2.9.3 Арифметика на основі абелевих груп

Нехай задана деяка скінченна множина цілих чисел, наприклад, $N_5 = \{0, 1, 2, 3, 4\}$. Оскільки ми хочемо побудувати адитивну абелеву групу, то ця множина обов'язково повинна включати 0. Для того, щоб N_5 перетворити в групу GN_5, необхідно коректно задати значення для операції додавання з одним із елементів групи, скажімо з 1. Дійсно, оскільки $a + 0 = a$ для довільного $a \in GN_5$, то перший рядок таблиці додавання елементів групи визначений (таблиця 1), а на підставі комутативності (оскільки GN_5 абелева) і перший стовпчик цієї таблиці. Нехай, наприклад, задано $0 + 1 = 1$, $1 + 1 = 4$, $1 + 4 = 2$, $1 + 2 = 3$, $1 + 3 = 0$. Таке задання коректне, оскільки має місце єдиність результату (але єдиність результату, як буде показано нижче, не достатня умова гарантії коректності). Тепер послідовно знаходимо результати додавання з елементом 4, оскільки 4=1+1:

$$4 + 2=(1+1)+2=1+(1+2)=1+3=0, \quad 4+3=(1+1)+3=1+(1+3)=1,$$
$$4+4=(1+1)+4=1+(1+4)=1+2=3,$$

Далі знаходимо значення 4+1=2 і обчислюємо операцію додавання з елементом 2:

$$2+2=(1+4)+2=1+(4+2)=1+0=1, \quad 2+3=(1+4)+3=1+(4+3)=1+1=4,$$
$$2+4=(1+4)+4=1+(4+4)=1+3=0.$$

Далі знаходимо значення 2+1=3 і обчислюємо операцію додавання з елементом 3:

$$3+2=(1+2)+2=1+(2+2)=1+1=4, \quad 3+3=(1+2)+3=1+(2+3)=1+4=2,$$
$$3+4=(1+2)+4=1+(2+4)=1+0=1.$$

Заносимо ці значення в таблицю 2.9.2 і на цьому закінчуємо побудову групи GN_5.

Таблиця 2.9.1

+	0	1	2	3	4
0	0	1	2	3	4
1	1	4	3	0	2
2	2	3			
3	3	0			
4	4	2			

,

Таблиця 2.9.2

+	0	1	2	3	4
0	0	1	2	3	4
1	1	4	3	0	2
2	2	3	1	4	0
3	3	0	4	2	1
4	4	2	0	1	3

,

Таблиця 2.9.3

+	0	1	2	3	4
0	0	1	2	3	4
1	1	3	0	4	2
2	2	0	4	1	3
3	3	4	1	2	0
4	4	2	3	0	1

.

Аналогічно можна задати і довільну іншу групу GN_5. Дійсно, для цього задамо рядок таблиці додавання таким:

$$1+0 = 1,\ 1 + 1 = 3,\ 1+2=0,\ 1+3=4,\ 1+4=2.$$

Звідси отримуємо вищенаведену таблицю 3.

Варто зауважити, що для визначення групи можна взяти довільний її елемент. Наприклад, визначимо групу GN_5, елементами якої є 0, 2, 3, 5, 6, за допомогою додавання з елементом 3:

Таблиця 2.9.4

+	0	3	5	6	2
0	0	3	5	6	2
3	3	5	6	2	0
5	5	6			
6	6	2			
2	2	0			

,

Таблиця 2.9.5

+	0	3	5	6	2
0	0	3	5	6	2
3	3	5	6	2	0
5	5	6	2	0	3
6	6	2	0	3	5
2	2	0	3	5	6

.

Зауважимо, що для побудови групи GN_k, мало вимагати тільки однозначності операції додавання. Якщо визначити додавання в групі так $0+1=1,\ 1+1=0,\ 1+2=3,\ 1+3=4,\ 1+4=2$, то, обчислюючи 1+3, отримаємо

$$1+3=1+(1+2)=(1+1)+2=0+2=2,$$

що не збігається з визначеним вище. Справа в тім, що так визначена операція додавання не охоплює весь цикл елементів групи, тому що має елемент скінченного порядку $2 < 5$ (1+1=0).

Всі три групи, побудовані вище, циклічні на підставі теореми Лагранжа (вони мають порядок 5). В перших двох групах твірним

був елемент 1, а в третій групі – елемент 3. Неважко переконатися, що всі три групи ізоморфні. Дійсно, бієктивне відображення для перших двох груп має вигляд:

$$f(0) = 0,\ f(1) = 1,\ f(4) = 3,\ f(2) = 4,\ f(3) = 2,$$

а ізоморфізм першої і третьої груп визначається таким відображенням:

$$f(0) = 0,\ f(1) = 3,\ f(4) = 5,\ f(2) = 6,\ f(3) = 2.$$

Поставимо у відповідність операції додавання з елементом групи a_1, за допомогою якого визначається група, підстановку

$$f_{a_1} = \begin{pmatrix} 0 & a_1 & a_2 & \dots & a_{k-1} \\ a_1 & a_{i_1} & a_{i_2} & \dots & a_{i_k} \end{pmatrix}.$$

Ця підстановка означає, що $f_{a_1}(0) = 0 + a_1 = a_1, f_{a_1}(a_1) = a_1 + a_1 = a_{i_1}, f_{a_1}(a_{i_1}) = a_{i_1} + a_1 = a_{i_j}, f_{a_1}(a_{i_j}) = a_{i_j} + a_1 = a_{i_l}$ і т. д.

Назвемо групу GN_k **повноциклічною**, якщо підстановка f_{a_1} є повним циклом довжини k. Справедлива

Теорема 52. *Всі скінченні повноциклічні абелеві групи одного і того порядку ізоморфні між собою.*

Доведення. Нехай f_{a_1} і f_{b_1} – підстановки, які визначають дві повноциклічні групи k-го порядку, такі що $a_{i_1} = a_1 + a_1, a_{j_1} = a_{i_1} + a_1, a_{j_2} = a_{j_1} + a_1, \dots, a_{j_{k-1}} = a_{j_{k-2}} + a_1$ і $b_{i_1} = b_1 + b_1, b_{j_1} = b_{i_1} + b_1, b_{j_2} = b_{j_1} + b_1, \dots, b_{j_{k-1}} = b_{j_{k-2}} + b_1$. Тоді ізоморфізмом буде відображення

$$f(0) = 0, f(a_1) = b_1, f(a_{i_1}) = b_{i_1}, f(a_{j_1}) = f(a_{i_1} + a_1) = b_{i_1} + b_1,$$
$$f(a_{j_2}) = f(a_{j_1} + a_1) = f(a_{j_1}) + b_1, \dots, f(a_{j_{k-3}}) = f(a_{j_{k-4}}) + b_1. \blacksquare$$

Пряма сума абелевих груп – це операція, яка дозволяє будувати абелеві групи більших порядків з абелевих груп менших порядків.

Означення 61 *Прямою (зовнішньою) сумою адитивних абелевих груп $G_1, \dots, G_m$ називається абелева група $G = G_1 \oplus \dots \oplus G_m$, яка складається зі всіх послідовностей $(a_1, \dots, a_m)$, де $a_i \in G_i$, з операцією додавання*

$$(a_1, \dots, a_m) + (b_1, \dots, b_m) = (a_1 +_1 b_1, \dots, a_m +_m b_m).$$

Приклад прямої суми абелевих груп. Нехай маємо групи лишків Z_3 і Z_4 за модулем 3 і 4 відповідно. Тоді абелева група $G = Z_3 \oplus Z_4$ має такий носій, елементам якого поставлені у відповідність числа:

$$0 - (0,0),\ 1 - (0,1),\ 2 - (0,2),\ 3 - (0,3),\ 4 - (1,0),\ 5 - (1,1),$$
$$6 - (1,2),\ 7 - (1,3),\ 8 - (2,0),\ 9 - (2,1),\ 10 - (2,2),\ 11 - (2,3).$$

За такої відповідності таблиця додавання групи G набуває вигляду:

$\oplus$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	0	5	6	7	4	9	10	11	8
2	2	3	0	1	6	7	4	5	10	11	8	9
3	3	0	1	2	7	4	5	6	11	8	9	10
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	4	9	10	11	8	1	2	3	0
6	6	7	4	5	10	11	8	9	2	3	0	1
7	7	4	5	6	11	8	9	10	3	0	1	2
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	8	1	2	3	0	5	6	7	4
10	10	11	8	9	2	3	0	1	6	7	4	5
11	11	8	9	10	3	0	1	2	7	4	5	6

Відображення $\varphi : Z_{12} \to G$ задане так, як показано нижче,

$$\varphi(0) = 0, \varphi(1) = 5, \varphi(1+k) = 5 + \varphi(k),\ k = 1, \ldots, 10,$$

є ізоморфізмом цих груп. ♠

Далі будуть розглянуті інші застосування груп, зокрема, при розв'язанні проблеми передачі ключів.