Algebra
2. Grupy, pierścienie, ciała - definicje i podstawowe przykłady.

Grupa – struktura algebraiczna definiowana jako zbiór z określonym na nim łącznym i odwracalnym dwuargumentowym działaniem wewnętrznym.
Dział matematyki badający własności grup nazywa się teorią grup.

Grupa:

Niech $\mathbb{R}_+$ oznacza zbiór dodatnich liczb rzeczywistych wraz z działaniem mnożenia, które przejawia własności analogiczne do powyższych:

- $\cdot$ jest działaniem dwuargumentowym na $\mathbb{R}_+$, tzn. dla dowolnych $a, b \in \mathbb{R}_+$ jest $a \cdot b \in \mathbb{R}_+$;
- dla dowolnych $a, b, c \in \mathbb{R}_+$ zachodzi $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- liczba $1 \in \mathbb{R}_+$ ma własność $a \cdot 1 = a$ dla wszystkich $a \in \mathbb{R}_+$;
- dla każdej liczby $a \in \mathbb{R}_+$ istnieje odwrotna do niej dodatnia liczba rzeczywista $1/a$, tzn. taka że $a \cdot \frac{1}{a} = 1$.

Zbiór G z (dobrze[a]) określonym na nim dwuargumentowym działaniem $\circ$ nazywa się **grupą**, jeżeli ma on następujące własności (spełnia poniższe aksjomaty):

- *Wewnętrzność*: dla dowolnych elementów a, b ze zbioru G ich wynik $a \circ b$ również należy do zbioru G; mówi się wtedy, że zbiór G jest *zamknięty* ze względu na $\circ$.
- *Łączność*: dla wszystkich a, b, c należących do G musi zachodzić $(a \circ b) \circ c = a \circ (b \circ c)$.
- *Element neutralny*: istnieje element e w zbiorze G spełniający dla dowolnego elementu a z tego zbioru warunek $a \circ e = a$.
- *Odwracalność*: dla każdego $a \in G$ musi istnieć $x \in G$, dla których $a \circ x = e$.

Pierścień – struktura formalizująca własności algebraiczne liczb całkowitych oraz arytmetyki modularnej; intuicyjnie zbiór, którego elementy mogą być bez przeszkód dodawane, odejmowane i mnożone, lecz niekoniecznie dzielone.

Pierścień:

Niech $(R, +, \cdot, 0)$ będzie algebrą, w której R jest pewnym niepustym zbiorem, symbole $+, \cdot$ oznaczają dwa działania dwuargumentowe określone w tym zbiorze, a 0 jest pewnym wyróżnionym elementem. Algebra ta nazwana jest **pierścieniem** jeśli:

- struktura $R^+ = (R, +, 0)$ jest grupą abelową, nazywaną grupą addytywną, z działaniem $+$ nazywanym **dodawaniem** i elementem neutralnym 0 nazywanym **zerem**:
  $\forall_{a,b,c \in R}\ a + (b + c) = (a + b) + c,$
  $\forall_{a \in R}\ a + 0 = a,$
  $\forall_{a \in R}\ \exists_{b \in R}\ a + b = 0,$
  $\forall_{a,b \in R}\ a + b = b + a;$
- struktura $(R, \cdot)$ jest półgrupą z działaniem $\cdot$ nazywanym **mnożeniem**:
  $\forall_{a,b,c \in R}\ a \cdot (b \cdot c) = (a \cdot b) \cdot c;$
- oba działania powiązane są ze sobą prawami rozdzielności:
  $\forall_{a,b,c \in R}\ a \cdot (b + c) = (a \cdot b) + (a \cdot c),$
  $\forall_{a,b,c \in R}\ (b + c) \cdot a = (b \cdot a) + (c \cdot a).$

Ciało – struktura formalizująca własności algebraiczne liczb wymiernych czy liczb rzeczywistych.

Ciało:

Ciałem nazywa się pierścień przemienny, w którym każdy niezerowy element jest odwracalny. Mówiąc wprost, ciało K to struktura $(K, +, \cdot, 0, 1)$ taka, że

- zbiór K zawiera co najmniej dwa elementy oznaczane symbolami $\mathbf{0}$ oraz $\mathbf{1}$,
- $(K, +, \cdot, 0, 1)$ jest pierścieniem przemiennym, to znaczy $+$ i $\cdot$ są działaniami w zbiorze K, nazywanymi odpowiednio **dodawaniem** i **mnożeniem** spełniającymi warunki:
  $\forall_{a,b,c\in K}\ a + (b + c) = (a + b) + c,$
  $\forall_{a\in K}\ a + 0 = a,$
  $\forall_{a\in K}\ \exists_{b\in K}\ a + b = 0,$
  $\forall_{a,b\in K}\ a + b = b + a;$
  $\forall_{a,b,c\in K}\ a \cdot (b \cdot c) = (a \cdot b) \cdot c,$
  $\forall_{a\in K}\ a \cdot 1 = a,$
  $\forall_{a,b,c\in K}\ a \cdot (b + c) = (a \cdot b) + (a \cdot c),$
  $\forall_{a,b\in K}\ a \cdot b = b \cdot a.$
- każdy niezerowy element jest odwracalny, tzn.:
  $\forall_{a\in K\setminus\{0\}}\ \exists_{b\in K}\ a \cdot b = 1,$