2 ГРУПИ. КІЛЬЦЯ. ПОЛЯ

2.1 Поняття алгебраїчної операції. Поняття групи

Нехай задано дві множини X та Y. Нехай x – деякий елемент множини X, y – деякий елемент множини Y. З цих двох елементів утворимо впорядковану пару (x, y). Множина усіх пар (x, y), $x \in X, y \in Y$ утворює нову множину, яка називається *декартовим добутком множин* X та Y (позначається $X \times Y$). Якщо множини X та Y співпадають, то декартовий добуток $X \times X$ називається *декартовим квадратом* та позначається символом X^2. Кажуть, що на множині X задано *бінарну алгебраїчну операцію*, якщо довільній парі (x, y) елементів множини X ставиться у відповідність один елемент цієї множини (або операція є замкненою на множині). Інакше кажучи, на X задано алгебраїчну операцію, якщо задано відображення множини X^2 на X. Алгебраїчну операцію зазвичай позначають одним із символів: $\cdot, \circ, +, \times, \otimes$.

Множину X, на якій задано одну алгебраїчну операцію над його елементами, називають *групоїдом* $X(\circ)$. Якщо множина X скінченна, то групоїд часто описують за допомогою *таблиці Келі.*

Приклад 2.1 На множині $X = \{0,1,2,3\}$ задано операцію «додавання» наступним чином: $\forall a,b \in X \;\; a \oplus b$ – остача від ділення $a+b$ на 3. Тоді дану операцію можна представити таблицею Келі (таблиця 2.1).

Таблиця 2.1 – Таблиця Келі операції $\oplus$ на множині $X = \{0,1,2,3\}$

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	0	1
2	2	0	1	2
3	3	1	2	0

Два групоїда $X(\cdot)$ та $Y(\circ)$ називаються *ізоморфними*, якщо існує таке взаємно однозначне відображення f між множинами X та Y, що $\forall\, x, y \in X \;\; f(x \cdot y) = f(x) \circ f(y)$. Відображення f групоїда $X(\cdot)$ на групоїд $Y(\circ)$ називається *гомоморфізмом*, $\forall\, x, y \in X \;\; f(x \cdot y) = f(x) \circ f(y)$.

Групоїд $X(\cdot)$ з асоціативною алгебраїчною операцією ($\forall x, y, z \in X \;\; x \cdot (y \cdot z) = (x \cdot y) \cdot z$) називається півгрупою. Півгрупа $X(\cdot)$, в якій існує нейтральний елемент e: $\forall x \in X \;\; e \cdot x = x \cdot e = x$, і в якій $\forall x \in X$ існує обернений елемент x^{-1}: $x^{-1} \cdot x = x \cdot x^{-1} = e$, називається групою. Група $X(\cdot)$ називається *абелевою*, якщо $\forall x, y \in X \;\; x \cdot y = y \cdot x$, тобто операція $"\cdot"$ є комутативною.

Якщо група X містить скінчене число елементів, то вона називається скінченою. Якщо операція над елементами групи називається додаванням, то група називається *адитивною*; якщо ж операція – множення, то *мультиплікативною*.

2.2 Поняття кільця та поля

Множина K, в якій визначені дві алгебраїчні операції $''+''$ і $''\cdot''$ – додавання і множення, називається кільцем, якщо ці операції задовольняють наступним вимогам: $\forall\ a,b,c \in K$

1. додавання асоціативне: $a+(b+c)=(a+b)+c$;
2. додавання комутативне: $a+b=b+a$;
3. $\exists!\ 0 \in K$ (нуль кільця): $a+0=0+a=a$;
4. $\forall\ a \in K\ \exists!\ -a \in K:\ a+(-a)=0$;
5. добуток асоціативний: $a\cdot(b\cdot c)=(a\cdot b)\cdot c$;
6. додавання та множення пов'язані законами дистрибутивності: $(a+b)\cdot c=a\cdot c+b\cdot c$, $a\cdot(b+c)=a\cdot b+a\cdot c$.

З перших п'яти умов випливає, що K повинно бути адитивною абелевою групою по відношенню до операції додавання, а по відношенню до множення – півгрупою. Якщо в кільці $K(+,\cdot)$ операція множення комутативна: $a\cdot b=b\cdot a$, то кільце називається комутативним. Якщо в кільці $K(+,\cdot)$ можна знайти такі елементи a та b, відмінні від нуля, що $a\cdot b=0$, то ці елементи називаються дільниками нуля, причому a – лівим дільником, а b – правим.

Множина P, в якій визначені дві алгебраїчні операції додавання $''+''$ та множення $''\cdot''$, називається полем, якщо ці операції задовольняють наступним вимогам: $\forall\, a,b,c \in P$

1. додавання асоціативне: $a+(b+c)=(a+b)+c$;
2. додавання комутативне: $a+b=b+a$;
3. $\exists!\ 0 \in K$ (нуль кільця): $a+0=0+a=a$;
4. $\forall\ a \in K\ \exists!\ -a \in K:\ a+(-a)=0$;
5. добуток асоціативний: $a\cdot(b\cdot c)=(a\cdot b)\cdot c$;
6. добуток комутативний: $a\cdot b=b\cdot a$;
7. у множині P існує такий елемент 1, що $a\cdot 1=1\cdot a=a$;
8. $\forall\ \ a \in P,\ a\neq 0\ \exists\, a^{-1}:\ a\cdot a^{-1}=a^{-1}\cdot a=1$;
9. додавання та множення пов'язані законами дистрибутивності: $(a+b)\cdot c=a\cdot c+b\cdot c$.

Вимоги 1-4 означають, що множина P по відношенню до операції додавання є абелевою групою. Вимоги 5-8 означають, що $P\backslash\{0\}$ є мультиплікативною абелевою групою. З означення поля P випливає, що P є кільцем. Таким чином можна сформулювати означення поля. Полем називається комутативне кільце з 1, у якому кожний ненульовий елемент оборотний.

Теоретичні питання

1. Що таке декартовий добуток двох множин, декартів квадрат множини?
2. Означення бінарної алгебраїчної операції. Асоціативна операція. Комутативна операція.
3. Нейтральний елемент. Протилежний, обернений елемент. Симетричний елемент.

4. Що таке групоїд? Який групоїд називається скінченим, асоціативним?
5. Означення півгрупи, групи
6. Мультиплікативна, адитивна група. Комутативна (абелева) група. Порядок групи.
7. Означення кільця, підкільця.
8. Асоціативне, комутативне кільце.
9. Оборотний (зліва, справа) елемент кільця. Ненульовий дільник нуля.
10. Означення поля, підполя. Скінчені поля.