Grupą, mości panowie

Teoria

Definicja *Zbiór G z określonym działaniem $*$ nazywamy* ***grupą*** *jeżeli*

1. *Dla wszystkich $a, b \in G$ jest $a * b \in G$,*
2. *Dla wszystkich $a, b, c \in G$ jest $(a * b) * c = a * (b * c)$ – kolejność wykonywania działań nie ma znaczenia*
3. *Istnieje* ***"jedynka"*** *–* ***element neutralny*** *działania, innymi słowy istnieje pewne $e \in G$ takie, że*

$$\text{dla każdego } x \in G \quad x * e = x \text{ i } e * x = x$$

4. *Dla każdego elementu $a \in G$ istnieje taki element $b \in G$, że*

$$a * b = e \text{ oraz } b * a = e$$

przypominam e to element neutralny grupy.

Podstawowe własności wynikające wprost z definicji. Można je wrzucić do definicji, ale wtedy sprawdzanie, czy dany zbiór jest podgrupą byłoby trudniejsze.

1. Z grupie jest dokładnie jeden element neutralny
   jeżeli $e, f \in G$ są elementami neutralnymi grupy G, to $e = f$.
2. W danej grupie G dany element $a \in G$ ma dokładnie jedną odwrotność.
   Innymi słowy, jeżeli elementy $b, c \in G$ są oba odwrotnościami a, to $b = c$.

Konwencje zapisu – jak pisać krócej.
Z pierwszej własności grup wynika, że w działaniu $*$ nie musimy używać nawiasów. Stosuje się konwencję

- ab jako zapis $a * b$,
- abc jako zapis $a * b * c$,
- 1 jako zapis elementu neutralnego grupy G,
- a^{-1} jako zapis elementu odwrotnego do elementu a.
- ab^{-1} jako zapis $a * (b^{-1})$.
- Tożsamość $aa^{-1} = 1$ już wygląda zwyczajnie prawda?

Alternatywna konwencja Zwłaszcza dla grup przemiennych często stosuje się zapis alternatywny "dodawanie" zamiast "mnożenia".

- $a + b$ jako zapis $a * b$,
- 0 jako zapis elementu neutralnego grupy G,
- $-a$ jako zapis elementu odwrotnego do a.
- $a - b$ jako zapis $a + (-b)$.
- Tożsamość (przykładowa) $a - a = 0$.

Przykładowe grupy

1. Dla danego zbioru X bijekcje $X \to X$ (bijekcja to funkcja różnowartościowa i przyjmująca wszystkie możliwe wartości) – działanie to składanie funkcji.
2. Dla danego zbioru X bijekcje $X \to X$, zachowujące dany punkt/zbiór punktów (Bijekcja $f : X \to X$ zachowuje podzbiór $Y \subset X$, jeżeli $f(Y) = Y$) – działanie to składanie funkcji.
3. Przekształcenia płaszczyzny zachowujące dany punkt.
4. Przekształcenia płaszczyzny zachowujące odległości pomiędzy punktami (*izometrie płaszczyzny*): w tym obroty, translacje, symetrie. . . (działanie = składanie przekształceń).
5. Izometrie płaszczyzny zachowujące dany trójkąt/czworokąt. . . (działanie = składanie przekształceń).
6. Zbiór liczb rzeczywistych/wymiernych/całkowitych z dodawaniem.
7. Zbiór liczb rzeczywistych/wymiernych/całkowitych bez zera z mnożeniem.
8. Zbiór $\{0, 1, \ldots, n-1\}$ z działaniem $a * b = a + b \mod n$.
9. Dla liczby pierwszej p zbiór $\{1, \ldots, p-1\}$ z mnożeniem $a * b = ab \mod p$.
10. Dla dowolnej liczby n zbiór liczb z $\{1, 2, \ldots, n\}$ które są względnie pierwsze z n, z mnożeniem $a * b = ab \mod n$. Ilość tych elementów oznacza się $\varphi(n)$.

Dodatkowe potrzebne definicje

1. **Definicja** *Jeżeli G jest grupą, oraz $H \subset G$ jest grupą ze względu na to samo działanie co G, to H nazywamy **podgrupą** grupy G.*

   Np. grupa liczb całkowitych z + jest podgrupą grupy liczb rzeczywistych z +.
2. **Definicja** *Jeżeli G jest grupą i G, jako zbiór jest skończony to mówimy, że grupa G jest **skończona**. W tym przypadku ilość elementów zbioru G oznaczamy (standardowo) $|G|$.*
3. Jeżeli dla każdych elementów a, b grupy G zachodzi $a * b = b * a$, to mówimy, że grupa jest **przemienna**.
4. Dla danego elementu a grupy skończonej G definiujemy **rząd** a jako najmniejsze $n \in \mathbb{Z}_+$ takie, że

   $$a^n = 1 \text{ w grupie } G$$

   Rząd elementu oznaczamy $\mathrm{ord}(a, G)$, lub $\mathrm{ord}(a)$, albo wręcz $o(a)$.

Wreszcie jakaś teoria

1. **Lemat** *Jeżeli G jest grupą z działaniem $*$ oraz $H \subset G$, przy czym zachodzi*

   $$\forall_{a,b \in H} \quad a * b \in H$$

   $$\forall_{a \in H} \quad a^{-1} \in H$$

   to H jest podgrupą G.
2. **Wniosek** *Jeżeli a jest elementem grupy skończonej G, to*

   $$\mathrm{ord}(a, G) \mid |G|$$

   $$a^{|G|} = 1 \text{ w grupie } G$$
3. **Twierdzenie (Lagrange)** *Jeżeli G jest grupą skończoną, zaś H jest podgrupą grupy G, to*

   $$|H| \mid |G|$$

4. **Wniosek (Fermat)** *Jeżeli p jest liczbą pierwszą zaś a jest całkowite dodatnie, to*

$$p|a^p - a$$

5. **Wniosek (Euler)** *Jeżeli liczby naturalne n, a są względnie pierwsze, to*

$$n|a^{\varphi(n)} - 1$$

6. **Wniosek (Lemat o rzędzie (słabsza forma))** *Jeżeli p jest liczbą pierwszą, zaś a jest liczbą całkowitą względnie pierwszą z p oraz $\mathrm{ord}(a, p)$ oznacza rząd a względem p (patrz kółko o rzędzie, definicja jest zgodna z powyższą) to*

$$\mathrm{ord}(a, p) \mid p - 1$$

Trochę teorii z * (dużo * na tym kółku :)

1. Dla danej grupy G i $g \in G$ zbiór postaci $\left\{1, g, g^2, \ldots, g^{\mathrm{ord}(g)-1}\right\}$ jest grupą; nazywamy go grupą generowaną przez g.

2. **Lemat** *Jeżeli grupa G jest skończona i przemienna, to dla dowolnych elementów $a, b \in G$ w grupie G istnieje element mający rząd $NWW(\mathrm{ord}(a), \mathrm{ord}(b))$.*

3. **Twierdzenie (Istnienie generatora)** *Jeżeli p jest liczbą pierwszą, to grupa*

$$\{1, 2, \ldots, p-1\}$$

z mnożeniem $\mod p$ jest grupą generowaną przez pewien element g, innymi słowy istnieje takie g, że liczby $\left\{g, g^2, \ldots, g^{p-1}\right\}$ dają parami różne reszty z dzielenia przez p.