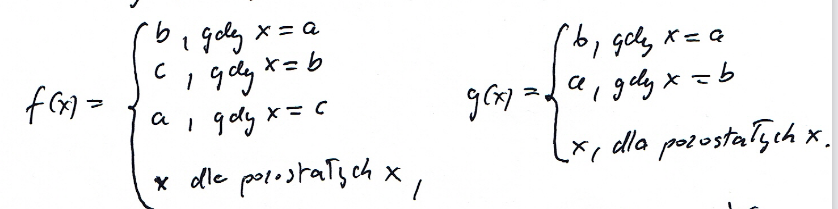
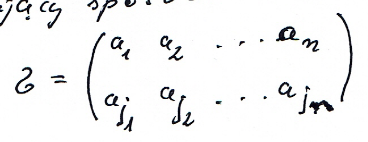
***Grupy odwzorowań. Permutacje****.*

 Kolejną grupę, istotną dla naszych dalszych rozważań, charakteryzuje następujące twierdzenie:  
 *Tw.* Jeżeli X jest niepustym zbiorem, to zbiór wszystkich jego bijekcji jest grupą ze składaniem odwzorowań jako działaniem grupowym.  
Przypomnijmy, że funkcja wzajemnie jednoznaczna zbioru X na siebie jest bijekcją.  
Grupę, o której mowa w twierdzeniu, nazywamy grupą symetryczną zbioru X i oznaczamy symbolem SX  
 Uwaga! Jeśli zbiór X zawiera co najmniej 3 elementy, to jego grupa symetryczna jest nieprzemienna. Istotnie, załóżmy że a, b i c są tymi elementami i określmy funkcje f i g wzorami:

Jest oczywiste, że f i g są bijekcjami zbioru X.  
Ponadto mamy:

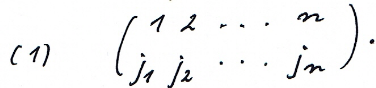
*(f ° g)(a) = f(g(a)) = f(b) = c* podczas gdy  
 *(g ° f)(a) = g(f(a)) = g(b) = a* Zatem f *° g* ≠ g *° f*  
Elementem neutralnym grupy SX jest oczywiście odwzorowanie idX (odwzorowanie tożsamościowe zbioru X).

Najbardziej będą nas interesować bijekcje zbioru mającego skończoną liczbę elementów.

 *Def.*  Niech X = {a1, a2, …, an). Bijekcję zbioru X na siebie nazywamy permutacją tego zbioru lub permutacją (przedstawieniem) elementów a1, a2, …, an. Permutację [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1): X 🡪 X , w której elementowi ak jest przyporządkowany element ajk  = [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1)(ak) zapisujemy symbolicznie:

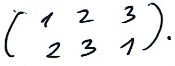


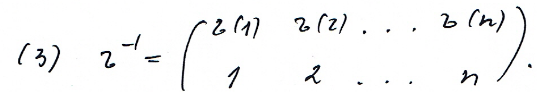
W górnym wierszu wpisujemy w kolejności rosnących wskaźników elementy zbioru X, a w dolnym, pod każdym z nich, umieszczamy jego obraz poprzez permutację [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1). Dolny wiersz różni się od górnego JEDYNIE zmienionym porządkiem wyrazów (każdy element zbioru X występuje w dolnym wierszu dokładnie raz.

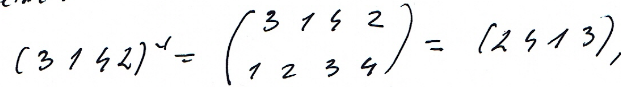
 *Uwaga! Każda permutacja* [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1): X 🡪 X dowolnego zbioru X o n elementach, określona wzorem  
 [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1)*(ak) = ajk (znowu podwójny dolny indeks)*  
 sprowadza się do permutacji k 🡪 jk zbioru Jn = {1, 2, …, n} (numerów elementów zbioru X), którą możemy zapisać w postaci

Tak więc, mówiąc o permutacji zbioru n-elementowego będziemy mieli na myśli permutację zbioru Jn (chyba że zaznaczymy wyraźnie że tak nie jest).

Ponieważ w symbolu (1), przy ustalonym n, pierwszy wiersz jest zawsze taki sam, będziemy dla uproszczenia zapisu pisać (2) (j1, j2, …, jn).

 *Przykład:*  
 (2 3 1) oznacza permutację zbioru J3 = {1, 2, 3}, która przeprowadza liczbę 1 w liczbę 2, liczbę 2 w liczbę 3, i liczbę 3 w liczbę 1, tj. w zapisie (1)

**Zgodnie z jednym z poprzednich stwierdzeń, zbiór wszystkich permutacji zbioru Jn jest grupą z działaniem składania permutacji. Grupę tę oznaczamy symbolem Sn (zamiast SJn ) i nazywamy grupą symetryczną stopnia n. Elementem neutralnym tej grupy jest permutacja identycznościowa (1 2 … n). Składanie permutacji wykonuje się stosując szereg prostych operacji. Zilustrujemy to na następującym przykładzie: złożyć permutacje (3 1 4 2) i (2 4 3 1). Mamy  
 *(2 4 3 1)(3 1 4 2) = (3 2 1 4),*  
w pierwszej permutacji (3 1 4 2) liczba 1 przechodzi w liczbę 3, a w drugiej permutacji liczba 3 przechodzi w liczbę 3. Dlatego w złożeniu (iloczynie) obu tych permutacji liczba 1 przechodzi w liczbę 3 itp. Podobnie mamy:  
 *(1 2 3 4)(3 1 4 2) = (3 1 4 2)  
 i  
 (3 1 4 2)(1 2 3 4) = (3 1 4 2)  
 ale  
 (3 1 4 2)(2 4 3 1) = (1 2 4 3)*Nietrudno (w przeciwieństwie do całej reszty tego tematu, huh?) też znaleźć permutację odwrotną (grupa!) do danej. Mamy

  
Tak więc np. permutacja odwrotna do permutacji (3 1 4 2) czyli permutacja (3 1 4 2)-1 to (2 4 1 3) [zapisujemy od tyłu do przodu]. Mamy bowiem



Łatwo sprawdzić że   
 *(2 4 1 3)(3 1 4 2) = (1 2 3 4) [transl: help :’)]  
 oraz  
 (3 1 4 2)(2 4 1 3) = (1 2 3 4)*

*Przykład:*   
 Znaleźć permutację spełniającą równanie  
 *(5 4 3 2 1)* [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) *(3 5 1 4 2) = (2 4 5 3 1)*

*Rozwiązanie:*  
 równanie mnożymy lewostronnie (obustronnie) przez permutację odwrotną do permutacji   
 (5 4 3 2 1). Mamy zatem  
 [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) *= (5 4 3 2 1)-1(2 4 5 3 1)(3 5 1 4 2)-1* i stąd otrzymujemy [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) = (1 5 4 3 2) [transl: wierzę na słowo]

*Def.* Niech dana będzie permutacja [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) 🡨 Sn, n ≥ 2, [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) = (j1, j2, …, jn).   
 Mówimy, że liczby jr i js tworzą inwersję, jeśli r < s oraz jr > js. Na przykład w permutacji (1 3 2) liczby 3 i 2 tworzą inwersję, natomiast liczby 1 i 3 jej nie tworzą.

Permutacja [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) nazywa się permutacją parzystą, jeżeli przy n ≥ 2 liczba inwersji w niej jest parzysta lub jeśli [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) ∈ S1. Permutacja [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) ∈ S1, n ≥ 2 jest permutacją nieparzystą, jeśli liczba inwersji w niej jest nieparzysta.  
*Przykład.* W permutacji [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) = (3 1 5 2 6 4) inwersje tworzą pary liczb: (3, 1), (3, 2), (5, 2), (5, 4), (6, 4). Liczba inwersji jest zatem nieparzysta (= 5), a więc permutacja ta jest nieparzysta.

*Def.* Znakiem permutacji [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) nazywamy liczbę +1, gdy [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) jest permutacją parzystą i liczbę -1, gdy nieparzystą. Znak permutacji oznaczamy symbolem sgn[Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1).

*Przykład.* Permutacja [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) = (3 1 5 2 6 4) jest nieparzysta, więc sng(3 1 5 2 6 4) = -1. Permutacja   
 [Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) = (3 5 4 1 6 2) jest parzysta, więc sgn(3 5 4 1 6 2) = +1

***Grupa Z/nZ***

  
*Def.* Niech n > 1 będzie ustaloną liczbą naturalną. W zbiorze liczb całkowitych Z określamy relację przystawiania modelu(?) n:  
 dla dowolnych a, b ∈ Z, a ~ b wtedy i tylko wtedy, gdy n|(a – b) [n dzieli a – b]  
Jeśli a ~ b, to mówimy że liczba a przystaje do liczby b modulo n i piszemy a b mod n.

*Lemat.* Relacja przystawania modulo n jest relacją równoważności na zbiorze Z.

Klasą abstrakcji [a]~ liczby a ∈ Z względem relacji przystawiania modulo n jest zbiór   
{a + kn: k ∈ Z}. Klasę abstrakcji [a]~ będziemy w skrócie oznaczać symbolem i nazywać klasą reszt modulo n. Zauważmy, że istnieje dokładnie n różnych klas reszt modulo n: , , …, , które wyznaczają podział zbioru Z. Zbiór klas abstrakcji { , , …, } oznaczamy symbolem Z/nZ i nazywamy zbiorem klas reszt modulo n. W zbiorze Z/nZ określamy operacje dodawania i mnożenia w następujący sposób:   
 + = , \* = , dla dowolnych , ∈ Z/nZ.

Łatwo pokazać, że dla n > 1 zbiór   
 Z/nZ = { , , …, } z powyżej określonym działaniem dodawania jest grupą abelową. Elementem neutralnym jest w tym przypadku klasa a elementem odwrotnym do ∈ Z/nZ jest klasa reszt liczby n – a.

*Przykład.* Dla n = 6 podać postać elementów zbioru Z/6Z. Mamy:

= { 0, ±6, ±12, ±18, …}  
 = {±1, ±7, ±13, ±19, …}  
 … (tutaj mamy 2-4 [z kreseczką ofc])  
 5 (bez kreseczki było) = {±5, ±11, ±17, ±23, …}

***Podgrupy***

*Def.* Niech G będzie grupą. Niepusty podzbiór H zbioru G jest podgrupą grupy G, jeżeli jest on grupą z   
 działaniem grupy G zawężonym do H × H.

W szczególności element neutralny podgrupy H jest identyczny z elementem neutralnym grupy G. Ponadto, dla każdego elementu a podgrupy H jego element odwrotny w grupie G należy również do H i jest elementem odwrotnym do a w grupie H.  
Jeśli zatem H jest podgrupą grupy G, to spełnione są następujące 2 warunki:

* jeżeli a, b ∈ H, to ab ∈ H
* jeżeli a ∈ H, to a-1 ∈ H

Łatwo zauważyć, że podzbiór złożony z elementu neutralnego grupy G jest oczywiście jej podgrupą. Podobnie, cała grupa G jest swoją własną podgrupą – są to tzw. podgrupy niewłaściwe grupy G. Wszystkie inne podgrupy będą nosiły nazwę podgrup właściwych. Podgrupa dowolnej grupy abelowej jest abelowa.

*Przykłady.* Ponieważ dla zbiorów Z, Q, R i C prawdziwe są relacje Z ⊂ Q ⊂ R ⊂ C i ponadto w każdym z tych zbiorów dodawanie liczb jest działaniem oraz są one zamknięte ze względu na operację brania elementu odwrotnego, więc każdy z nich jest kolejno podgrupą następnego z działaniem dodawania.

Zbiór wszystkich permutacji parzystych n elementów jest podgrupa grupy Sn. Oznaczamy ją przez An i nazywamy grupą alternującą stopnia n.

*Tw.* Rzęd podgrupy grupy skończonej jest podzielnikiem rzędu grupy.

*Def.* Podgrupa H grupy G jest jej podgrupą niezmienniczą, jeśli dla każdego elementu a grupy G zachodzi równość aHa-1 = H (zaśmiałam się z aHa xd), gdzie aHa-1 = {aba-1: b ∈ H}. Podgrupę niezmienniczą nazywa się również dzielnikiem normalnym grupy G.

*Przykłady.* W dowolnej grupie G jej podgrupy niewłaściwe G i {e} są podgrupami niezmienniczymi.  
W grupie abelowej **każda** podgrupa jest podgrupą niezmienniczą.

Podgrupa alternująca An jest podgrupą niezmienniczą grupy symetrycznej Sn. Zajmujemy się obecnie opisem odwzorowań działających pomiędzy zbiorami G i H będącymi grupami

***Homomorfizmy grup***

*Def.* Odwzorowanie h: G 🡪 H grupy G w grupę H nazywamy homomorfizmem grup lub krótko homomorfizmem, jeśli dla dowolnych dwóch elementów a i b grupy G zachodzi równość  
 *h(ab) = h(a)h(b).* Homomorfizm g: G 🡪 H nazywamy monomorfizmem, jeśli jest on iniekcją - parze różnych elementów a, b grupy G odpowiada para h(a), h(b) różnych elementów grupy H.  
 Homomorfizm h nazywamy epimorfizmem, jeśli jest on suriekcją – gdy obrazem grupy G poprzez odwzorowanie h jest cała grupa H.

*Przykład.* Odwzorowanie h: Sn 🡪 {-1, 1} dane wzorem h([Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1)) = sgn[Ƨ](https://lingwistyka.fandom.com/pl/wiki/%C6%A7?action=edit&redlink=1) jest epimorfizmem (nie jest to monomorfizm dla n > 2).

*Uwaga!* Homomorfizm h: G 🡪 H przeprowadza element neutralny grupy G na element neutralny grupy H, natomiast obrazem odwrotności dowolnego elementu jest odwrotność obrazu tego elementu, tj. h(a-1) = (h(a))-1, b.  
 *h(a)h(a-1) = h(aa-1) = h(e) = e* i *h(a-1)h(a) = h(a-1a) = h(e) = e*

***Def. (!!!)*** Jądrem homomorfizmu h: G 🡪 H nazywamy **zbiór wszystkich elementów grupy G**, które poprzez odwzorowanie h przechodzą na element neutralny grupy H. Zbiór ten oznaczamy symbolem Ker h. Zbiór ten **nigdy** nie jest pusty (zawsze zawiera element neutralny grupy G). Obrazem homomorfizmu h nazywamy zbiór wszystkich elementów grupy H, które są obrazami choć jednego elementu grupy G, tzw. zbiór h(G). Obraz homomorfizmu h oznaczamy symbolem lm h. Tak więc  
 *Ker h = {a* ∈ *G: h(a) = e}*,   
 *lm h = {b* ∈ *H: istnieje a* ∈ *G takie, że b = h(a)}.*

*Tw.* Obraz homomorfizmu h: G 🡪 H jest podgrupą grupy H. Jądro homomorfizmu h jest podgrupą niezmienniczą grupy G.

*Przykład.* Jądrem homomorfizmu h: Sn 🡪 {-1, 1} jest An, tj. Ker h = An (zbiór {-1, 1} jest grupą abelową z działaniem mnożenia).

*Def.* Homomorfizmem h: G 🡪 H nazywamy izomorfizmem, jeśli jest on równocześnie monomorfizmem i epimorfizmem, czyli jest to homomorfizm, który jest bijekcją grupy G na grupę H.

*Uwaga!* Jeżeli h: G 🡪 H jest izomorfizmem, to odwzorowanie odwrotne h-1: H 🡪 G również nim jest.

Grupę G nazywamy izomorficzną z grupą H, jeśli istnieje izomorfizm h: G 🡪 H. Wówczas (pow. Uwaga), grupa H jest izomorficzna z grupą G, dzięki czemu mówimy, że grupy G i H są izomorficzne – zapisujemy to w postaci G H. Relacja izomorfizmu jest relacją równoważności. Dzieli ona zbiór wszystkich grup na rozłączne klasy grup izomorficznych.

Grupy izomorficzne identyfikujemy ze sobą. Ich „organizacja” algebraiczna i wszystkie wynikające z niej konsekwencje są jednakowe (jednakowo?).

*Przykłady.* Niech n będzie dodatnią liczbą całkowitą. Wówczas zbiór pierwiastków zespolonych n-tego stopnia z 1 z działaniem mnożenia liczb zespolonych jest grupą, którą oznaczamy symbolem Tn. Ponadto, grupą jest też zbiór reszt z dzielenia przez n z działaniem dodawania modulo n w zbiorze Z i grupę tę oznaczamy symbolem Zn.

Grupy Zn i Tn **są izomorficzne** – odpowiedni izomorfizm dany jest wzorem:  
 *Zn* ∈ *k 🡪* ε *kn* ∈ *Tn ,*gdzie ε n jest pierwiastkiem pierwotnym n-tego stopnia z 1.

Grupy R i R+: = (0, nieskończoność) **są izomorficzne** – odpowiedni izomorfizm dany jest wzorem:  
 *R* ∈ *x -> ex* ∈ *R+*

*Tw.* **Każda** grupa skończona rzędu n jest izomorficzna z podgrupą grupy Sn.