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*

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

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

$$a * b = e \ oraz\ b * a = e$$

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 $e = f$.
   Dowód:
   Niech e, f będą elementami neutralnymi grupy G. Wtedy
   $$e = ef = f$$
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 $b = c$.
   Dowód:
   Niech b, c będą odwrotnościami a, zaś e będzie elementem neutralnym. Wtedy
   $$b = be = b(ac) = (ba)c = ec = c$$

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 tych liczb z $\{1, 2, \ldots, n\}$ które są względnie pierwsze z n, z mnożeniem $a * b = ab \mod n$.
    Ilość elementów grupy 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.

Dowód:
Własności 1, 2 i 4 grupy są spełnione, pozostaje wykazać własność 3, czyli istnienie elementu neutralnego.
Weźmy dowolny element $a \in H$. Wiemy, że $a^{-1} \in H$, a więc także $e = aa^{-1} \in H$.

2. **Twierdzenie (Lagrange)** *Jeżeli G jest grupą skończoną, zaś H jest podgrupą grupy G, to*

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

Dowód:

(a) Dla każdego $a \in G$ definiujemy zbiór

$$aH := \{ah \ \mid \ h \in H\}$$

(b) Rozważmy $a, b \in G$. Chcemy udowodnić, że

$$aH = bH \text{ albo } aH \cap bH = \emptyset$$

Załóżmy, że $aH \cap bH \neq \emptyset$, niech $c \in aH \cap bH$. Z definicji istnieją takie $h_1, h_2 \in H$, że

$$ah_1 = c = bh_2$$

Stąd $ah_1 = bh_2$, więc $a = ah_1h_1^{-1} = bh_2h_1^{-1} \in bH$.
Weźmy dowolny element aH. Ma on postać ah dla pewnego $h \in H$. Mamy

$$ah = (bh_2h_1^{-1})h = b(h_2h_1^{-1}h) \in bH$$

stąd $aH \subseteq bH$, analogicznie $bH \subseteq aH$, a więc $aH = bH$.

(c) Widzimy, że grupa G rozpada się na skończoną liczbę rozłącznych podzbiorów: $a_1H, \ldots, a_nH$. Jeżeli udowodnimy, że każdy z tych podzbiorów ma $|H|$ elementów, to teza będzie dowiedziona, gdyż

$$|G| = |a_1H| + \cdots + |a_nH| = n|H|$$

(d) Weźmy dowolny zbiór

$$aH = \{ah \ \mid \ h \in H\}$$

zbiór ten ma $|H|$, jeżeli elementy ah_1, ah_2 są różne dla różnych $h_1, h_2 \in H$. Załóżmy, że

$$ah_1 = ah_2 \text{ stąd } h_1 = a^{-1}ah_1 = a^{-1}ah_2 = h_2$$

dowód jest zakończony.

3. Dla danej grupy G i $a \in G$ zbiór postaci $\left\{1, a, a^2, \ldots, a^{\mathrm{ord}(a)-1}\right\}$ jest grupą; nazywamy go grupą generowaną przez a i oznaczamy $\langle a \rangle$. Grupa ta ma $\mathrm{ord}(a)$ elementów.
Dowód:

(a) Zauważmy, że dla wszystkich $k \in \mathbb{Z}$ zachodzi $a^k \in \langle a \rangle$.
Podzielmy z resztą; niech $q, r \in \mathbb{Z}$, $0 \leq r < \operatorname{ord}(a)$ będą takie, że $k = q \operatorname{ord}(a) + r$.

$$a^k = a^{q \operatorname{ord}(a) + r} = (a^{\operatorname{ord}(a)})^q a^r = 1^q a^r = a^r \in \langle a \rangle$$

gdyż $r \in \{0, 1, \ldots, \operatorname{ord}(a) - 1\}$.

(b) Uzasadnię na początek, że $\langle a \rangle$ jest grupą.
Korzystając z lematu wystarczy pokazać własności 1 i 4 grupy.
Niech $a^k, a^l \in \langle a \rangle$. Chcę pokazać, że $a^{k+l} \in \langle a \rangle$ oraz $a^{-k} \in \langle a \rangle$. To wynika wprost z poprzedniego podpunktu.

(c) Pozostaje uzasadnić, że elementy $1, a, \ldots, a^{\operatorname{ord}(a)-1}$ są parami różne.
Niech $a^k = a^l$ dla $\operatorname{ord}(a) > l > k$. Wtedy

$$1 = a^{-k} a^k = a^{-k} a^l = a^{l-k}$$

sprzeczność z definicją $\operatorname{ord}(a)$.

(d) Z powyższych rozważań wynika w szczególności, że

$$\langle a \rangle = \{\ldots, a^{-2}, a^{-1}, a^0, a, a^2, \ldots\}$$

z prawej strony niektóre elementy powtarzają się.

4. **Wniosek** *Jeżeli a jest elementem grupy skończonej G, to*

$$\operatorname{ord}(a, G) \mid |G|$$
$$a^{|G|} = 1 \text{ } \textit{w grupie } G$$

Dowód:

(a) *Warto przypomnieć definicję rzędu.*

(b) Wystarczy uzasadnić, że $\operatorname{ord}(a, G) \mid |G|$, gdyż wtedy $a^{|G|} = (a^{\operatorname{ord}(a)})^{\cdots} = 1^{\cdots} = 1$ w grupie G.

(c) Podzbiór

$$\langle a \rangle = \left\{1, a, \ldots, a^{\operatorname{ord}(a)-1}\right\}$$

jest podgrupą G, mającą $\operatorname{ord}(a)$ elementów. Podzielność z tezy wniosku wyniknie wprost z tw. Lagrange.

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

$$p | a^p - a$$

Dowód:
Przypadek $p|a$ jest banalny. Można uznać, że a względnie pierwsze z p. Z wniosku 4. zastosowanego do grupy $\{1, 2, \ldots, p-1\}$ z mnożeniem $\mod p$ otrzymujemy $p | a^{p-1} - 1$, a stąd tezę.

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

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

Dowód:
Zastosowanie wniosku 4. do grupy z 10. przykładu, warto zauważyć, że tw. Fermata jest szczególnym przypadkiem tego twierdzenia.

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

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

Dowód:
Bezpośrednie skorzystanie z wniosku dla grupy $\{1, 2, \ldots, p-1\}$ z mnożeniem $\mod p$.

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

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

   Dowód:

   (a) Niech $a, c \in G$, niech $d = NWD(\mathrm{ord}(a), \mathrm{ord}(c))$. Element c^d ma rząd $\frac{o(c)}{d}$ (sprawdź to!), więc $NWD(\mathrm{ord}(c^d), \mathrm{ord}(a)) = 1$ [tutaj kryje się nieścisłość, tak naprawdę można jedynie wziąć takie d_1, d_2, że $d_1 d_2 = d$ oraz $NWD(\mathrm{ord}(c^{d_1}), \mathrm{ord}(a^{d_2})) = 1$. Nie ma to wpływu na przebieg dowodu], $NWW(\mathrm{ord}(c^d), \mathrm{ord}(a)) = NWW(\mathrm{ord}(a), \mathrm{ord}(c))$.
   Oznaczam $b := c^d$. Udowodnię, że element ab ma szukany rząd $NWW(\mathrm{ord}(a), \mathrm{ord}(b))$.

   (b) Na początek udowodnię, że
   $$\langle a \rangle \cap \langle b \rangle = 1$$
   Niech $g \in \langle a \rangle \cap \langle b \rangle$. Z wniosku z tw. Lagrange
   $$\mathrm{ord}(g) \mid |\langle a \rangle| = \mathrm{ord}(a)$$
   $$\mathrm{ord}(g) \mid |\langle b \rangle| = \mathrm{ord}(b)$$
   a więc $\mathrm{ord}(g) \mid NWD(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$. Tym samym $g = g^1 = g^{\mathrm{ord}(g)} = 1$.
   Oczywiście $1 \in \langle a \rangle \cap \langle b \rangle$ (dlaczego?).

   (c) Niech dla zwięzłości $O := \mathrm{ord}(ab)$, więc $(ab)^O = 1$. Skoro grupa jest przemienna, to
   $$1 = (ab)^O = a^O b^O$$
   Popatrzmy na element a^O. $a^O \in \langle a \rangle$ oraz $a^O = (b^O)^{-1} = b^{-O} \in \langle b \rangle$. A więc
   $$a^O \in \langle a \rangle \cap \langle b \rangle \text{ stąd } a^O = 1 \text{ więc } \mathrm{ord}(a) \mid O$$
   Analogicznie $\mathrm{ord}(b) \mid O$, stąd
   $$NWW(\mathrm{ord}(a), \mathrm{ord}(b)) \mid O$$

   (d) Obliczam
   $$(ab)^{NWW(\mathrm{ord}(a),\mathrm{ord}(b))} = a^{NWW(\mathrm{ord}(a),\mathrm{ord}(b))} b^{NWW(\mathrm{ord}(a),\mathrm{ord}(b))} = 1 * 1 = 1$$
   stąd wynika $O = \mathrm{ord}(ab) \mid NWW(\mathrm{ord}(a), \mathrm{ord}(b))$, co w połączeniu z
   $$NWW(\mathrm{ord}(a), \mathrm{ord}(b)) \mid O$$
   daje $O = NWW(\mathrm{ord}(a), \mathrm{ord}(b))$, czyli tezę.

2. **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 $\{g, g^2, \ldots, g^{p-1}\}$ dają parami różne reszty z dzielenia przez p.*

   Dowód:

   (a) Grupa $G := \{1, 2, \ldots, p-1\}$ ma skończenie wiele elementów, weźmy element a największego rzędu M. Jeżeli udowodnimy, że $M = p - 1$, to grupa cykliczna $\langle a \rangle$ będzie miała $p - 1$ elementów, więc będzie równa grupie G.

(b) Weźmy dowolny element $b \in G$. Jeżeli $\mathrm{ord}(b) \not| \mathrm{ord}(a)$, to z lematu istnieje takie $g \in G$, że

$$\mathrm{ord}(g) = NWW(\mathrm{ord}(a), \mathrm{ord}(b)) > \mathrm{ord}(a)$$

sprzeczność z określeniem a jako elementu o największym rzędzie. Tak więc

$$\text{dla każdego } b \in G \ \mathrm{ord}(b) \mid \mathrm{ord}(a) = M$$

$$\text{dla każdego } b \in G \ b^M = 1.$$

(c) Chciałbym teraz zdefiniować, co to jest wielomian o współczynnikach w $\mathbb{Z}_p := \{0, 1, \ldots, p-1\}$. Niestety do tego potrzeba mi jeszcze trochę definicji.

(d) **Definicja** *Zbiór F z działaniami $+$ i $\cdot$ taki, że*

i. F jest grupą przemienną ze względu na działanie $+$. Będziemy oznaczać działanie tej grupy w konwencji dodawania, tj. element neutralny oznaczymy 0 itd.

ii. $F \setminus \{0\}$ jest grupą przemienną ze względu na $\cdot$.

iii. Zachodzą prawa rozdzielności:

$$a(b+c) = ab + ac$$

$$(b+c)a = ba + ca$$

nazywamy ***ciałem***.

Liczby rzeczywiste są ciałem, liczby wymierne są ciałem.

(e) **Lemat** *Dla dowolnej liczby pierwszej p zbiór*

$$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$$

z działaniami $+ \mod p$ i $\cdot \mod p$ jest ciałem.

Dowód:
Udowodniliśmy, że $\mathbb{Z}_p$ z działaniem $+$ jest grupą, oraz $\mathbb{Z}_p \setminus \{0\}$ z działaniem $\cdot \mod p$ jest grupą. Pozostaje przeliczyć prawa rozdzielności (a raczej jedno z nich, bo w przypadku przemiennym one są równoważne), czyli "udowodnić", że

$$a(b+c) \equiv ab + ac \mod p$$

co jest oczywiste.

(f) Tak jak rozważamy wielomiany o współczynnikach w $\mathbb{R}$ (niektórzy również $\mathbb{C}$), tak samo możemy rozważyć wielomiany o współczynnikach z dowolnego ciała, w szczególności z $\mathbb{Z}_p$.

(g) **Twierdzenie (Bézout)** *Jeżeli wielomian $P(x)$ o współczynnikach z ciała, spełnia równość $P(a) = 0$ dla elementu ciała a, to*

$$P(x) = (x-a)Q(x)$$

dla pewnego wielomianu $Q(x)$ o współczynnikach z ciała.

Dowód:
Identyczny jak w klasycznym twierdzeniu.

(h) **Wniosek (Langange)** *Wielomian $W(x)$ stopnia n może mieć co najwyżej n pierwiastków, licząc z krotnościami.*

Dowód:
Jest to wniosek z tw. Bèzout, dowód analogiczny jak dla wielomianów nad $\mathbb{R}$.

(i) **Dokończenie dowodu** Przypominam: $G = \{1, 2, \ldots, p-1\}$ i

$$\text{dla każdego } b \in G \ b^M = 1.$$

Wielomian $W(x) := x^M - 1$ o współczynnikach z ciała $\mathbb{Z}_p$ ma pierwiastki $1, 2, \ldots, p-1$. Z tw. Lagrange wynika, że

$$M = \deg W(x) \geq p - 1$$

Nierówność $\mathrm{ord}(a) = M \leq p-1$ wynika np. z tego, że $\mathrm{ord}(a) \mid p-1$. Otrzymaliśmy więc $M = p-1$ co było do udowodnienia.