Лекція 10. Алгебраїчні операції.

Вступні зауваження до теми "Елементи абстрактної алгебри"

Основу сучасних швидких та якісних технологій обробки інформації становлять комп'ютери – від персональних до суперкомп'ютерів. Подання інформації для електронних обчислювальних машин дискретне, і її обробка складається з послідовностей елементарних перетворень тих чи інших інформаційних одиниць (слів, літер, цифр тощо). Тобто, фундаментальною ідеєю щодо відображення реального світу в комп'ютері є ідея дискретизації об'єктів. Для ефективної роботи на комп'ютері необхідно навчитися будувати моделі реальних об'єктів та процесів їх перетворення. Досить часто такими моделями можуть бути конструкції дискретної математики, зокрема, такі, як алгебраїчні структури, що розглядаються в даних методичних вказівках.Під абстрактною оболонкою більшості аксіоматичних теорій алгебри ховаються цілком конкретні задачі прикладного характеру. Складна взаємодія теоретичних і прикладних аспектів теорії, яка притаманна всій математиці, в алгебрі проявляється дуже виразно.

Наведемо кілька прикладів практичного використання алгебраїчних структур – множин з алгебраїчними операціями.

Однією з областей застосування є кодування інформації при передачі через канал зв'язку. При цьому ставиться вимога забезпечити виправлення помилок, які виникають внаслідок фізичних завад у каналах зв'язку або пристроях зберігання інформації. Це досягається шляхом введення при кодуванні надлишковості, яка дозволяє так вибрати послідовності символів для передачі, щоб вони задовольняли додатковим умовам, перевірка яких після прийому дає можливість виявити й виправити помилки. Найкращих результатів досягнуто, коли символи, що передаються, розглядаються як елементи певних алгебраїчних структур, зокрема скінченних полів (полів Галуа). При цьому простими стають процедури кодування й декодування, зменшується ймовірність неправильного декодування даних (циклічні коди, коди Ріда-Соломона тощо).

Іншою областю застосування є криптографія: захист інформації шляхом її перетворення, що виключає прочитання цієї інформації сторонньою особою. Ще кілька десятиліть тому такий підхід стосувався в основному військових операцій або був пов'язаний з шпигунськими історіями, а не був предметом широкого використання. Причиною бурхливого розвитку криптографії є широке використання комп'ютерних мереж, зокрема глобальної мережі

Internet, по яких передаються великі обсяги інформації державного, військового, комерційного й приватного характеру, що не допускає можливості доступу до неї сторонніх осіб. При виконанні сучасних алгоритмів шифрування з таємним ключем використовуються алгебраїчні структури скінчених полів (наприклад, стандарт AES симетричного шифрування США). Широко вживані алгоритми шифрування з відкритим ключем (багато провідних світових IT-компаній вклали в їх розвиток значні кошти, вони лежать в основі функціонування Internet-платежів eMoney) ґрунтуються на алгебраїчних поняттях фактор-кільця кільця цілих чисел за модулем великого натурального числа або еліптичних кривих над скінченними полями.

Іншими областями, де використовуються алгебраїчні структури, є аналіз та синтез скінченних автоматів; реляційні бази даних.

Алгебраїчні операції та їх властивості

Нехай X – довільна множина. n-арною операцією на множині X називається відображення $f: X^n \to X$, яке кожному вектору $(x_1, x_2, \ldots, x_n) \in X^n$ ставить у відповідність однозначно визначений елемент $x \in X$. Це записується наступним чином: $x = f(x_1, x_2, \ldots, x_n)$. Таких операцій на множині X можна задати декілька. Множина операцій, заданих на X, називається його сигнатурою й позначається $F = (f_1, f_2, \ldots)$.

Множину X разом з її сигнатурою F називаємо алгеброю (алгебраїчною структурою) та позначаємо $A(X, F)$. Множина X – це так звана множина-носій алгебри.

Найбільш поширеними є бінарні операції, які далі будемо називати просто операціями. Бінарна операція (або закон композиції) на X – це довільне (але фіксоване) відображення $f: X^2 \to X$. Таким чином, будь-якій впорядкованій парі (x_1, x_2) елементів із X ставиться у відповідність однозначно визначений елемент $f(x_1, x_2)$ цієї ж множини X. Часто бінарну операцію позначають якимось спеціальним символом: T, *, ∘, + та замість $f(x_1, x_2) = z$ записують $x\ T\ y = z$. Коли зрозуміло про що йдеться, символ операції може пропускатися.

У випадку, коли алгебраїчна структура має скінченне число елементів, можна для кожної заданої на ній бінарної операції будувати так звану таблицю Келі, яка повністю описує дану операцію. Число рядків і стовпців таблиці рівне числу елементів алгебри, а на перетині рядка й стовпця записується результат виконання операції над відповідними цим рядку й стовпцю двома елементами. Побудова таблиці Келі для операції T алгебри показана в табл. 2.

Табл. 2. Таблиця Келі

T	a_1	a_2	…	a_n
a_1	a_1Ta_1	a_1Ta_2	…	a_1Ta_n
a_2	a_2Ta_1	a_2Ta_2	…	a_2Ta_n
…	…	…	…	…
a_n	a_nTa_1	a_nTa_2	…	a_nTa_n

Операція T називається асоціативною, якщо для будь-яких $x, y, z \in X$ виконується умова $(x\ T\ y)\ T\ z = x\ T\ (y\ T\ z)$. Операція в алгебраїчній стуктурі не обов'язково володіє властивістю асоціативності, як показують два наведені далі приклади. У першому прикладі алгебра складається з двох елементів, а операція на ній задана табл. 3. Зауважимо, що одна клітинка в цій таблиці не заповнена, бо все сказане далі не залежить від того, що є в цій клітинці. У ній може бути будь-який з двох елементів алгебри, що розглядаємо.

Табл. 3.

T	a	b
a	b	b
b		a

Дійсно, розглянемо рівність $(aTb)Tb = aT(bTb)$. Оскільки, виходячи з табл. 3, ліва частина дорівнює a, а права дорівнює b, то остання рівність не виконується. Значить, задана цією таблицею операція T не є асоціативною.

У другому прикладі алгебра складається з трьох елементів, а операція на ній задана табл. 4. Зауважимо, що низка клітинок у вказаній таблиці не заповнені, бо все сказане далі не залежить від того, що є в цих клітинках. У кожній із них може бути будь-який з трьох елементів алгебри, що розглядаємо.

Табл. 4.

T	a	b	c
a	c	c	
b			a
c			b

Дійсно, розглянемо рівність $(aTb)Tc = aT(bTc)$. Оскільки, виходячи з таблиці Келі, ліва частина дорівнює b, а права дорівнює c, то остання рівність не виконується. Значить, задана цією таблицею операція T також не є асоціативною.

Операція T називається комутативною, якщо для будь-яких $x, y \in X$ виконується умова $x\,T\,y = y\,T\,x$. Операція в алгебраїчній стуктурі не обов'язково володіє властивістю комутативності, як показує наведений далі в табл. 5 приклад.

Табл. 5.

T	a	b
a	b	b
b	a	a

Дійсно, виходячи з цієї таблиці, $aTb \neq bTa$. Інші приклади некомутативних операцій будуть розглянуті в подальших лекціях.

Операція T_1 називається дистрибутивною зліва відносно операції T_2, якщо для будь-яких $x, y, z \in X$ виконується умова $x\,T_1\,(y\,T_2\,z) = (x\,T_1\,y)\,T_2\,(x\,T_1\,z)$. Операція T_1 називається дистрибутивною справа відносно операції T_2, якщо для будь-яких $x, y, z \in X$ виконується умова $(y\,T_2\,z)\,T_1\,x = (x\,T_1\,y)\,T_2\,(x\,T_1\,z)$. Операція T_1 називається дистрибутивною відносно операції T_2, якщо операція T_1 є одночасно дистрибутивною зліва й справа відносно операції T_2.

Елемент e є нейтральним (одиничним) зліва відносно операції T, якщо для будь-якого $x \in X$ виконується $e\,T\,x = x$. Елемент e є нейтральним (одиничним) справа відносно операції T, якщо для будь-якого $x \in X$ має місце рівність $x\,T\,e = x$. Елемент e є нейтральним (одиничним) відносно операції T, якщо він є одночасно нейтральним зліва й справа, тобто для будь-якого $x \in X$ виконується $x\,T\,e = e\,T\,x = x$. Можливі різні варіанти, пов'язані з існуванням односторонніх нейтральних елементів. Нейтральний зліва елемент бути не єдиним або не існувати. Нейтральних зліва елементів може бути навіть нескінченна кількість. Так само нейтральний справа елемент бути не єдиним або не існувати. Нейтральних справа елементів також може бути навіть нескінченна кількість. Як показує приклад в табл. 6, всі елементи нескінченної алгебри можуть бути нейтральними зліва і разом з цим у цій алгебрі немає ні одного нейтрального справа.

Табл. 6.

T	a_1	a_2	a_3	…
a_1	a_1	a_2	a_3	…
a_2	a_1	a_2	a_3	…
a_3	a_1	a_2	a_3	…
…	…	…	…	…

Проте, якщо двосторонній нейтральний елемент існує, то він є єдиним. Дійсно, якщо припустити, що маємо два різних двосторонніх нейтральних елементи $e_1 \neq e_2$, то з рівностей $e_1 = e_1 \, T \, e_2 = e_2$ отримуємо $e_1 = e_2$ – суперечність.

Елемент x^* називається оберненим зліва до елемента $x \in X$ відносно операції T, коли $x^* \, T \, x = e$. Елемент x^* називається оберненим справа до елемента $x \in X$ відносно операції T, коли $x \, T \, x^* = e$. Елемент x^* називається оберненим до елемента $x \in X$ відносно операції T, коли він є одночасно оберненим зліва й справа, тобто $x^* \, T \, x = x \, T \, x^* = e$. Обернений зліва елемент може бути не єдиним або не існувати. Обернений справа елемент може бути не єдиним або не існувати. Двосторонній обернений елемент єдиний.