Навчальні завдання до лабораторних занять з Алгебри для студентів 2 курсу спеціальності "комп'ютерна математика"

Андрій Степанович Олійник

Київський національний університет імені Тараса Шевченка

2018

Зміст

Лабораторна робота 1

- Мета курсу
- Система оцінювання
- SageMath
- GAP

Знайомство з SageMath

- Призначення та історія
- Веб-сторінка проекту www.sagemath.org
- Завантаження і встановлення
- Веб-інтерфейс SageMathCell
- Хмарне середовище розробки CoCalc
- Документація

Базові можливості SageMath

1. Інтерактивний режим
2. Науковий калькулятор
3. Лінійна алгебра
4. Символьні обчислення
5. Побудова графіків
6. Робота з графами
7. OEIS
8. Розробка для SageMath

Домашнє завдання 1

1. Створіть екаунт на CoCalc
2. Задайте граф з 5 вершинами і 10 ребрами, виведіть його зображення, знайдіть матрицю суміжності, для кожного $l \geq 1$ знайдіть кількість шляхів та замкнених шляхів довжини l.
3. Реалізуйте алгоритми для візуалізації мозаїк Пенроуза

Лабораторна робота 2

Проект на CoCalc

1. Інтерфейс CoCalc
2. Створення проекту
3. Додавання учасника

Бінарні дії

1. Об'єкти і класи в SageMath
2. Клас OperationTable
3. Робота з наперед визначеними бінарними діями
4. Клас FiniteSetMaps
5. Визначення бінарної дії на скінченній множині
6. Перевірка властивостей бінарної дії на скінченній множині

Домашнє завдання 2

1. Визначити усіма можливими способами бінарну дію на множині з n ($n = 2, 3$) елементів.
2. Побудувати таблицю Келі для кожної з визначених дій.
3. Для кожної з визначених дій перевірити, чи буде дія асоціативною. У випадку, якщо дія не асоціативна, знайти впорядковану трійку елементів, для якої порушується рівність з умови асоціативності.
4. Визначити, які з визначених множин з бінарними діями будуть ізоморфними між собою і знайти кількість класів попарно ізоморфних між собою множин.

Лабораторна робота 3

Групи, порядок елемента групи

1. Групи в SageMath
2. Задання груп і найпростіші операції з групами
3. Група кватерніонів Q_8
4. Симетрична група S_4

Домашнє завдання 3

1. Задайте групи $D_{10}, \mathbb{Z}_{16}$, A_5. Для кожної з них виведіть таблицю Келі, знайдіть порядок групи, перевірте, чи група абелева.
2. Знайдіть кількість елементів кожного можливого порядку в групах S_{100} та A_{100}.
3. Для заданих натуральних n, k $(1 \leq n \leq 1000000,\ 1 \leq k \leq n!)$ визначте, чи існує в групі S_n елемент порядку k.

Лабораторна робота 4

Підгрупи, системи твірних

1. Знаходження підгрупи, породженої заданими елементами
2. Знаходження усіх підгруп заданої групи
3. Знайомство з GAP
4. Групи підстановок

Домашнє завдання 4

1. Знайдіть всі незвідні системи твірних групи S_4.
2. Знайдіть усі підгрупи груп S_4, A_4, S_5, A_5.
3. Задайте дві випадкові підстановки з групи S_n $(1 \leq n \leq 100)$. Перевірте, чи є вони парними. Знайдіть порядок підгрупи, ними породженої. Чи буде ця група дорівнювати A_n? S_n?

Лабораторна робота 5

Дискретний логарифм

1. Задача знаходження дискретного логарифма
2. Знаходження в SageMath дискретного логарифма в групі $\mathbb{Z}_p^*$, p — просте
3. ρ алгоритм Полларда

Щоб обчислити $x = ord_a(b)$, знаходимо такі цілі k, l, K, L що $a^k b^l = a^K b^L$ і знаходимо розв'язок рівняння

$$x(L - l) = k - K \pmod{n}.$$

ρ алгоритм Полларда I

Нехай G — циклічна група порядку n, a — твірний елемент G, $b \in G$. Зафіксуємо розбиття $G = S_0 \cup S_1 \cup S_2$ і визначимо функції $f : G \to G$, $g : G \times \mathbb{Z} \to \mathbb{Z}$, $h : G \times \mathbb{Z} \to \mathbb{Z}$

$$f(x) = \begin{cases} bx, & x \in S_0 \\ x^2, & x \in S_1 \\ ax, & x \in S_2 \end{cases}, \quad g(x,k) = \begin{cases} k, & x \in S_0 \\ 2k \pmod{n}, & x \in S_1 \\ k+1 \pmod{n}, & x \in S_2 \end{cases},$$

$$h(x,k) = \begin{cases} k+1 \pmod{n}, & x \in S_0 \\ 2k \pmod{n}, & x \in S_1 \\ k, & x \in S_2 \end{cases}.$$

ρ алгоритм Полларда II

Data: a — твірний елемент G, $b \in G$
Result: значення $x = ord_a(b)$ або помилка
ініціалізувати $i = 1, x_0 = e \in G, a_0 = 0, b_0 = 0$;
while $i < n$ **do**
  $x_i = f(x_{i-1}), a_i = g(x_{i-1}, a_{i-1}), b_i = h(x_{i-1}, b_{i-1})$;
  $x_{2i} = f(f(x_{2i-2})), a_{2i} = g(f(x_{2i-2}), g(x_{2i-2}, a_{2i-2}))$,
   $b_{2i} = h(f(x_{2i-2}), h(x_{2i-2}, b_{2i-2}))$;
  if $x_i == x_{2i}$ **then**
    $r = b_i - b_{2i}$;
    if $GCD(r, n) > 1$ **then**
      повернути помилку;
    else
      повернути $x = r^{-1}(a_{2i} - a_i) \pmod{n}$;
    end
  else
    $i = i + 1$;
  end
end

Algorithm 1: ρ алгоритм Полларда

Домашнє завдання 5

1. Реалізуйте ρ алгоритм Полларда
2. Порівняйте швидкість обчислення дискретного логарифма в групі $\mathbb{Z}_p^*$ вбудованим і реалізованим методами
3. Задайте випадкову підстановку a з групи S_n $(1 \leq n \leq 1000)$. Для випадкового елемента $b \in \langle a \rangle$ знайдіть значення дискретного логарифма b за основою a

Лабораторна робота 6

Нормальні підгрупи

1. Знаходження класів суміжності
2. Метод `.cosets`
3. Визначення, чи підгрупа нормальна
4. Метод `.is_normal`
5. Функція `sorted()`
6. Метод `.subgroups`
7. Метод `.normal_subgroups`
8. Метод `.is_simple`

Домашнє завдання 6

1. В групі рухів правильного восьмикутника задайте циклічну підгрупу порядку 4, побудуйте для неї ліві та праві класи суміжності, перевірте, чи буде ця підгрупа нормальною.
2. Побудуйте всі підгрупи знакозмінної групи A_5 і перевірте двома способами, що жодна неодинична власна підгрупа цієї групи не є нормальною. Порівняйте час перевірки.
3. Знайдіть кількість усіх підгруп та кількість усіх нормальних підгруп в групі $D_n, 3 \leq n \leq 1000$.

Лабораторна робота 7

Факторгрупи і гомоморфізми

1. Функція множення класів суміжності.
2. Гомоморфізми.
3. Метод `.kernel`
4. Метод `.image`
5. Метод `.quotient`
6. Метод `.is_isomorphic`

Домашнє завдання 7

1. Знайдіть кількість гомоморфізмів з циклічної групи порядку n в циклічну групу порядку m $(1 \leq n, m \leq 1000000)$, для кожного з них вкажіть порядок ядра і образу. Для кожного можливого порядку ядра визначте кількість гомоморфізмів, ядро кожного з яких має цей порядок.
2. Для кожної нормальної підгрупи H групи $D_n, 3 \leq n \leq 1000$, побудуйте гомоморфізм в D_n, ядром якого буде H.
3. Перевірте, чи існує епіморфізм групи $D_n, 3 \leq n \leq 1000$, на циклічну групу порядку k, $2 \leq k \leq 1000$.

Лабораторна робота 8

Групові дії. Спряженість. Групи автоморфізмів графів.

1. Метод `.orbits`
2. Метод `.stabilizer`
3. Метод `.conjugacy_classes_representatives`
4. Метод `.centralizer`
5. Клас `graphs`
6. Метод `.automorphism_group`

Домашнє завдання 8

1. Знайдіть кількість орбіт та їх потужності для природної дії групи діедра D_n на множині $\{1, \ldots, n\}$, $3 \le n \le 1000$.
2. Знайдіть кількість класів спряженості та їх потужності в знакозмінній групі A_n, $3 \le n \le 1000$, виберіть у кожному класі по представнику, вкажіть приклад підстановок, які спряжені в S_n, але не спряжені в A_n.
3. Знайдіть простий неорієнтований граф з найменшою можливою кількістю вершин, група автоморфізмів якого ізоморфна групі A_n, $4 \le n \le 10$. Скільки він має ребер?

Лабораторна робота 9

Кільця та факторкільця

1. Числові кільця і кільця лишків
2. Кільця многочленів
3. Ідеали та факторкільця

Домашнє завдання 9

1. Знайдіть кількості дільників одиниці, дільників нуля, нільпотентних елементів та ідеалів кільця $\mathbb{Z}_n$, $n \leq 10^{10}$.
2. В кільці многочленів $\mathbb{Z}_p[x]$ виберіть два випадкові елементи, породіть ними ідеал I, покажіть, що він є головним, знайшовши елемент, який його породжує, знайдіть кількість елементів у факторкільці $\mathbb{Z}_p[x]/I$ та кількість дільників нуля у ньому, $p \leq 1000$, p — просте.
3. Розкладіть на незвідні множники всі многочлени степеня меншого k над $\mathbb{Z}_p$, $k \leq 100, p \leq 1000$, p — просте.

Лабораторна робота 10

Симетричні многочлени

1. Симетричні многочлени з раціональними коефіцієнтами
2. Степеневі суми
3. Цілі гаусові числа

Домашнє завдання 10

1. Напишіть функцію, яка виражає заданий симетричний многочлен над $\mathbb{Z}_p$ (p — просте) через елементарні симетричні многочлени.
2. Напишіть функцію, яка виражає заданий симетричний многочлен над $\mathbb{Z}_p$ (p — просте) через степеневі суми.
3. Напишіть функцію, яка знаходить найбільший спільний дільник і його лінійний розклад для двох цілих гаусових чисел.

Лабораторна робота 11

Поля. Розширення полів

1. Числові поля.
2. Метод `.is_irreducible`
3. Функція `NumberField`
4. Метод `.polynomial`
5. Метод `.minpoly`
6. Метод `.degree`
7. Метод `.parent`
8. Метод `.splitting_field`

Домашнє завдання 11

1. Побудуйте розширення $\mathbb{Q}(\alpha) \supset \mathbb{Q}$ поля раціональних чисел за допомогою приєднання алгебраїчного елемента α степеня 6. Знайдіть мінімальний многочлен m_α цього елемента. Чи буде побудоване поле полем розкладу многочлена m_α?
2. Для многочлена $f(x) = x^4 + x^2 + 1 \in \mathbb{Q}[x]$ побудуйте його поле розкладу і знайдіть розклад $f(x)$ на лінійні множники.
3. Нехай a — корінь многочлена $g(x) = x^3 + 3x^2 + 3x - 2 \in \mathbb{Q}[x]$. Побудуйте розширення $\mathbb{Q}(a) \supset \mathbb{Q}$ і перевірте, чи розкладається в ньому $g(x)$ на лінійні множники. Побудуйте поле розкладу $g(x)$ як розширення поля $\mathbb{Q}(a)$, його степінь над $\mathbb{Q}(a)$ і над $\mathbb{Q}$.

Лабораторна робота 12

Скінченні поля

1. Створення скінченного поля
2. Виведення елементів скінченного поля
3. Арифметичні дії в скінченному полі
4. Експоненціювання і логарифмування в скінченному полі
5. Метод `.log`

Домашнє завдання 12

1. Створіть скінченне поле $GF(p^k)$, $p < 1000$ — просте, $2 \leq k \leq 3$. Скількома способами можна вибрати незвідний многочлен для побудови такого поля?
2. У мультиплікативній групі поля $GF(p^k)$, $p < 100$ — просте, $2 \leq k \leq 10$, знайдіть всі твірні елементи.
3. Створіть скінченні поля $GF(p^4)$ і $GF(p^2)$, $p < 1000$ — просте. В першому з них знайдіть підполе, ізоморфне другому, і побудуйте ізоморфізм.

Лабораторна робота 13

Еліптичні криві

1. Функція `EllipticCurve`
2. Метод `.cardinality`
3. Метод `.abelian_group`
4. Метод `.gens`
5. Метод `.order`

Домашнє завдання 13

1. Задайте еліптичну криву над простим скінченним полем характеристики $p, 2 < p < 1000000$, визначте кількість точок на ній, знайдіть будову групи точок, визначте точки найвищого порядку.
2. Задайте еліптичну криву над полем $GF(p^k)$, $p < 1000$ — просте, $2 \leq k \leq 3$, визначте кількість точок на ній, знайдіть будову групи точок, визначте точки найвищого порядку.
3. Задайте еліптичну криву над простим скінченним полем характеристики $p, 2 < p < 1000$, знайдіть точку найвищого порядку, побудуйте функцію для знаходження дискретного логарифму за основою цієї точки.