МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІМЕНИ СЕМЕНА КУЗНЕЦЯ

Лабораторна робота №5

“Тема №5”

з дисципліни «Математичні основи криптології»

Виконав:

Студент групи 6.04.125.010.21.2

факультету Інформаційних технологій

спеціальності 125

П.І.П. Бойко В.В.

Перевірив:

Чугай А.М.

Харків – 2022

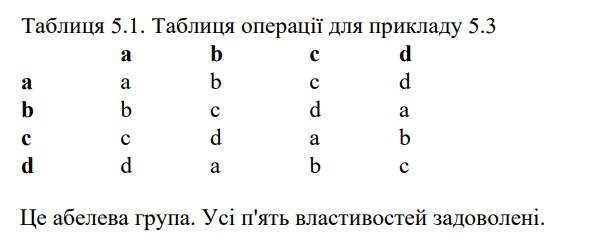
**Алгебраїчні структури. Групи.**

1. Для групи G = <Z4, +>:

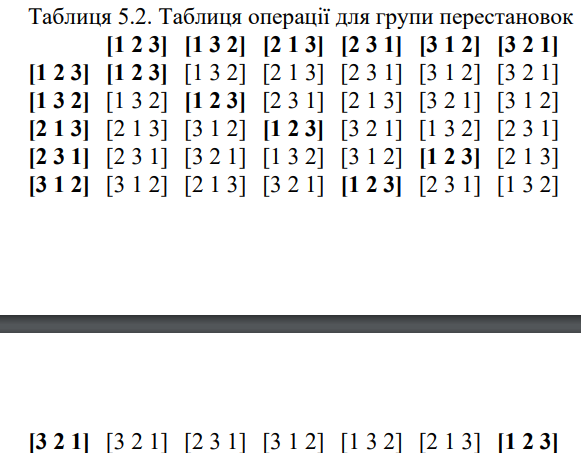
**H1 = <{0}, +>, H2 = <{0, 2, }, +>, H3 = <{0, 2}, +>іH4 = G**

* 1. Доведіть, що це – абелева група.
  2. Покажіть результат операцій 3 + 2 та 3–2 у цій групі.

1. Для множини G = <{a, b, c, d,}, •> Покажіть таблицю для операції віднімання (зворотна операція).



1. Доведіть, що перестановка у групі, показаній у таблиці 5.2 (див. лекцію), частково, у кількох випадках, задовольняє властивості асоціативності.



**Вхідні та вихідні сигнали можуть бути символами (лекції 2-3) або бітами.**

**Ми зобразили кожну перестановку прямокутником, всередині якого**

**показано, де вихідний вхідний сигнал та індекс (1,2,3) визначає вихідний**

**сигнал. Композиція складається з двох перестановок одна за одною. При**

**трьох вхідних сигналах та трьох вихідних сигналах може бути3! Або6різних**

**перестановок.Таблиця 5.2дає визначення цього оператора. Перший рядок -**

**перша перестановка; перший стовпець - друга перестановка. Результат**

**міститься на перетині.**

**У цьому випадку задоволені лише чотири властивості; тому група – не**

**абелева.**

1. Створіть таблицю перестановки для двох входів і двох виходів, подібних до показаних у [таблиці 5.2](https://intuit.ru/studies/courses/552/408/lecture/9358?page=4).
2. Аліса застосовує три послідовні перестановки.[1 3 2],

[3 2 1]і[2 1 3]. Покажіть, як Боб може використовувати лише одну перестановку, щоб змінити процес на протилежний. Користуйтесь [таблицею 5.2](https://intuit.ru/studies/courses/552/408/lecture/9358?page=4).

**Боб може [231]i[132] та [321]i[123].**

1. Знайдіть усі підгрупи наступних груп:
   1. image3.png

H1 = <{0}, +>, H2 = <{0, 2, 4,6,8,10,12,14,16}, +>, H3 = <{0, 9}, +>іH4 = G

* 1. image4.png

H1 = {1},\*,H2={1,15},\*H3=G

1. Використовуючи теорему Лагранжа, знайдіть порядок усіх потенційних підгруп для наступних груп:
   1. image3.png

**H1 = <{0}, +>, H2 = <{0, 2, 4,6,8,10,12,14,16}, +>, H3 = <{0, 9}, +>іH4 = G**

* 1. **10 mod 18 = 0**
  2. **11 mod 18 = 1**
  3. **12 mod 18 = (1 + 1) mod 18 = 2**
  4. **13 mod 18 = (1 + 1 + 1) mod 18 = 3**
  5. **14 mod 18 = (1 + 1 + 1 + 1) mod 18 = 4**
  6. **15 mod 18 = (1 + 1 + 1 + 1 + 1) mod 18 = 5**
  7. **16 mod 18 = (1 + 1 + 1 +1 + 1 +1) mod 18 = 6**
  8. **17 mod 18 = (1 + 1 + 1 + 1 + 1 + 1 + 1) mod 18 = 7**
  9. **18 mod 18 = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) mod 18 = 8**
  10. **19 mod 18 = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) mod 18 = 9**
  11. **20 mod 18 = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) mod 18 = 10**
  12. **21 mod 18 = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) mod 18 = 11**
  13. **22 mod 18 = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) mod 18 = 12**
  14. **23 mod 18 = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) mod 18 = 13**
  15. **24 mod 18 = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) mod 18 = 14**
  16. **25 mod 18 = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) mod 18 = 15**
  17. **26 mod 18 = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) mod 18 = 16**
  18. **27 mod 18 = (1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1) mod 18 = 17(зупинка, далі процес повторюється)**

1. Знайдіть порядок всіх елементів у наступних групах:
   1. image6.png

**H1 = <{0}, +>, H2 = <{0, 2, 4,6,}, +>, H3 = <{0, 4}, +>іH4 = G**

**50 mod 8 = 0**

**50 mod 8 = 7**

**50 mod 8 = 6**

**51 mod 8 = 5**

**52 mod 8 = 4**

**53 mod 8 = 3**

**54 mod 8 = 2**

**55 mod 8 = 1 (зупинка, далі процес повторюється)**