має тільки тривіальні ідемпотенти 0 та 1.

Доведення. Нехай l – ідемпотент в Z/m, тобто $l \in \{1,2,...,m\}$ і $l^2 \equiv l(\mathrm{mod}\, m)$ або

$$l(l-1) \equiv 0(\mathrm{mod}\, p^s) \iff \left[\begin{array}{l} l \equiv 0(\mathrm{mod}\, p^s) \\ l \equiv 1(\mathrm{mod}\, p^s) \end{array}\right.$$

За умовою, $l < p^s$, тоді $\left[\begin{array}{l} l = 0 \\ l = 1 \end{array}\right.$.

Теорема 6. Нехай i – ідемпотент в кільці Z/m. Тоді елемент $m-i+1$ теж є ідемпотентом в даному кільці.

Доведення. Дано, що $i^2 - i \equiv 0 \ (\mathrm{mod}\, m)$.

Тоді

$$(m-i+1)^2 \equiv m^2 + i^2 + 1 - 2mi - 2i + 2m \equiv i^2 - 2i + 1 \equiv 1 - i \equiv m - i + 1 \ (\mathrm{mod}\, m).$$

А це означає, що елемент $m-i+1$ також є ідемпотентом у даному кільці.

Наслідок. При відшуканні ідемпотентів у даному кільці досить знайти всі ідемпотенти серед чисел $A = \{1,2,...[\frac{m}{2}]\}$. Інші ідемпотенти знаходяться за формулою $m-i+1$, де i - всі ідемпотенти з множини A.

Нехай $i < \left[\frac{m}{2}\right]$ та i є ідемпотентом в кільці Z/m, $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, тоді, згідно означення, $i^2 - i \equiv 0(\mathrm{mod}\, p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n})$, або

$$\left|\begin{array}{l} i^2 - i \equiv 0(\mathrm{mod}\ p_1^{\alpha_1}), \\ i^2 - i \equiv 0(\mathrm{mod}\, p_2^{\alpha_2}), \\ \ldots\ldots\ldots \\ i^2 - i \equiv 0(\mathrm{mod}\, p_n^{\alpha_n}), \end{array}\right. \iff \left|\begin{array}{l} i(i-1) \equiv 0(\mathrm{mod}\ p_1^{\alpha_1}), \\ i(i-1) \equiv 0(\mathrm{mod}\, p_2^{\alpha_2}), \\ \ldots\ldots\ldots \\ i(i-1) \equiv 0(\mathrm{mod}\, p_n^{\alpha_n}). \end{array}\right.$$

Звідси $\forall j = 1, \dots, n$ або i, або $i-1$ кратне $p_j^{\alpha_j}$.

Розглянемо задачу відшукання всіх ідемпотентів у кільці Z/m. Для цього потрібно:

– знайти канонічний розклад числа m на прості множники:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n};$$

– знайти максимальний серед простих множників:

$$p^{\alpha} = \max_{1 \le i \le n} \{ p_i^{\alpha_i} \};$$

– скласти послідовність чисел kp^{α}, де $k = 1, 2, \dots,$ причому найбільше з них не повинно перевищувати $\left[\frac{m}{2} \right]$;

– до знайденої послідовності додати пари $kp-1$, $kp+1$;

– серед трійок $kp-1, kp, kp+1$ вибрати ті, в яких є принаймні два числа a і b такі, що $\forall j = 1, 2, \dots n$ або $a \vdots p_j^{\alpha_j}$, або $b \vdots p_j^{\alpha_j}$. При цьому $\max\{a, b\}$ є ідемпотентом;

Нехай i_j є ідемпотентами в кільці Z/m. Тоді інші ідемпотенти знаходимо за формулою:

$$f_j = m - i_j + 1.$$

Іншими ідемпотентами будуть також 0, 1.

Methods of search of idempotents and nilpotents in rings $Z/_m$ of residual classes $Z/_m$ for arbitrary modulus m are developed..

1. Иванов Д. Н. Сбалансированные системы из примитивных идемпотентов в алгебрах матриц // Матем. сборник. – 2000. – №4.– С. 67-73.
2. Марков В. Т., Нечаев А. А.. Радикалы полусовершенных колец, связанные с идемпотентами // Матем. Сборник.– 2000. – Т.6.– С.293-298.