Алгебраїчні структури

Модуль 4 Лекція 1

План

- Частково-впорядковані множини
- Напівгрупи та напіврешітки
- Решітки
- Групи
- Групи і гомоморфізми

Умовні позначення

 - визначення

 - приклад

 - примітка

! - важливо!

☑ - теорема

Частково-впорядковані множини

Відношення R на множині A є відношенням порядку, якщо воно рефлексивне, антисиметричне і транзитивне. Множину A в цьому випадку називають ***частково впорядкованою множиною*** або ***ЧВ-множиною*** з порядком R.

Для підмножини B ЧВ-множини A елемент a з A називають ***верхньою гранню*** B, якщо $a \geq b$ $\forall$ b з B. Елемент a називають ***найменшою верхньою гранню*** (***нвг***) підмножини B, якщо: (a) a – верхня грань B; (b) якщо будь-який інший елемент
a' множини A є верхньою гранню B, то $a \leq a'$.

Найменшу верхню грань всієї ЧВ-множини A (якщо вона існує) називають ***найбільшим елементом*** A.

Найбільшу нижню грань всієї ЧВ-множини A (якщо вона існує) називають ***найменшим елементом*** A.

Елемент a підмножини B ЧВ-множини A називають ***максимальним елементом*** B, якщо для будь-якого елемента $b \in B$ з того, що $b \geq a$, випливає $b = a$. Тобто, в множині B немає елемента, який був би "більшим", ніж a.

Елемент a підмножини B ЧВ-множини A називають ***мінімальним елементом*** B, якщо для для будь-якого $b \in B$ з того, що $b \leq a$, випливає $b = a$. Тобто, в B немає елемента, який був би "менший", ніж a. Звичайно терміни "мінімальний" і "максимальний" елемент відносять до всієї множини.

Нехай $C = \{1, 2, 3\}$ і X - булеан множини C: $X = P(C) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Визначимо відношення $\leq$ на множині X : $T \leq V$, якщо $T \subseteq V$.

За означенням, $\{1, 2\}$ є найбільша нижня грань для $\{\varnothing, \{1\}, \{2\}\}$, а також для $\{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$. Множина $\{1, 2, 3\}$ - найменша верхня грань для X. Елемент $\varnothing$ є найбільшою нижньою гранню для всіх трьох множин.

Алгебраїчною структурою (або просто алгеброю) називається множина разом з визначеними на ній замкнутими операціями. Така множина називається основною, а множина операцій – сигнатурою.

Структури разом з теоремами, правилами обчислень і виведення іноді називають ***алгебраїчною системою***.

Елемент 0 множини A називають ***нулем*** відносно даної операції *, якщо $0 * x = 0$ ($x * 0 = 0$) для будь-якого $x \in A$.

Елемент 1 множини A називають ***нейтральним елементом*** відносно даної операції *, якщо $1 * x = x$ ($x * 1 = x$) для будь-якого $x \in A$.

Напівгрупи та напівґратки

Напівгрупа – це множина S з однією асоціативною бінарною операцією: a * (b * c) = (a * b) * c.

Якщо для всіх a і b з S виконується $a * b = b * a$, то множину S з оператором * називають ***абелевою*** (***комутативною***) ***напівгрупою***.

Якщо в (S, *) існує елемент I такий, що $I * a = a * I = a$ для всіх a з A, то таке I називають ***одиницею*** напівгрупи (S, *), а (S, *) - називають ***напівгрупою з одиницею***, або ***моноїдом***.

Якщо (S, *) - напівгрупа, і $S' \subseteq S$, то S' називають ***піднапівгрупою*** напівгрупи S, якщо * - бінарна операція на S'. Це еквівалентно наступному: (S', *) – піднапівгрупа напівгрупи (S, *), якщо $S' \subseteq S$, і для кожних $a, b \in S'$ маємо $a * b \in S'$.

$(S, \cdot)$ - напівгрупа матриць $n \times n$ раціональних чисел з операцією $\cdot$ матриць, $(\square S, \cdot)$ - напівгрупа матриць $n \times n$ цілих чисел. Тоді $(\square S, \cdot)$ - *піднапівгрупа* напівгрупи $(S, \cdot)$.

$S_n^{\,0} = \{x : x \in Z$ і $x \geq n\} \cup \{0\}$ для $n \in N$. Напівгрупа $S_n^{\,0}$ - *комутативний моноїд* з операцією + цілих чисел і нейтральним 0. $S_n^{\,1} = \{x : x \in Z$ і $x \geq n\} \cup \{1\}$. $S_n^{\,1}$ - *комутативний моноїд* з операцією $\cdot$ цілих чисел і одиницею. Якщо $m \geq n$, то $S_m^{\,0}$ - *піднапівгрупа* напівгрупи $S_n^{\,0}$ і $S_m^{\,1}$ - *піднапівгрупа* напівгрупи $S_n^{\,1}$.

Напівгрупу $<a>$ називають ***циклічною напівгрупою***, породженою елементом a.

ТЕОРЕМА 16.1. Нехай $(S, \cdot)$ - напівгрупа і $a_1, a_2, ..., a_k \in S$. Нехай $A = \{a_1, a_2, ..., a_k\}$ і $A^* = <a_1, a_2, ..., a_k>$ - множина всіх скінченних добутків елементів $a_1, a_2, ..., a_k$. Тоді A^* - напівгрупа і A^* - найменша піднапівгрупа напівгрупи S, що містить A.

Напівгрупу A^* називають напівгрупою, породженою множиною A. Якщо для кожної власної підмножини B множини A маємо $B^* \neq A^*$, то A називається ***мінімальною породжуючою множиною*** для напівгрупи A^*.

Нехай $(S, \cdot)$ і $(T, \circ)$ - напівгрупи і $f : S \to T$ - така функція, що $f(s \cdot s') = f(s) \circ f(s')$. Функцію f називають ***гомоморфізмом*** з S в T.

ТЕОРЕМА 16.2. Нехай $(S, \cdot)$ і $(T, \circ)$ - напівгрупи і $f : S \to T$ – гомоморфізм з S в T. Якщо S' - піднапівгрупа напівгрупи S, то $f(S')$ піднапівгрупа напівгрупи T.

ТЕОРЕМА 16.3. Нехай $(S, \cdot)$ і $(T, \circ)$ – напівгрупи і $f : S \to T$ – гомоморфізм з S в T. Якщо T' - піднапівгрупа напівгрупи T, то $f^{-1}(T')$ – піднапівгрупа напівгрупи S.

Нехай $(S, \cdot)$ - напівгрупа і R - відношення еквівалентності на S. R має властивість: якщо s_1Rs_2 і s_3Rs_4, то $s_1s_3Rs_2s_4$ $\forall$ $s_1, s_2, s_3, s_4 \in S$. Тоді R називають ***відношенням конгруентності***.

ТЕОРЕМА 16.4. Нехай $(S, \cdot)$ і $(T, \circ)$ - напівгрупи і $f : S \to T$ – гомоморфізм з S у T. Відношення R на множині S таке: sRs', якщо $f(s) = f(s')$. Тоді відношення R - відношення конгруентності.

Комутативну напівгрупу $(S, *)$ називають ***напіврешіткою***, якщо $a * a = a$ для всіх $a \in S$.

ТЕОРЕМА 16.5. Нехай S - напіврешітка. Відношення $\le$ на S визначимо так: $a \le b$, якщо $a * b = b$ для $a, b \in S$. Тоді $(S, \le)$ - це ЧУ-множина, і $a * b$ – найменша верхня грань для a і b. Отже, $(S, *)$ – верхня напіврешітка. Аналогічно, $(S, *)$ можна розглядати як нижню напіврешітку.

Решітки

Решітка – це множина M з двома бінарними операціями $\wedge$ і $\vee$, такими, що виконуються наступні умови (аксіоми решітки)

а) Комутативність

$$a \wedge b = b \wedge a;$$
$$a \vee b = b \vee a.$$

б) Асоціативність

$$(a \wedge b) \wedge c = a \wedge (b \wedge c);$$
$$(a \vee b) \vee c = a \vee (b \vee c).$$

в) Поглинання

$$a \wedge (a \vee b) = a;$$
$$a \vee (a \wedge b) = a.$$

Непорожню підмножину S' решітки (S, $\vee$, $\wedge$) називають ***підрешіткою*** решітки S, якщо для всіх $a, b \in S'$ $a \wedge b \in S'$ і $a \vee b \in S'$.

Решітку (S, $\vee$, $\wedge$) називають ***обмеженою***, якщо множина S, як ЧВ-множина, має найменшу верхню грань (позначають 1) і найбільшу нижню грань (позначають 0). Еквівалентно, решітка обмежена, якщо існують елементи $0, 1 \in S$ такі, що $0 \wedge a = 0$ і $1 \vee a = 1$ для всіх $a \in S$.

ТЕОРЕМА 16.6. В обмежених решітках $1 \wedge a = 1$ і $0 \vee a = a$ для всіх a з решітки.

Решітку (S, $\vee$, $\wedge$) називають ***дистрибутивною***, якщо для всіх $a, b, c \in S$ маємо $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$; $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Групи

Групою є множина G разом з бінарною операцією $\circ$ на $G \times G$, що має наступні властивості:

1. ***асоціативність***: $a \circ (b \circ c) = (a \circ b) \circ c$ $\forall$ a, b і $c \in G$.

2. існування ***одиниці***: в G існує такий елемент 1, $\forall$ $a \in G$ $a \circ 1 = 1 \circ a = a$.

3. існування ***симетричного*** (***оберненого***, ***протилежного***) ***елементу***: $\forall$ $a \in G$ $\exists$ $a^{-1} \in G$, такий, що $a \circ a^{-1} = a^{-1} \circ a = 1$.

Група – це моноїд, в якому $\forall$ a $\exists$ a^{-1} що $a * a^{-1} = a^{-1} * a = 1$.

Якщо група G має властивість $a \circ b = b \circ a \ \forall \ a, b$ з G, то її називають ***комутативною*** (***абелевою***) групою.

Якщо G - група з n елементами, то n називається ***порядком*** групи G.

Будь-яка група є напівгрупою. Обернене не завжди вірно.

ТЕОРЕМА 16.7. Одиниця групи G єдина.

ТЕОРЕМА 16.8. В кожній групі обернений елемент для кожного елементу єдиний.

ТЕОРЕМА 16.9. Для кожного елемента a групи G $(a^{-1})^{-1} = a$.

ТЕОРЕМА 16.10. Для елементів a і b групи G маємо

$(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

ТЕОРЕМА 16.11. Нехай G - група і a - елемент групи G.

а) $a^n \circ a^{-n} = 1 \ \forall \ n \in N$.

б) $a^{(m+n)} = a^m \circ a^n$ для всіх цілих чисел n і m.

в) $(a^m)^n = a^{mn}$ для всіх цілих чисел m і n.

г) $(a^{-n})^{-1} = a^n$ для всіх цілих чисел n.

ТЕОРЕМА 16.12. Якщо a - елемент групи $(G, \circ)$ і $a \circ a = a$, то $a = 1$, одиниці групи G.

ЛЕМА. Якщо G - скінченна група і a - елемент G, то $a^s = 1$ для деякого натурального числа s.

ТЕОРЕМА 16.13. Нехай G - група і a - елемент G такий, що $a^s = 1$ для деякого s. Якщо p - найменше додатне ціле число таке, що $a^p = 1$, то $p \mid s$. Ціле число p називають ***порядком*** a.

Підмножина H групи G є ***підгрупою*** G, якщо H з тією ж самою операцією, що і G, також є групою.

Нехай $(R, +)$ - група дійсних чисел з операцією $+$. Тоді група $(Q, +)$ - раціональні числа з $+$, є підгрупою групи $(R, +)$.

Нехай $(R^+, \cdot)$ - група додатніх дійсних чисел з множенням. Група $(Q^+, \cdot)$ додатніх раціональних чисел з множенням є підгрупою групи $(R^+, \cdot)$.

ТЕОРЕМА 16.14. Непорожня підмножина H групи $(G, \cdot)$ буде підгрупою тоді і лише тоді, коли для всіх $h_1, h_2 \in H$ $h_1 \cdot h_2^{-1} \in H$.

ТЕОРЕМА 16.15. Якщо g - елемент групи G | $g^n = 1$ для деякого n, і p - найменше натуральне число | $g^p = 1$, тоді множина $\{g, g^2,..., g^p\}$ є підгрупою групи G.

Множину $\{g, g^2,..., g^p\}$ називають ***циклічною групою***, породженою g. Вона позначається через $<g>$.

ТЕОРЕМА 16.16. Нехай $(G, \cdot)$ – група і $a_1, a_2, a_3,\ldots, a_k \in G$. Нехай $A = \{a_1, a_2, a_3,\ldots, a_k\}$ і $A^* = <a_1, a_2, a_3,\ldots, a_k>$ - множина всіх скінченних добутків елементів $a_1, a_2, a_3,\ldots, a_k$ і обернених до них. Тоді A^* - група. Більш того, A^* - найменша підгрупа групи G, що містить A.

Підгрупу A^* називають групою, ***породженою*** множиною A. Якщо для кожної власної підмножини B множини A маємо $B^* \neq A^*$, тоді A називають ***породжуючою множиною*** для A^*. Якщо множина A породжує групу G і жодна власна підмножина множини A не породжує G, тоді A називається ***мінімальною породжуючою множиною*** для групи G.

Для підгрупи H групи G і довільного a з G $a \circ H = \{x: x = a \circ h$ для деякого h з $H\}$ називають ***лівим суміжним класом*** підгрупи H групи G.

ЛЕМА. Для фіксованої підгрупи H групи G ліві суміжні класи підгрупи H групи G утворюють розбиття групи G.

ЛЕМА. Якщо G - скінченна група і H - підгрупа групи G, то всі ліві суміжні класи підгрупи H групи G містять однакову кількість елементів, а саме, кількість елементів, що містяться в підгрупі H.

☑ **ТЕОРЕМА**. **(Лагранж)** Якщо G - скінченна група і H - підгрупа групи G, то порядок H ділить порядок G.

☑ **ТЕОРЕМА 16.17**. Якщо G - група порядку n і $a \in G$, то $g^n = 1$.

Групи і гомоморфізми

Нехай (G, •) і (H, *) - групи, де • і * - операції на G і H відповідно.

Нехай $f : G \to H$ - функція. Функція f називається ***гомоморфізмом***, якщо $f(g \bullet g') = f(g) * f(g')$ для всіх g і g' з G. Гомоморфізм f називається ***мономорфізмом***, якщо функція f - ін'єкція, ***епіморфізмом***, якщо функція f – сюр’єкція, і ***ізоморфізмом***, якщо функція f - бієкція.

ТЕОРЕМА 16.18 Нехай $f : G \to H$ - гомоморфізм з групи G в групу H і 1 - одиниця групи G. Тоді $f(1)$ - одиниця групи H.

ТЕОРЕМА 16.19. Нехай $f : G \to H$ - гомоморфізм з групи G в групу H і g' - елемент, обернений елементу g з G. Тоді $f(g')$ є елемент, обернений елементу $f(g)$ з H.

ТЕОРЕМА 16.20. Якщо $f : G \to H$ - гомоморфізм з групи G в групу H і K - підгрупа групи H, то $f^{-1}(K)$ - підгрупа групи G.

ТЕОРЕМА 16.21. Якщо $f : G \to H$ - гомоморфізм з групи G в групу H і K - підгрупа G, то $f(K)$ - підгрупа групи H.

ТЕОРЕМА 16.22. Якщо H, J і K - підмножини групи $(G, \circ)$, то $(H \circ J) \circ K = H \circ (J \circ K)$.

Якщо H - підгрупа групи $(G, \circ)$, що має властивість $gHg^{-1} = H$ для всіх $g \in G$, то така група H називається ***нормальною підгрупою.***

Нехай $f : G \to H$ - гомоморфізм з групи G в групу H. ***Ядром*** гомоморфізму f називається множина $\{x : x \in G$ і $f(x) = 1\} = f^{-1}(\{1\})$, де 1 - одиниця групи H.

ТЕОРЕМА 16.23. Ядро гомоморфізму $f : G \to H$ є нормальна підгрупа групи G.

ТЕОРЕМА 16.24. Підгрупа H групи $(G, \circ)$ є нормальною підгрупою тоді і лише тоді, коли $gH = Hg$ для всіх $g \in G$.

ТЕОРЕМА 16.25. Якщо H - підгрупа групи $(G, \circ)$, то $H \circ H = H$.

ТЕОРЕМА 16.26. Якщо H - нормальна підгрупа групи $(G, \circ)$, то $abH = (aH)(bH)$ для всіх $a, b \in G$.

НАСЛІДОК. Якщо H - нормальна підгрупа групи $(G, \circ)$, то суміжні класи підгрупи H в групі G породжують групу відносно операції $(aH)(bH) = abH$. Ця група називається ***фактор-групою*** і позначається G/H.

НАСЛІДОК. Якщо $f : G \to G/H$ визначити співвідношенням $f(a) = aH$, то f - гомоморфізм.

Література

- Андерсон Д.А. Дискретная математика и комбинаторика: Пер. с англ.. – М.: Изд. дом «Вильямс», 2003. – 960 с
- Грэхем Р., Кнут Д., Паташник О., Конкретная математика. Основание информатики: Пер. с англ. – М.: Мир, 1998. – 703 с.
- Новиков Ф.А. Дискретная математика для программистов: Учебник для вузов. 3-е изд. – Спб.: Питер, 2008. – 384 с.
- Белоусов А.И., Ткачев С.Б. Дискретная математика: Учеб. для вузов. 3-е изд. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2004. – 744 с.

Дякую за увагу