Niezbyt formalny i niezbyt intuicyjny wstęp do algebry abstrakcyjnej

1. Nawiasami [[]] oznaczać będę komentarze.

2. **Definicja 0.1** ***Grupą*** *z [[jakimś abstrakcyjnym]] działaniem $\oplus$ nazywamy zbiór G spełniający warunki*

   (a) Dla wszystkich $a, b \in G$ jest $a \oplus b \in G$

   (b) Dla wszystkich $a, b, c \in G$ jest $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ [[czyli kolejność nie ma znaczenia]]

   (c) Istnieje specjalny element $e \in G$, taki, że $a \oplus e = e \oplus a = a$ dla wszystkich $a \in G$ [[element neutralny działania $\oplus$]] Element ten jest jedyny. Element ten będę dalej oznaczać przez 0_G.

   (d) Dla każdego $a \in G$ istnieje odwrotność elementu a, czyli taki element $b \in G$, że $a \oplus b = b \oplus a = 0_G$. [[gdzie 0_G jest tym elementem neutralnym]] . Ten element oznaczę przez $\ominus a$.

   (e) Jeżeli dodatkowo *zachodzi dla wszystkich $a, b \in G$ równość $a \oplus b = b \oplus a$, to grupę nazywamy* ***przemienną*** *[[tylko takimi się będziemy zajmować]]*

   Parę uwag:

   - W grupie jest dokładnie jeden element neutralny: Niech $e, f \in G$ będą elementami neutralnymi. Wtedy $e = ef = f$ [[Pierwsza równość z określenia f, druga z określenia e]] .
   - Dla każdego elementu $a \in G$ istnieje w grupie G dokładnie jeden element odwrotny do a: Niech $a \oplus b = b \oplus a = 0_G$ i $a \oplus c = c \oplus a = 0_G$ to $c = 0_G \oplus c = b \oplus a \oplus c = b \oplus 0_G = b$.
   - Elementem odwrotnym do 0_G jest 0_G. Ponadto $0_G \oplus 0_G = 0_G$.
   - Dalej będę dla uproszczenia pisać $a \ominus b$ zamiast $a \oplus (\ominus b)$. Oczywiście jeżeli $a, b \in G$, to $\ominus b \in G$, więc $a \ominus b = a \oplus (\ominus b) \in G$.

3. Przykłady grup przemiennych:

   - Liczby całkowite z dodawaniem - elementem neutralnym jest 0, a elementem odwrotnym do liczby a jest $-a$ bo $a + (-a) = 0$ i $(-a) + a = 0$.
   - Liczby wymierne bez 0 z mnożeniem - elementem neutralnym jest 1, a elementem odwrotnym do danej liczby jest $\frac{1}{a}$.
   - Liczby wymierne z dodawaniem.
   - Liczby rzeczywiste z dodawaniem.
   - Zbiór reszt z dzielenia przez n czyli zbiór $\{0, 1, 2, \cdots, n-1\}$ tworzy grupę ze względu na „dodawanie modulo n", czyli na działanie $a + b \mod n$. 0 jest elementem neutralnym, elementem przeciwnym do a jest element $n - a$, gdyż $a + (n - a) = n = 0 \mod n$. Grupę tę zwykle oznaczamy $\mathbb{Z}_n^+$.
   - Jeżeli p jest liczbą **pierwszą** to zbiór $\{1, 2, \cdots, p-1\}$ z „mnożeniem modulo p", czyli z działaniem $a \cdot b \mod p$. 1 jest elementem neutralnym. Grupę tę oznaczamy $\mathbb{Z}_p^*$.
     Aby wykazać, że istnieje odwrotność $a \in \{1, 2, \cdots, p-1\}$ weźmy zbiór liczb $\{0a \mod p, 1a \mod p, 2a \mod p, \cdots, (p-1)a \mod p\}$. Łatwo zauważyć, że $p | ka - la = (k-l)a$ tylko jeśli $k = l$ (bo a jest względnie pierwsze z p) a więc liczby $\{0a \mod p, 1a \mod p, 2a \mod p, \cdots, (p-1)a \mod p\}$ dają różne reszty z dzielenia przez p. Skoro reszt jest p i tych liczb jest p, to któraś z nich musi dawać resztę 1. Istnieje więc takie $b \in \{1, 2, \cdots, p-1\}$, że $ab = 1$. Liczba b jest odwrotnością a.

- Liczby dodatnie, względnie pierwsze z $n \in \mathbb{N}$ i mniejsze od n z działaniem $a \cdot b \mod n$. Dowodzimy podobnie jak w poprzednim przykładzie, lecz trzeba udowodnić też warunek a). Ilość elementów tej grupy, czyli ilość liczb względnie pierwszych z n i mniejszych od n oznaczamy przez $\phi(n)$.
- [[tylko na wszelki wypadek]] Liczby zespolone z dodawaniem i liczby zespolone bez 0 z mnożeniem.
- Liczby naturalne z dodawaniem **nie** są grupą, gdyż nie istnieje np. taka liczba dodatnia n, że $1 + n = 0$, czyli nie istnieje odwrotność 1.
- Liczby całkowite bez 0 z mnożeniem nie są grupą - nie ma liczby całkowitej k takiej, że $2k = 1$, czyli nie ma odwrotności 2.

Przykładem grupy, która jest nie przemienna są macierze odwracalne 2×2 z mnożeniem macierzy. [[Podkreślam, takimi przykładami nie będziemy się zajmować]] .

4. **Pytanie**: po co komplikować sobie życie, mówiąc, że „zwykłe" liczby całkowite tworzą jakąśtam grupę?
Chodzi o to, że jeżeli udowodnimy jakieś twierdzenie dla grup, to będziemy je mieli udowodnione dla wszystkich grup: będzie to jakieś twierdzenie dla liczb całkowitych, inne twierdzenie dla macierzy itd. Twierdzenia te mogą wydawać się bardzo różne i trudne do powiązania, jeżeli nie będziemy mówić o grupach.

5. **Definicja 0.2** *Powiemy, że H jest **podgrupą** G, jeżeli zbiór H jest zawarty w G: $H \subseteq G$ i H jest grupą ze względu na to samo działanie co G.*

   Lemat 0.3 *Do tego, żeby $H \subseteq G$, było podgrupą, gdy wiemy, że G jest grupą, wystarczy*

   $$a, b \in H \to a \oplus b \in H \text{ i } a \in H \to \ominus a \in H$$

   Faktycznie pierwszy i czwarty warunek definicji jest spełniony z założenia, drugi warunek jest spełniony dla G, a więc tym bardziej dla H. Ponadto jeżeli $a \in H$ i $\ominus a \in H$, to z $a, b \in H \to a \oplus b \in H$ otrzymuję, podstawiając $b = \ominus a$, $0_G = a + \ominus a \in H$. A więc każda podgrupa zawiera element neutralny grupy i jest on elementem neutralnym podgrupy!
   Ponadto jeżeli G jest przemienna to i H jest przemienna.

6. Pierwsze koty za płoty, czyli pierwsze twierdzenie w teorii grup.

   Twierdzenie 0.4 (Twierdzenie Lagrange) *Jeżeli H jest podgrupą grupy G, która ma skończenie wiele elementów, to $|H|$ dzieli $|G|$, gdzie $|X|$ oznacza ilość elementów zbioru X.*

   Dowód: Zdefiniujmy sobie relację $\sim$ pomiędzy elementami grupy G: niech $a \sim b$ oznacza, że $a \ominus b \in H$ [[z definicji G dla każdych elementów $a, b \in G$ jest $a \ominus b \in G$, ale wcale nie musi być $a \ominus b \in H$!]] . Relacja $\sim$ spełnia warunki:

   - $a \sim a$, gdyż $a \ominus a = 0_G \in H$
   - $a \sim b \to b \sim a$. Jeżeli $a \ominus b \in H$, to z definicji grupy $\ominus(a \ominus b) \in H$, a $\ominus(a \ominus b) = b \ominus a$, czyli $b \ominus a \in H$, a więc z definicji $\sim$ jest $b \sim a$.
   - $a \sim b \wedge b \sim c \to a \sim c$. Jeżeli $a \ominus b \in H$ i $b \ominus c \in H$, to $(a \ominus b) \oplus (b \ominus c) \in H$, a $(a \ominus b) \oplus (b \ominus c) = a \ominus c$, więc $a \ominus c \in H$, czyli $a \sim c$.

   Relacja $\sim$ rozbija G na pewną ilość podzbiorów, których elementy pozostają ze sobą w relacji np. Niech G będzie grupą $\{0, 1, 2, \cdots, 7\}$ z dodawaniem modulo 8, a $H = \{0, 2, 4, 6\}$ z tym samym działaniem. Wtedy H jest podgrupą G. Relacja określona wyżej rozbija G na 2 zbiory:

   $$\{0, 2, 4, 6\} \text{ i } \{1, 3, 5, 7\}$$

   Wracajac do przypadku ogólnego, niech relacja $\sim$ rozbija G na podzbiory $A_1, A_2, \cdots, A_m$, których elementy pozostają ze sobą w relacji $\sim$.

Jeżeli udowodniłbym, że dowolny podzbiór A_k ma tyle samo elementów co H, to z tego wynikałoby, że

$$|G| = |A_1| + |A_2| + \cdots + |A_m| = |H| + |H| + \cdots + |H| = m|H|$$

czyli teza.
Pozostaje udowodnić, że $|A_i| = |H|$ dla dowolnego i. Niech $a \in A_i$. Rozważmy zbiór

$$B = \{a \oplus h_1, a \oplus h_2, a \oplus h_3 \cdots, a \oplus h_k\}$$

gdzie $h_1, h_2, \cdots, h_k$ to **wszystkie** elementy H. Zauważmy, że zbiór B ma $|H|$ elementów.
Zauważmy, że $a \ominus (a \oplus h_i) = h_i \in H$, czyli element a jest w relacji $\sim$ ze wszystkimi elementami zbioru B, a więc $B \subseteq A_i$, gdyż A_i był zbiorem elementów będących w relacji $\sim$ z a.
Z drugiej strony, jeżeli $a \sim b$ to $a \ominus b \in H$, czyli $a \ominus b = h$ (gdzie $h \in H$), czyli $b = a \ominus h = a \oplus (\ominus h)$. Element $\ominus h$ należy do H, a więc b można zapisać w postaci $a \oplus$ element z H , więc $b \in B$. b było wybrane dowolnie, więc każdy element pozostający w relacji $\sim$ z a należy do B! Stąd wynika $A_i \subseteq B$ a wcześniej było $B \subseteq A_i$ więc $B = A_i$ i $|H| = |B| = |A_i|$. To kończy dowód.

7. Zastosowania twierdzenia Lagrange'a:

   (a) Niech G będzie skończoną grupą i $a \in G$. Niech $\sigma(a)$ będzie najmniejszą liczbą dodatnią, taką, że

   $$\underbrace{a \oplus a \oplus \cdots \oplus a}_{\sigma(a)} = 0_G$$

   [[Taka liczba istnieje, dowód korzysta z metody szufladkowej Dirichleta]] Można udowodnić, że $\{0_G, a, a+a, \cdots, \underbrace{a \oplus a \oplus \cdots \oplus a}_{\sigma(a)-1}\}$ to podgrupa G i podgrupa ta ma $\sigma(a)$ elementów [[dla $k > l$ równość $\underbrace{a \oplus a \oplus \cdots \oplus a}_{k} = \underbrace{a \oplus a \oplus \cdots \oplus a}_{l}$ implikuje $\underbrace{a \oplus a \oplus \cdots \oplus a}_{k-l} = 0_G$, a dla $k, l < \sigma(a)$ równość ta nie może zajść, więc elementy są różne]] . Z twierdzenia Lagrange wynika

   $$\sigma(a) \mid |G|$$

   Wynika stąd:

   $$\underbrace{a \oplus a \oplus \cdots \oplus a}_{|G|} = \underbrace{(\underbrace{a \oplus a \oplus \cdots \oplus a}_{\sigma(a)}) \oplus (\underbrace{a \oplus a \oplus \cdots \oplus a}_{\sigma(a)}) \oplus \cdots \oplus (\underbrace{a \oplus a \oplus \cdots \oplus a}_{\sigma(a)})}_{k} =$$

   $$\underbrace{0_G \oplus 0_G \oplus \cdots \oplus 0_G}_{k} = 0_G$$

   gdzie $k = \frac{|G|}{\sigma(a)}$. Liczbę $\sigma(a)$ nazywamy **rzędem** elementu a.

   (b) **Twierdzenie 0.5 (Małe twierdzenie Fermata)** *Jeżeli p jest liczbą pierwszą i a jest względnie pierwsze z p, to*

   $$p | a^{p-1} - 1$$

   Rozważamy podzielność przez p, więc można założyć $a \in \{1, 2, \cdots, p-1\}$. Wiemy, że $\{1, 2, \cdots, p-1\}$ tworzą grupę ze względu na mnożenie modulo p. Korzystam z pierwszego wniosku: $\underbrace{a \oplus a \oplus \cdots \oplus a}_{|G|}$ i zamieniam abstrakcyjne $\oplus$ na działanie $a \cdot b \mod p$ i podstawiam $|G| = p - 1$:

   $$a^{p-1} = 1 \mod p$$

   (c) **Twierdzenie 0.6 (Twierdzenie Eulera)** *Jeżeli a jest względnie pierwsze z n, to*

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

   gdzie $\phi(n)$ to ilość liczb względnie pierwszych z n i mniejszych od n.
   Dowód jest analogiczny jak wyżej dla grupy elementów względnie pierwszych z n i mniejszych od n.

8. [[Dowód istnienia generatora]]

Twierdzenie 0.7 *W grupie* $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$ *z działaniem* $a \cdot b \mod p$ *istnieje element* g *taki, że*

$$\{g, g^2, g^3, \cdots, g^{p-1}\} = \{1, 2, \cdots, p-1\} \mod p$$

(a) **Dowód**: Skoro dla dowolnego b, elementy

$$\{0_{\mathbb{Z}_p^*}, b, b \oplus b, \cdots, \underbrace{b \oplus b \oplus \cdots \oplus b}_{\sigma(b)-1}\}$$

tworzą podgrupę $\mathbb{Z}_p^*$ mającą $\sigma(b)$ elementów, to wystarczy udowodnić, że istnieje element, którego rząd to $p-1$.
Niech a oznacza element, którego rząd $\sigma(a)$ jest maksymalny i niech b oznacza dowolny inny element.

(b) Udowodnię, że

$$\sigma(b) | \sigma(a)$$

Jeżeli $\sigma(b) \not| \sigma(a)$ to znaczy, że istnieje taka liczba pierwsza q, że

$$\sigma(b) = q^x \cdot r$$

$$\sigma(a) = q^y \cdot s$$

gdzie $x > y$, $q \not| r$ i $q \not| s$ [[Wynika z to rozkładu na czynniki pierwsze, chwila zastanowienia jest potrzebna, żeby to zobaczyć]] .

(c) Niech

$$a' = \underbrace{a \oplus a \oplus \cdots \oplus a}_{q^y}$$

$$b' = \underbrace{b \oplus b \oplus \cdots \oplus b}_{r}$$

$$A' := \{0_{\mathbb{Z}_p^*}, a', a' \oplus a', \cdots, \underbrace{a' \oplus a' \oplus \cdots \oplus a'}_{\sigma(a')-1}\}$$

$$B' := \{0_{\mathbb{Z}_p^*}, b', b' \oplus b', \cdots, \underbrace{b' \oplus b' \oplus \cdots \oplus b'}_{\sigma(b')-1}\}$$

Jest $|A'| = \sigma(a') = s$ i $|B'| = \sigma(b') = q^x$ [[rząd a' jest związany z rzędem a, gdyż a' jest „wielokrotnością" a]] .

(d) Niech $x \in A'$ i $x \in B'$. Z twierdzenia Lagrange $\sigma(x) \mid |A'| = s$ i $\sigma(x) \mid |B'| = q^x$. Ale liczby s, q^x są względnie pierwsze, więc ich jedyny wspólny dzielnik to 1. Stąd $\sigma(x) = 1$, a więc $x = 0_{\mathbb{Z}_p^*}$. Jedynym elementem wspólnym A' i B' jest więc element neutralny.

(e) Rozważmy element $a' \oplus b'$.
Jest

$$0_{\mathbb{Z}_p^*} = \underbrace{a' \oplus b' \oplus a' \oplus b' \oplus \cdots \oplus a' \oplus b'}_{\sigma(a'b')}$$

Wynika stąd w szczególności, że

$$\underbrace{b' \oplus b' \oplus \cdots \oplus b'}_{\sigma(a'b')} = \ominus \underbrace{a' \oplus a' \oplus \cdots \oplus a'}_{\sigma(a'b')} \in A$$

$$\underbrace{b' \oplus b' \oplus \cdots \oplus b'}_{\sigma(a'b')} \in B$$

więc $\underbrace{b' \oplus b' \oplus \cdots \oplus b'}_{\sigma(a'b')} = 0_{\mathbb{Z}_p^*}$ i $q^x = \sigma(b') \mid \sigma(a'b')$. Analogicznie $s = \sigma(a') \mid \sigma(a'b')$, a skoro s, q^x są względnie pierwsze, to

$$sq^x \mid \sigma(a'b')$$

Stąd wynika, że $\sigma(a) < sq^x \leq \sigma(a'b')$, czyli rząd $a'b'$ jest większy niż rząd a, wbrew określeniu a. Sprzeczność.
Wiemy więc, że dla każdego $b \in \mathbb{Z}_p^*$ jest

$$\sigma(b)|\sigma(a)$$

(f) Rozważmy wielomiany o współczynnikach z $\mathbb{Z}_p^*$ na których wszystkie działania wykonywane są mod p. Dla takich wielomianów działa schemat Hornera i w związku z tym działa twierdzenie Bezout. W szczególności, każdy wielomian może mieć najwyżej tyle pierwiatków, ile wynosi jego stopień. [[To się może wydać podejrzane, ale dowód jest długi i po prostu definiuje ponownie schemat Hornera]]
Z poprzedniej części wiemy, że wielomian $x^n - 1$ gdzie $n = \sigma(a)$ było zdefiniowane wyżej, ma jako pierwiastki wszystkie liczby z $\{1, 2, \cdots, p-1\}$, gdyż dla każdego elementu $b \in \{1, 2, \cdots, p-1\}$ jest

$$b^{\sigma(a)} - 1 = (b^{\sigma(b)})^k - 1 = 1^k - 1 = 0 \mod p$$

gdzie $k = \frac{\sigma(a)}{\sigma(b)}$ jest liczbą całkowitą.
Skoro tak, to znaczy, że stopień wielomianu $x^n - 1$ jest niemniejszy niż $p-1$. Stopień ten jest równy $n = \sigma(a)$, czyli $\sigma(a) \geq p-1$. Z tw. Lagrange $\sigma(a)|p-1$, więc $\sigma(a) \leq p-1$. Ostatecznie $\sigma(a) = p-1$ i a jest szukanym generatorem.

9. To jest 1. część skryptu. Podkreślam, że skrypt ten jest niezbyt użyteczny na poziomie szkolnym i dlatego nie należy się denerwować, jeżeli po paru przeczytaniach nadal mało się rozumie. Jeżeli pojawią się głosy zachęty, może być stworzona 2. część skryptu o ciałach: dowód, że ciało ma p^n elementów, przykłady ciał mających p^2, p^3 elementów i inne.