- X,Y-zbiory. Przekształcenie (odwzorowanie, funkcja) $F : X \to Y$ jest *różnowartościowe* (jest *injekcją,*) jeśli $\forall x, y \in X \; F(x) = F(y) \Rightarrow x = y$.

  Przekształcenie $F : X \to Y$ jest *na* Y (jest *surjekcją,*) jeśli $\forall y \in Y \; \exists x \in X \;\; F(x) = y$.

  Przekształcenie $F : X \to Y$ jest *bijekcją,* jeśli jest injekcją i surjekcją.

- *Permutacje.* X-zbiór skończony $|X| < \infty$. Jeśli $|X| = n$, to X można utożsamiać ze zbiorem $\{1, ..., n\}$.

  Permutacją zbioru X nazywamy dowolną bijekcję zbioru X na zbiór X.

  Przykłady: $X = \{1, 2, 3, 4, 5, 6\}$. Wtedy permutację można zapisać

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$$

  lub $(1, 6)(2, 4, 5)(3)$ lub $(1, 6)(2, 4, 5)$.

  Ilość permutacji zbioru n-elementowego to $n!$.

  Złożenie dwóch permutacji zbioru X jest permutacją zbioru X. Składanie jest łączne tzn. $\forall a, b, c \;\; (a \circ b) \circ c = a \circ (b \circ c)$.

  Niech e oznacza permutację identycnościową tzn. $\forall x \in X \;\; e(x) = x$. Wtedy $a \circ e = e \circ a = a$.

  Niech a^{-1} oznacza funcję odwrotną do a. Wtedy $\forall a \;\; a \circ a^{-1} = a^{-1} \circ a = e$.

  Przykład:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 6 & 4 & 3 & 5 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 4 & 1 \end{pmatrix}.$$

- *Grupy.* Niech G będzie zbiorem. Jeśli istnieją

$$\bullet : G \times G \ni (a, b) \mapsto a \bullet b \in G \;\; (\textit{działanie})$$
$$G \ni a \mapsto a^{-1} \in G \;\; (\textit{operacja brania elementu odwrotnego})$$

  oraz $e \in G$ (*element neutralny*) spełniające warunki:

  - (*łączność działania*) $\forall a, b, c \in G \;\; (a \bullet b) \bullet c = a \bullet (b \bullet c)$,
  - $\forall a \in G \;\; a \bullet e = e \bullet a = a$,
  - $\forall a \in G \;\; a \bullet a^{-1} = a^{-1} \bullet a = e$,

  to G (lub $(G, \bullet)$ lub $(G, \bullet, ^{-1}, e)$) nazywamy *grupą.*

  Jeśli dodatkowo działanie grupowe jest przemienne, tzn.$\forall a, b \in G \;\; a \bullet b = b \bullet a$, to grupę G nazywamy *abelową.*

  Przykłady: Permutacje zbioru X wraz ze składaniem, $GL(n, R)$-grupa nieosobliwych rzeczywistych macierzy n na n z mnożeniem macierzowym, $SGL(n, R)$-grupa rzeczywistych macierzy n na n o wyznaczniku równym 1 z mnożeniem macierzowym, $GL(n, C)$-grupa macierzy nieosobliwych zespolonych n na n z mnożeniem macierzowym,
  grupy abelowe:$(Z, +)$, $(Q, +)$,$(R, +)$,$(C, +)$, $(Q \setminus \{0\}, \cdot)$, $(R \setminus \{0\}, \cdot)$, $(C \setminus \{0\}, \cdot)$, $(Z_p, +mod\ p)$.

  Tw. $\forall a, b \in G \;\; (a \bullet b)^{-1} = b^{-1} \bullet a^{-1}$

- *Podgrupy.* $H \subset G$ jest *podgrupą* grupy G jeśli $(H, \bullet|_{H \times H}, ^{-1}|_H, e)$ jest grupą.

  Przykłady: $SGL(n, R)$-podgrupa $GL(n, R)$,$(Z, +)$-podgrupa $(Q, +)$-podgrupa $(R, +)$-podgrupa $(C, +)$, $(Q \setminus \{0\}, \cdot)$-podgrupa $(R \setminus \{0\}, \cdot)$-podgrupa $(C \setminus \{0\}, \cdot)$.

  Tw. $H \subset G$ jest *podgrupą* grupy G wtedy i tylko wtedy, gdy

  - $\forall a, b \in H \;\; a \bullet b \in H$,
  - $\forall a \in H \;\; a^{-1} \in H$.

- *Grupy skończone.* G-grupa *skończona,* jeśli $|G| < \infty$.

  Tw.$\forall a \in G$-grupa skończona $\exists n \in N \setminus \{0\} \quad a^n = e$.

  Rzędem elementu $a \in G$ nazywamy najmniejsze takie $n \in N \setminus \{0\}$, że $a^n = e$.

  Tw. $H \subset G$ jest podgrupą grupy skończonej G wtedy i tylko wtedy, gdy $\forall a, b \in H \quad a \bullet b \in H$.

- *Grupy permutacji.* Grupę wszystkich permutacji zbioru X nazywamy *grupą symetryczną* zbioru X i oznaczamy $S(X)$. Jeśli $|X| = n$, to $S(X)$ nazywamy *grupą symetryczną stopnia* n i oznaczmy przez S_n.

  Każdą podgrupę G grupy S_n nazywamy *grupą permutacji stopnia* n *działającą na zbiorze* X, czyli grupa permutacji to para uporządkowana (G, X), gdzie G jest podgrupą $S_n = S(X)$.

  Przykład: $G = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ podgrupa S_4.

  Tw. Rząd permutacji a jest równy najmniejszej wspólnej wielokrotności długości cykli występujących w rozkładzie permutacji na cykle.

  Przykład: $rz\k{a}d(1,2,3,4)(5,6,7)(8,9)(10) = NWW(4,3,2,1) = 12$.

- *Homomorfizm grup.* $(G, \bullet), (H, \star)$-grupy. Odwzorowanie $\phi : G \to H$ nazywamy *homomorfizmem,* jeśli

$$\forall a, b \in G \quad \phi(a \bullet b) = \phi(a) \star \phi(b).$$

  $\phi : G \to H$ nazywamy $izomorfizmem$, jeśli ϕ jest homomorfizmem i bijekcją.

  Przykład: Jeśli $\phi : (R, +) \to (R, +)$ jest homomorfizmem to $\phi(a + b) = \phi(a) + \phi(b)$. Najprostszym przykładem jest $\phi(a) = \lambda a$. Jeśli $\lambda \neq 0$ to ϕ jest izomorfizmem.

- *Tw. Cayleya. Zał.* G-dowolna grupa, $G^\star$-grupa wszystkich permutacji zbioru G działających na G następująco:

  Niech $g \in G$. Wtedy $g^\star \in G^\star$, jeśli $\forall a \in G \quad g^\star(a) = a \bullet g$.

  Teza. $G \ni g \to g^\star \in G^\star$ jest izomorfizmem grup.

  Przykład: Niech $G = S_3$. Wtedy $S_3^\star$ jest następującą podgrupą $S(S_3) = S_6$:

$$S_3^\star = \{e, (1,2)(3,6)(4,5), (1,3)(2,5)(4,6), (1,4)(2,6)(3,5), (1,5,6)(2,3,4), (1,6,5)(2,4,3)\}.$$

- *Podobieństwo grup permutacji.* Dwie grupy permutacji (G, X) i (H, Y) są *podobne,* jeśli istnieje taka bijekcja $f : X \to Y$, że $H = \left\{f \circ a \circ f^{-1} : a \in G\right\}$.

  Tw. $\phi : G \ni a \to f \circ a \circ f^{-1} \in H$ jest izomorfizmem.

- *Generatory grupy* $a_1, ..., a_k \in G$ *generują* grupę G, jeśli $\forall a \in G \quad \exists x_1, ..., x_n \in \left\{a_1, ..., a_k, a_1^{-1}, ..., a_k^{-1}\right\}$ takie, że $g = x_1 \bullet ... \bullet x_n$.

  Tw. Następujące zbiory są zbiorami generatorów S_n

  - wszystkie transpozycje,
  - $\{(1,2), (2,3), ..., (n-1, n)\}$,
  - $\{(1,2), (1,3), ..., (1,n)\}$,
  - $\{(1,2), (1,2,...,n)\}$.

  Tw. Jeśli permutacja a jest przedstawiona jako iloczyn transpozycji na dwa sposoby, to w obu przedstawieniach liczba transpozycji jest parzysta albo nieparzysta.

  Permutacje, które można przedstawić w postaci iloczynu parzystej (nieparzystej) liczby transpozycji nazywamy *parzystymi* (*nieparzystymi*).

  Tw. Permutacja jest parzysta wtedy i tyko wtedy, gdy w jej rozkładzie na cykle liczba cykli długosci parzystej jest parzysta.