** **
Teoria w PDF (dość brzydko spisana).

Źródło w texu.

documentclass[10pt]{article} usepackage{amssymb} usepackage{amsmath} textwidth 16cm textheight 24cm oddsidemargin 0cm topmargin 0pt headheight 0pt headsep 0pt usepackage[polish]{babel} usepackage[utf8]{inputenc} usepackage[T1]{fontenc} %usepackage{MnSymbol} % --- vfuzz4pt % Don't report over-full v-boxes if over-edge is small hfuzz4pt % Don't report over-full h-boxes if over-edge is small % THEOREMS -- newtheorem{thm}{Twierdzenie}[section] newtheorem{cor}[thm]{Wniosek} newtheorem{lem}[thm]{Lemat} newtheorem{defn}[thm]{Definicja} newtheorem{tozs}[thm]{Tożsamość} newtheorem{hyp}[thm]{Hipoteza} newtheorem{useless}[thm]{} begin{document} defrozw{\ textbf{Rozwiązanie}: \} defcomm#1{ [[#1]] } defdeg{^{oplus}} title{Niezbyt formalny i niezbyt intuicyjny wstęp do algebry abstrakcyjnej} date{} maketitle begin{enumerate} item Nawiasami comm{} oznaczać będę komentarze. item begin{defn} textbf{Grupą} z comm{jakimś abstrakcyjnym} działaniem $oplus$ nazywamy zbiór G spełniający warunki begin{enumerate} item Dla wszystkich $a,bin G$ jest $aoplus bin G$ item Dla wszystkich $a,b,cin G$ jest $(aoplus b)oplus c = aoplus(boplus c)$ comm{czyli kolejność nie ma znaczenia} item Istnieje specjalny element $ein G$, taki, że $aoplus e = eoplus a = a$ dla wszystkich $ain G$ comm{element neutralny działania $oplus$} Element ten jest jedyny. Element ten będę dalej oznaczać przez 0_G. item Dla każdego $ain G$ istnieje odwrotność elementu a, czyli taki element $bin G$, że $aoplus b= boplus a =0_G$. comm{gdzie 0_G jest tym elementem neutralnym}. Ten element oznaczę przez $ominus a$. item Jeżeli emph{dodatkowo} zachodzi dla wszystkich $a,bin G$ równość $aoplus b = boplus a$, to grupę nazywamy textbf{przemienną} comm{tylko takimi się będziemy zajmować} end{enumerate}end{defn} Parę uwag: begin{itemize} item W grupie jest dokładnie jeden element neutralny: Niech $e,fin G$ będą elementami neutralnymi. Wtedy $e = ef = f$ comm{Pierwsza równość z określenia f, druga z określenia e}. item Dla każdego elementu $ain G$ istnieje w grupie G dokładnie jeden element odwrotny do a: Niech

$aoplus b = boplus a = 0_G$ i $aoplus c = coplus a = 0_G$ to $c = 0_Goplus c = boplus aoplus c = b oplus 0_G = b$. item Elementem odwrotnym do 0_G jest 0_G. Ponadto $0_Goplus 0_G = 0_G$. item Dalej będę dla uproszczenia pisać $aominus b$ zamiast $aoplus (ominus b)$. Oczywiście jeżeli $a,bin G$, to $ominus bin G$, więc $aominus b = aoplus(ominus b)in G$. end{itemize} item Przykłady grup przemiennych: begin{itemize} item Liczby całkowite z dodawaniem - elementem neutralnym jest 0, a elementem odwrotnym do liczby a jest $-a$ bo $a+(-a) = 0$ i $(-a) + a =0$. item Liczby wymierne bez 0 z mnożeniem - elementem neutralnym jest 1, a elementem odwrotnym do danej liczby jest $frac{1}{a}$. item Liczby wymierne z dodawaniem. item Liczby rzeczywiste z dodawaniem. item 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 $mathbb{Z}_n^+$. item Jeżeli p jest liczbą textbf{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 $ain {1,2,cdots,p-1}$ weźmy zbiór liczb ${0a mod p,1a mod p,2a mod p,cdots,(p-1)amod p}$. Łatwo zauważyć, że $p|ka - la = (k-l)a$ tylko jeśli $k=l$ (bo a jest względnie pierwsze z p) a więc liczby ${0a mod p, 1a mod p,2a mod p,cdots,(p-1)amod p}$ 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 $bin {1,2,cdots,p-1}$, że $ab = 1$. Liczba b jest odwrotnością a. item Liczby dodatnie, względnie pierwsze z $nin mathbb{N}$ 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 $phi(n)$. item comm{tylko na wszelki wypadek} Liczby zespolone z dodawaniem i liczby zespolone bez 0 z mnożeniem. item Liczby naturalne z dodawaniem textbf{nie} są grupą, gdyż nie istnieje np. taka liczba dodatnia n, że $1+n=0$, czyli nie istnieje odwrotność 1. item Liczby całkowite bez 0 z mnożeniem nie są grupą - nie ma liczby całkowitej k takiej, że $2k=1$, czyli nie ma odwrotności 2. end{itemize} Przykładem grupy, która jest nie przemienna są macierze odwracalne $2times 2$ z mnożeniem macierzy. comm{Podkreślam, takimi przykładami nie będziemy się zajmować}. item textbf{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. item begin{defn} Powiemy, że H jest textbf{podgrupą} G, jeżeli zbiór H jest zawarty w G: $Hsubseteq G$ i H jest grupą ze względu na to samo działanie co G. end{defn} begin{lem}Do tego, żeby $Hsubseteq G$, było podgrupą, gdy wiemy, że G jest grupą, wystarczy $$a,bin Hrightarrow aoplus bin H hbox{ i } ain Hrightarrow ominus ain H$$ end{lem} Faktycznie pierwszy i czwarty warunek definicji jest spełniony z założenia, drugi warunek jest spełniony dla G, a więc tym bardziej dla H. Ponadto jeżeli $ain H$ i $ominus ain H$, to z $a,bin Hrightarrow aoplus bin H$ otrzymuję, podstawiając $b=ominus a$, $0_G = a + ominus ain H$. A więc każda podgrupa zawiera element neutralny grupy i jest on elementem neutralnym podgrupy!\ Ponadto jeżeli G jest przemienna to i H jest przemienna. item Pierwsze koty za płoty, czyli pierwsze twierdzenie w teorii grup. begin{thm}[Twierdzenie Lagrange] Jeżeli H jest podgrupą grupy G, która ma skończenie wiele elementów, to $|H|$ dzieli $|G|$, gdzie $|X|$ oznacza ilość

elementów zbioru X.end{thm} textbf{Dowód}: Zdefiniujmy sobie relację sim pomiędzy elementami grupy G: niech $asim b$ oznacza, że $aominus bin H$ comm{z definicji G dla każdych elementów $a,bin G$ jest $aominus bin G$, ale wcale nie musi być $aominus bin H$!}. Relacja sim spełnia warunki: begin{itemize} item $asim a$, gdyż $aominus a=0_Gin H$ item $asim brightarrow bsim a$. Jeżeli $aominus bin H$, to z definicji grupy $ominus(aominus b)in H$, a $ominus(aominus b) = b ominus a$, czyli $ b ominus ain H$, a więc z definicji sim jest $bsim a$. item $asim bwedge bsim crightarrow asim c$. Jeżeli $aominus bin H$ i $bominus cin H$, to $(aominus b)oplus (bominus c)in H$, a $(aominus b)oplus (bominus c) = aominus c$, więc $aominus cin H$, czyli $asim c$. end{itemize} 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: $${0,2,4,6} hbox{ i } {1,3,5,7}$$ 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.\ % Zauważmy, że jednym z tych podzbiorów jest H. Faktycznie, jeżeli weźmiemy dowolny element $hin H$, to $hominus cin H$ implikuje $c = hominus (hominus c)in H$ i jeżeli $h_1in H$, to oczywiście $hominus h_1in H$, więc $hsim h_1$, czyli h pozostaje w relacji tylko i wyłącznie ze wszystkimi elementami H. Tak więc pewien podzbiór A_i, zawierający h, jest równy H.\ 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 $ain A_i$. Rozważmy zbiór $$B = {aoplus h_1,aoplus h_2,aoplus h_3cdots,aoplus h_k}$$ gdzie $h_1,h_2,cdots,h_k$ to textbf{wszystkie} elementy H. Zauważmy, że zbiór B ma $|H|$ elementów.\ Zauważmy, że $aominus (a oplus h_i) = h_iin H$, czyli element a jest w relacji sim ze wszystkimi elementami zbioru B, a więc $Bsubseteq A_i$, gdyż A_i był zbiorem elementów będących w relacji sim z a.\ Z drugiej strony, jeżeli $asim b$ to $aominus bin H$, czyli $aominus b = h$ (gdzie $hin H$), czyli $b = aominus h = aoplus (ominus h)$. Element $ominus h$ należy do H, a więc b można zapisać w postaci $aoplus hbox{ element z }Hhbox{ }$, więc $bin B$. b było wybrane dowolnie, więc każdy element pozostający w relacji sim z a należy do B! Stąd wynika $A_isubseteq B$ a wcześniej było $Bsubseteq A_i$ więc $B = A_i$ i $|H| = |B| = |A_i|$. To kończy dowód. item Zastosowania twierdzenia Lagrange'a: begin{enumerate} item Niech G będzie skończoną grupą i $ain G$. Niech $sigma(a)$ będzie najmniejszą liczbą dodatnią, taką, że $$underbrace{aoplus aopluscdotsoplus a}_{sigma(a)}=0_G$$ comm{Taka liczba istnieje, dowód korzysta z metody szufladkowej Dirichleta} Można udowodnić, że ${0_G,a,a+a,cdots, underbrace{aoplus aopluscdotsoplus a}_{sigma(a)-1}}$ to podgrupa G i podgrupa ta ma $sigma(a)$ elementów comm{dla $k>l$ równość $underbrace{aoplus aoplus cdotsoplus a}_k = underbrace{aoplus aoplus cdotsoplus a}_l$ implikuje $underbrace{aoplus aoplus cdotsoplus a}_{k-l} = 0_G$, a dla k,ly, $qnot |r$ i $qnot |s$ comm{Wynika z to rozkładu na czynniki pierwsze, chwila zastanowienia jest potrzebna, żeby to zobaczyć}. item Niech $$a'=underbrace{aoplus aoplus cdotsoplus a}_{q^y}$$ $$b'=underbrace{boplus boplus cdotsoplus b}_r$$ $$A':={0_{mathbb{Z}_p^*},a',a'oplus a',cdots,underbrace{a'oplus a'oplus cdotsoplus a'}_{sigma(a')-1}}$$ $$B':={0_{mathbb{Z}_p^*},b',b'oplus b',cdots,underbrace{b'oplus b'oplus cdotsoplus b'}_{sigma(b')-1}}$$ Jest $|A'| = sigma(a')=s$ i $|B'| = sigma(b')=q^x$ comm{rząd a' jest związany z rzędem a, gdyż a' jest ,,wielokrotnością'' a}. item Niech $xin A'$ i $xin B'$. Z twierdzenia Lagrange $sigma(x) | |A'|=s$ i $sigma(x) | |B'|=q^x$. 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. item Rozważmy element $a'oplus b'$.\ Jest $$0_{mathbb{Z}_p^*}=underbrace{a'oplus b'oplus a'oplus b'oplus cdotsoplus a'oplus b'}_{sigma(a'b')}$$ Wynika stąd w szczególności, że $$underbrace{b'oplus b'oplus cdotsoplus b'}_{sigma(a'b')} = ominusunderbrace{a'oplus a'oplus cdotsoplus a'}_{sigma(a'b')}in A$$ $$underbrace{b'oplus b'oplus cdotsoplus b'}_{sigma(a'b')}in B$$ więc $underbrace{b'oplus b'oplus cdotsoplus b'}_{sigma(a'b')} = 0_{mathbb{Z}_p^*}$ i $q^x=sigma(b') | sigma(a'b')$. Analogicznie $s=sigma(a') | sigma(a'b')$, a skoro s,q^x są względnie pierwsze, to $$sq^x | sigma(a'b')$$ 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 $bin mathbb{Z}_p^*$ jest $$sigma(b) | sigma(a)$$ item 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.comm{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 $bin {1,2,cdots,p-1}$ 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. end{enumerate} item 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. end{enumerate} end{document}