ЛЕКЦІЯ 12. АЛГЕБРИЧНІ СТРУКТУРИ

12.1. Алгебричні операції та їхні властивості
12.2. Алгебри
12.3. Кільця
12.4. Поля
12.5. Векторні простори
12.6. Ґратки

Поняття алгебричної структури містить визначену множину об'єктів та операцій над цими об'єктами.

12.1. Алгебричні операції та їхні властивості

1. n-*арною операцією* на множині X називають функцію $f : X^n \to X, n \in \mathbb{N}$. Число n називають *рангом* операції. Найчастіше розглядають *унарні* операції $f : X \to X$ та *бінарні* операції $f : X^2 \to X$.

Елементи упорядкованого набору з n елементів множини X^n називають *операндами*. Операції зазвичай позначають символами, які називають *операторами*. Символ оператора унарної операції зазвичай ставлять перед або над операндом.

2. Операції записують одним із трьох способів. У першому випадку оператор ставлять між операндами (*infix*), у другому — перед операндами (*prefix*), у третьому — після операндів (*postfix*). Розгляньмо три варіанти запису бінарної операції додавання:

1) infix $a + b$;

2) prefix $+ab$;

3) postfix $ab+$.

Користуватимемось записом prefix для унарних операцій та infix для бінарних.

3. Для бінарних операцій користуватимемось символами $\odot$ та $\oplus$. Бінарні операції на скінченних множинах задають за допомогою *таблиць Келі* $C = (c_{ij})$, її рядки та стовпці нумерують елементами множини X, а елементи таблиці $c_{ij} = x_i \odot x_j$.

Приміром, розгляньмо операцію $\odot$, означену на множині $\{a,b,c\}$ таблицею 12.1.

Таблиця 12.1

$\odot$	a	b	c
a	a	a	b
b	b	a	c
c	a	b	b

Отже,

$$a \odot b = a, b \odot b = a, c \odot b = b, \ldots$$

4. Властивості операцій. Нехай на множині X означено деякі бінарні операції $\odot$ та $\oplus$.

Бінарну операцію $\odot$ називають *комутативною*, якщо для всіх $x, y \in X$ виконано рівність

$$x \odot y = y \odot x.$$

Бінарну операцію $\odot$ називають *асоціативною*, якщо для всіх $x, y, z \in X$ виконано рівність

$$(x \odot y) \odot z = x \odot (y \odot z).$$

Якщо операція $\odot$ асоціативна, то можна дужки випустити й писати $x \odot y \odot z$ замість $(x \odot y) \odot z$ або $x \odot (y \odot z)$.

Бінарну операцію $\odot$ називають *дистрибутивною* відносно операції $\oplus$, якщо для всіх $x, y, z \in X$ виконано рівність

$$x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z),$$
$$(x \oplus y) \odot z = (x \odot z) \oplus (y \odot z).$$

Приміром, додавання та множення раціональних чисел є комутативними та асоціативними бінарними операціями.

Операція віднімання на множини раціональних чисел не комутативна і не асоціативна.

Множення цілих чисел дистрибутивно відносно додавання. Додавання цілих чисел не є дистрибутивним відносно множення.

5. Нейтральний елемент. Елемент $e \in X$ називають *лівим нейтральним* відносно операції $\odot$, якщо для будь-якого $x \in X$ виконана рівність

$$e \odot x = x.$$

Елемент $e \in X$ називають *правим нейтральним* відносно операції $\odot$, якщо для будь-якого $x \in X$ виконана рівність

$$x \odot e = x.$$

Елемент $e \in X$ називають *нейтральним* відносно операції $\odot$, якщо для будь-якого $x \in X$ виконані рівності

$$x \odot e = x = e \odot x.$$

Якщо нейтральний елемент відносно асоціативної бінарної операції $\odot$ існує, то він єдиний.

Число 0 є нейтральним елементом відносно додавання цілих чисел. Число 1 є нейтральним елементом відносно множення цілих чисел.

6. Симетричний елемент. Елемент $u \in X$ називають *лівим симетричним* до елемента $x \in X$ відносно операції $\odot$, якщо

$$u \odot x = e.$$

Елемент $v \in X$ називають *правим симетричним* до елемента $x \in X$ відносно операції $\odot$, якщо

$$x \odot v = e.$$

Елемент $x' \in X$ називають *симетричним* до елемента $x \in X$ відносно операції $\odot$, якщо

$$x \odot x' = x' \odot x = e.$$

Елемент x називають *симетризовним*, а елементи x та x' — взаємно симетричними.

Якщо операція $\odot$ асоціативна та елемент x симетризовний, то існує єдиний елемент, симетричний до x.

Якщо елементи x та y симетризовні відносно асоціативної операції $\odot$, то елемент $x \odot y$ також симетризований та елемент $y' \odot x'$ є симетричним до $x \odot y$.

Приміром, відносно додавання цілих чисел симетричним до заданого цілого числа x є протилежне до нього число $(-x)$. Відносно множення раціональних чисел симетричним до ненульового числа x є обернене до нього число $\dfrac{1}{x}$; число 0 не має симетричного елемента відносно множення.

7. Підмножину Y множини X називають *замкненою* відносно операції $\odot$, якщо для будь-яких $x, y \in Y$ елемент $x \odot y \in Y$.

Множина всіх елементів, симетризовних відносно асоціативної бінарної операції $\odot$, є замкненою відносно $\odot$.

Приміром, множина всіх парних чисел замкнена відносно додавання та множення цілих чисел. Множина всіх непарних чисел замкнена відносно множення, але не є замкненою відносно додавання цілих чисел.

12.2. Алгебри

1. *Алгеброю* називають упорядковану пару $\mathcal{A} = (A,\Omega)$, де A — непорожня множина та Ω — множина операцій на A.

Множину A називають *основною множиною* алгебри $\mathcal{A}$, а його елементи — елементи алгебри $\mathcal{A}$.

Множину операцій Ω називають *головними операціями* алгебри $\mathcal{A}$.

Алгебру з асоціативною бінарною операцією й нейтральним елементом називають *моноїдом*.

2. Групи. Алгебра $\mathcal{G} = (G,*,')$ називають *групою*, якщо її головні операції справджують умови:

1) бінарна операція $*$ асоціативна;

2) у G існує правий нейтральний елемент відносно операції $*$, тобто такий елемент e, для будь-якого $a \in G$ виконано рівність

$a * e = a$;

3) для будь-якого елемента $a \in G$ виконано рівність $a * a' = e$.

Отже, група — це непорожня множина з асоціативною бінарною операцією, яка має правий нейтральний елемент та унарною операцією переходу до правого симетричного елемента відносно бінарної операції, тобто кожен елемент групи має правий симетричний до нього елемент відносно бінарної операції групи $*$.

Групу називають $\mathcal{G} = (G,*,')$ *комутативною* (*абелевою*), якщо бінарна операція групи комутативна.

Порядком групи називають кількість елементів основної множини групи.

3. Мультиплікативний запис. Під час вивчення груп зазвичай використовують мультиплікативну або адитивну форму запису головних операцій групи. Для мультиплікативного запису бінарну операції групи називають множенням і пишуть $a \cdot b$ замість $a * b$, називаючи елемент $a \cdot b$ добутком елементів a та b. Елемент симетричний до a, позначають

a^{-1} і називають *оберненим* до a. Нейтральний елемент відносно множення позначають e і називають *одиничним елементом* або *одиницею* групи.

Поняття натурального степеня a^n елемента $a \in G$ означують так:

$$a^0 = e, a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ разів}}, n \in \mathbb{N}.$$

4. Адитивний запис. Для адитивного запису бінарну операцію групи називають додаванням і пишуть $a + b$ замість $a * b$, називаючи елемент $a + b$ сумою елементів a та b. Елемент симетричний елементу a, позначають $(-a)$ і називають *протилежним* елементу a. Нейтральний елемент відносно додавання позначають символом 0 і називають *нульовим елементом* або *нулем* групи.

5. Властивості групи. Для будь-якого елемента групи a $a^{-1}a = e$, тобто правий обернений до a елемент є також лівим оберненим.

Для кожного елемента a групи елемент a^{-1} є єдиним оберненим елементом. Кожен елемент a групи має єдиний правий та єдиний лівий обернений елемент, причому вони обидва рівні a^{-1}.

Для будь-якого елемента a групи $ea = a$, тобто права одиниця є також лівою одиницею.

Елемент e групи є єдиним одиничним елементом групи. Він є також єдиним лівим та єдиним правим одиничним елементом групи.

Для будь-яких елементів a, b групи кожне з рівнянь $ax = b$ та $ya = b$ відносно змінних x та y має єдиний розв'язок:

$$x = a^{-1}b, \ y = ba^{-1}.$$

Для будь-яких елементів a, b, c групи з $ac = bc$ випливає $a = b$ та з $ca = cb$ випливає $a = b$.

Для будь-яких елементів a, b, c групи з $ab = a$ випливає $b = e$ та з $ca = a$ випливає $c = e$.

У групі елемент a є оберненим до a^{-1}, тобто $(a^{-1})^{-1} = a$.

12.3. Кільця

1. *Кільцем* називають алгебру $\mathcal{K} = (K, +, -, \cdot, 1)$ з двома бінарними операціями додаванням $+$ та множенням $\cdot$, таким що:

1) за додаванням є абелевою групою;

2) за множенням є моноїд з одиничним елементом 1;

3) множення дистрибутивно відносно додавання.

Нуль групи за додаванням називають *нулем кільця* і позначають як 0. Одиничний елемент для множення 1, називають *одиницею кільця*.

Кільце називають *комутативним*, якщо для будь-яких елементів кільця $a \cdot b = b \cdot a$.

2. Кільце називають областю цілісності, якщо воно комутативно, $0 \neq 1$, і для будь-яких $a, b \in K$ з $a \cdot b = 0$ випливає $a = 0$ або $b = 0$.

Елементи a та b називають дільниками нуля, якщо $a \neq 0, b \neq 0$ та $ab = 0$.

Будь-яка область цілісності не має дільників нуля.

3. Властивості кілець. Для будь-яких елементів $a, b \in K$ рівняння $b + x = a$ має єдиний розв'язок $a + (-b)$, який позначають як $a - b$.

Для будь-яких елементів a, b, c кільця:

1) якщо $a + b = a$, то $b = 0$;

2) якщо $a + b = 0$, то $b = -a$;

3) $-(-a) = a$;

4) $0 \cdot a = a \cdot 0 = 0$;

5) $(-a)b = a(-b) = -(ab)$;

6) $(-a)(-b) = ab$;

7) $(a - b)c = ac - bc$ та $c(a - b) = ca - cb$.

12.4. Поля

1. *Алгебричною системою* називають упорядковану трійку (A, Ω, Ω_0), де A — непорожня множина, яку називають основною множиною системи; Ω — головні операції системи; Ω_0 — головні відношення системи.

2. Поля. Елемент a кільця називають *оборотним* елементом кільця, якщо в кільці існує такий елемент b, що $ab = ba = 1$. Елементи a та b називають взаємно оберненими.

Полем називають комутативне кільце, у якому нуль відмінний від одиниці, і будь-який ненульовий елемент є оборотним.

3. Властивості поля. Нехай a,b елемента поля. Рівняння $bx = a$ має в полі єдиний розв'язок ab^{-1}, який позначають $\dfrac{a}{b}$.

Для будь-яких елементів a,b,c поля:

1) якщо $ab = 1$, то $a \neq 0$ та $b = a^{-1}$;

2) якщо $ac = bc$ та $c \neq 0$, то $a = b$;

3) якщо $ab = 0$, то $a = 0$ або $b = 0$;

4) якщо $a \neq 0$ та $b \neq 0$, то $ab \neq 0$;

5) $\dfrac{a}{b} = \dfrac{c}{d} \Leftrightarrow ad = bc, b \neq 0, d \neq 0$;

6) $\dfrac{a}{b} \pm \dfrac{c}{d} = \dfrac{ad \pm bc}{bd}$;

7) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{ac}{bd}$;

8) $\dfrac{a}{b} + \dfrac{(-a)}{b} = 0, -\left(\dfrac{a}{b}\right) = \dfrac{-a}{b}$;

9) якщо $a \neq 0$ та $b \neq 0$, то $\left(\dfrac{a}{b}\right)^{-1} = \dfrac{b}{a}$;

10) $\dfrac{ac}{bc} = \dfrac{a}{b}$.

4. Алгебраїчну систему $(F,<)$ називають *лінійно упорядкованою* множиною, якщо виконано умови:

1) для будь-яких $a,b,c \in F$, якщо $a < b$ та $b < c$, то $a < c$;

2) для будь-якої пари елементів $a,b \in F$ виконано лише одне співвідношення: $a < b, a = b, b < a$.

5. *Упорядкованим полем* називають алгебричну систему $(F,+,-,\cdot,1,<)$, яка справджує умови:

1) алгебра $(F,+,-,\cdot,1)$ є полем;

2) система $(F,<)$ є упорядкованою множиною;

3) для будь-яких $a,b,c \in F$, якщо $a < b$, то $a + c < b + c$ (монотонність додавання);

4) для будь-яких $a,b,c \in F$, якщо $a < b$ та $0 < c$, то $ac < bc$ (монотонність множення).

Елемент упорядкованого поля називають додатним, якщо $0 < a$. За означенням $b > a$ тоді й лише тоді, коли $a < b$. Далі за означенням $a \leq b$ тоді й лише тоді, коли $a < b$ або $a = b$.

6. Властивості впорядкованого поля. Нехай a,b,c,d — елементи впорядкованого поля. Тоді

1) $a < b$ тоді й лише тоді, коли $b - a > 0$;

2) для будь-якого a виконується лише одна умова: $a < 0, a = 0, a > 0$;

3) якщо $a > 0, b > 0$, то $a + b > 0$ та $ab > 0$;

4) якщо $a < b, c < d$, то $a + c < b + d$;

5) якщо $a < b$ та $c < 0$, то $ac > bc$;

6) якщо $a \neq 0$, то $a^2 > 0$;

7) $1 > 0$ та $n \cdot 1 > 0$ для будь-якого натурального n;

8) поле $(F,+,-,\cdot,1)$ є область цілісності.

12.5. Векторні простори

1. Нехай $\mathcal{F}$ — поле з основною множиною F, елементи якого називають скалярами і Нехай V — непорожня множина.

Множину V із заданою на ньому бінарною операцією (додаванням) і операцією множення елементів поля скалярів $\mathcal{F}$ на елементи множини V називають *векторним простором* над полем $\mathcal{F}$, якщо будь-яких $\overline{a},b \in V$ та для будь-яких $\alpha,\beta \in F$ виконано наступні умови:

1) алгебра $(V,+,-)$, де $-$ є операцією множення на скаляр (-1) елементів з V, є абелевою групою;

2) $(\alpha\beta)\overline{a} = \alpha(\beta\overline{a})$;

3) $\alpha(\overline{a} + \overline{b}) = \alpha\overline{a} + \alpha\overline{b}$;

4) $(\alpha + \beta)\overline{a} = \alpha\overline{a} + \beta\overline{b}$;

5) $1 \cdot \overline{a} = \overline{a}$.

Векторний простір з основною множиною V позначають $\mathcal{V}$.

Групу $(V,+,-)$ називають *адитивною групою* векторного простору $\mathcal{V}$. Нуль цієї групи $\overline{0}$ називають *нульовим вектором* простору $\mathcal{V}$. Елементи множини V називають *векторами* векторного простору $\mathcal{V}$. Вектори $\overline{a}$ та $(-1)\overline{a}$ називають *взаємно протилежними*.

2. Найпростіші властивості векторних просторів. Нехай $\mathcal{V}$ — векторний простір над полем $\mathcal{F}, \overline{a}, \overline{b} \in V$ та $\alpha, \beta \in F$. Тоді

1) якщо $\overline{a} + \overline{b} = \overline{a}$, то $\overline{b} = \overline{0}$;
2) $0 \cdot \overline{a} = \overline{0}$;
3) $\alpha \cdot \overline{0} = \overline{0}$;
4) якщо $\overline{a} + \overline{b} = \overline{0}$, то $\overline{b} = (-1)\overline{a} = -\overline{a}$;
5) якщо $\alpha \cdot \overline{a} = \alpha \cdot \overline{b}$ та $\alpha \neq 0$, то $\overline{a} = \overline{b}$;
6) якщо $\alpha \cdot \overline{a} = \overline{0}$, то $\alpha = 0$ або $\overline{a} = \overline{0}$;
7) якщо $\alpha\overline{a} = \beta\overline{b}$ та $\overline{a} \neq \overline{0}$, то $\alpha = \beta$.

12.6. Ґратки

1. Ґраткою називають множину M з двома бінарними операціями $\cap$ та $\cup$, такими що виконано такі умови:

1) *ідемпотентність*
$$a \cap a = a, \;\; a \cup a = a;$$

2) *комутативність*
$$a \cap b = b \cap a, \;\; a \cup b = b \cup a;$$

3) *асоціативність*
$$(a \cap b) \cap c = a \cap (b \cap c), \;\; (a \cup b) \cup c = a \cup (b \cup c);$$

4) *поглинання*
$$(a \cap b) \cup a = a;$$

5) ґратку називають *дистрибутивною*, якщо
$$a \cup (b \cap c) = (a \cup b) \cap (a \cup c), \;\; a \cap (b \cup c) = (a \cap b) \cup (a \cap c).$$

2. Обмежені ґратки. Якщо в ґратці існує $0 \in M$, такий, що для будь-якого елемента $a \in M$ виконано $0 \cap a = 0$, то 0 називають *нулем* (*нижньою межею*) ґратки. Якщо у ґратці існує $1 \in M$ така, що для будь-якого $a \in M$ виконано рівність $1 \cup a = a$, то 1 називають *одиницею* (*верхньою межею*) ґратки. Ґратку з верхньою та нижньою межами називають *обмеженою*.

3. Властивості обмеженої ґратки. Якщо нижня (верхня) межа існують, то вона єдина.

$a \cap b = b$, тоді й лише тоді, коли $a \cup b = a$.
$0 \cap a = 0 \Leftrightarrow 0 \cup a = a, \; 1 \cup a = 1 \Leftrightarrow 1 \cap a = a.$

4. Ґратка з доповненням. В обмеженій ґратці елемент a' називають *доповненням* елемента a, якщо $a \cap a' = 0$ та $a \cup a' = 1$.

Якщо для будь-якого елемента $a \in M$ існує $a' \in M$ такий, що $a \cap a' = 0, a \cup a' = 1$, то обмежену ґратку називають ґраткою з доповненням.

5. Властивості ґратки з доповненням. В обмеженій дистрибутивній ґратці з доповненням виконано:

1) доповнення a' єдине;

2) доповнення інволютивно: $a'' = a$;

3) меже доповнюють одна одну: $1' = 0, 0' = 1$;

4) виконано закони де Моргана:
$(a \cup b)' = a' \cap b', (a \cap b)' = a' \cup b'$.

6. Частковий порядок на ґратці. У будь-якій ґратці можна природнім чином запровадити частковий порядок, а саме:

$$a \prec b \Leftrightarrow a \cap b = a.$$

Нехай M — частково упорядкована множина з частковим порядком $\prec$. Елемент x називають *нижньою межею* для a та b, якщо $x \prec a, x \prec b$. Так само, y називають *верхньою межею* для a та b, якщо $a \prec y$ та $b \prec y$.

Елемент x називають *точною нижньою межею* елементів a та b, якщо x — нижня межа елементів a та b і для будь-якої іншої нижньої межі v елементів a та b виконано $v \prec x$. Позначають $x = \inf(a,b)$.

Так само, y називають *точною верхньою межею* елементів a та b, якщо y — верхня меже елементів a та b і для будь-якої іншої верхньої межі u елементів a та b виконано $y \prec u$. Позначають: $y = \sup(a,b)$.

Якщо точна нижня (верхня) межа існує, то вона єдина.

Якщо в частково упорядкованій множині для будь-яких двох елементів існує нижня та верхня межа, то ця множина утворює ґратку відносно inf та sup, тобто

$$x \cap y = \inf(x,y), x \cup y = \sup(x,y).$$

7. Дистрибутивна обмежена ґратка, у якій для кожного елемента існує доповнення, називають *булевою алгеброю*.