3.2. Grupy, pierścienie, ciała - definicje i podstawowe przykłady

Zbiór G wraz z działaniem dwuargumentowym

$$*: G\times G \quad [(x,y)\text{—>}*(x,y)= x*y=x\cdot y]$$

nazywamy **grupą** o ile są spełnione następujące własności:

I. $\forall_{x,y,z\in G}$ (x * y) * z = x* (y * z) (łączność)
II. $\exists_{e\in G}\ \forall_{x\in G}$ x*e = x = e*x (istnienie elementu neutralnego)
III. $\forall_{x\in G}\ \exists_{y\in G}$ x*y = e =y *x (istnienie elementu odwrotnego dla każdego elementu grupy)

G=(G,*) jest grupą przemienną(abelową) o ile dodatkowo :

IV. $\forall_{x,y\in G}$ x*y = y*x

Niech G będzie grupą zaś H≠Ø podzbiorem G. Wówczas H nazywamy podgrupą G o ile:

I. $\forall_{a,b\in H}$ a*b $\in H$
II. $\forall_{a\in H}\ a^{-1} \in H$

Przykłady:

I. Grupy macierzowe są podgrupami abstrakcyjnymi (podgrupy grupy Gl_n(k))
II. $\mathbb{R}^+$ =($\mathbb{R}$,+: $\mathbb{R}\times\mathbb{R}$ —> $\mathbb{R}$) jest grupą przemienną
    - + jest poprawnie określoną funkcja
    - funkcja + jest łączna
    - 0 jest elementem neutralnym dla +
    - $\forall_{a\in R}$ -a jest elementem odwrotnym (przeciwnym gdy działanie oznaczymy +)
    - + jest działaniem przemiennym
III. $\mathbb{Z}^+$= ($\mathbb{Z}$, +: $\mathbb{Z}\times\mathbb{Z}$—> $\mathbb{Z}$) jest grupą addytywną przemienną liczb całkowitych
    - Z+Z⊂Z
    - łączność i przemienność jest dziedziczona z R
    - 0 jest elementem neutralnym
    - $\forall_{a\in Z}$ -a jest elementem odwrotnym
IV. X = zbiór S_x=(σ: X—>X- bijekcja) $S_x = (S_x,\circ)$ S_x jest grupą nieprzemienną o ile |X|≥3 (złożenie bijekcji jest bijekcją)
V. Grupa $\mathbb{Z}_n$ reszt modulo n. Na zbiorze $\mathbb{Z}_n$ zadajemy działanie
   $\odot=\odot_n$: $\mathbb{Z}_n\times\mathbb{Z}_n$ —>$\mathbb{Z}_n$
   $a\odot b = r_n$(a·b) , a,b $\in\mathbb{Z}_n$
   r_n − reszta z dzielenia x przez n
VI. Uwaga ($\mathbb{Z}$\{0},·) NIE jest grupą
VII. $\mathbb{R}^+$ =($\mathbb{R}$\{0}, · : $\mathbb{R}\times\mathbb{R}$ —> $\mathbb{R}$) jest grupą multiplikatywną
    - $\mathbb{R}\ni a,b\neq 0 \implies 0\neq a\cdot b\in\mathbb{R}$
    - $1\in\mathbb{R}$ element neutralny
    - $\mathbb{R}\ni a\neq 0\implies 0\neq\frac{1}{a}\in\mathbb{R}$ element odwrotny w sensie działania ·

Układ $R=(R,+,\cdot)$ gdzie $+,\cdot: R\times R \longrightarrow R$ są działaniami dwuargumentowymi (+ - dodawanie, · - mnozenie) nazywamy **pierścieniem** o ile:

I. $R^+ = (R,+)$ jest grupą przemienną
II. $\forall_{a,b,c\in R}$ $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ mnożenie jest łączne
III. $\forall_{a\in R}\ \exists_{e\in R}$ $a\cdot e=e\cdot a=a$ element neutralny (oznaczony przez 1)
IV. $\forall_{a,b,c\in R}$ $a\cdot(b+c)=a\cdot b+a\cdot c$
$(b+c)\cdot a=b\cdot a+c\cdot a$ - mnozenie jest rozdzielne względem dodawania

Pierścień R nazywamy przemiennym o ile mnożenie jest przemienne:

$$\forall_{a,b\in R} \quad a\cdot b=b\cdot a$$

Układ $R=(R,+,\cdot)$ nazywamy **ciałem** o ile spełniony jest pierścieniem przemiennym i spełniony jest dodatkowy warunek :

$$\forall_{0\neq a\in R}\ \exists_{0\neq b\in R}\ a\cdot b=1$$

Niech R=(R,+, ·) będzie pierścieniem (przemiennym). Podzbiór S ⊂R nazywamy **podpierścieniem** (ewentualnie **podciałem**) o ile:

I. $\forall_{a,b,c\in S}$ $a+b\in S$ $a\cdot b\in S$
II. $1,0\in S$
III. (dla podciała) $\forall_{0\neq a\in S}\ \exists_{x\in S}$ $x\cdot s=s\cdot x=1$
IV. (równoważne) $\forall_{0\neq a\in S}\ a^{-1}\in S$

Przykłady:

I. $\mathbb{Z}=(\mathbb{Z},+,\cdot)$ – pierścień liczb całkowitych
- Działania sa, łac, zne i przemienne
- 0 jest elementem neutralnym dla +
- 1 jest elementem neutralnym dla ·
- rozdzielno´s´c jest spełniona
- to nie jest ciało bowiem 2 · x = 1 nie ma rozwia, zania w Z

II. $\mathbb{Q}=(\mathbb{Q},+,\cdot)$- ciało liczb wymiernych
- posiada te same własno´sci jak pier´scie ´n liczb całkowitych
- $\mathbb{Q}\ni q(\neq 0)=\frac{a}{b}\Longrightarrow q^{-1}=\frac{b}{a}\in\mathbb{Q}$

III. $\mathbb{R}=(\mathbb{R},+,\cdot)$- ciało liczb rzeczywistych
IV. $M_n(\mathbb{R})=(M_n,+,\cdot)$ pierścień naprzemienny(n≥2)
V. Pierścień reszt modulo n
VI. Ciałami są elementy łańcucha: liczby wymierne ← liczby rzeczywiste ← liczby zespolone.