** **
Zadania PDF.

** **
Skrypt z dowodami PDF.

Źródło skryptu w texu.

% File: grupy.tex % Created: nie lut 28 08:00 2010 C % Last Change: nie lut 28 08:00 2010 C % 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} usepackage{import} % ---------- 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]{} %newenvironment{proof}{noindenttextsc{Proof.}} {nolinebreak[4]hfill$blacksquare$\par} % fontsf=cmss10 overfullrule0pt defVrule{smash{vrule height7pt depthbaselineskip}}

defVarule{smash{vrule height7pt depth3pt}} defHrule #1{Squeezemultispan#1hrulefill} defCompressMatrices{ifmmode defquad{hskip.5emrelax}fi} defSqueeze{noalign{vskip-.5baselineskip}} defrk{operatorname {rank}} deflin{operatorname {lin}} defdim{operatorname{dim}} defker{operatorname{ker}} defdet{operatorname{det}} defim{operatorname{im}} defid{operatorname{id}} defRe{operatorname{Re}} defIm{operatorname{Im}} defdist{operatorname{dist}} defAbs #1{leftvert #1rightvert} defNorm #1{leftVert #1rightVert} defcc #1{overline{#1}} defip#1#2{langle #1,#2 rangle} defdist{operatorname{dist}} defideal{Ihd} deflideal{ k$. Wtedy $$1 = a^{-k}a^k = a^{-k}a^l = a^{l-k}$$ sprzeczność z definicją $o(a)$. end{enumerate} item begin{cor} Jeżeli a jest elementem grupy skończonej G, to $$o(a, G) | |G|$$ $$a^{|G|} = 1 hbox{ w grupie G}$$ end{cor} dowod begin{enumerate} item emph{Warto przypomnieć definicję rzędu}. item Wystarczy uzasadnić, że $o(a, G) | |G|$, gdyż wtedy $a^{|G|} = (a^{o(a)})^{dots} = 1^{dots} = 1$ w grupie G. item Podzbiór $$gen{a} = left{ 1,a,dots,a^{o(a)-1} right}$$ jest podgrupą G, mającą $o(a)$ elementów. Podzielność z tezy wniosku wyniknie wprost z tw. Lagrange. end{enumerate} item begin{cor}[Fermat] Jeżeli p jest liczbą pierwszą zaś a jest całkowite dodatnie, to $$p | a^p - a$$ end{cor} dowod Przypadek $p|a$ jest banalny. Można uznać, że a względnie pierwsze z p. Z powyższego wniosku otrzymujemy $p | a^{p-1} - 1$, a stąd tezę. item begin{cor}[Euler] Jeżeli liczby naturalne n, a są względnie pierwsze, to $$n | a^{varphi(n)} - 1$$ end{cor} dowod Zastosowanie wniosku do grupy liczb z $left{ 1,2,dots, n right}$ względnie pierwszych z n (trzeba udowodnić, że tworzą one grupę!). $varphi(n)$ jest zdefiniowane wyżej. item begin{cor}[Lemat o rzędzie (słabsza forma)] Jeżeli p jest liczbą pierwszą, zaś a jest liczbą całkowitą względnie pierwszą z p oraz $o(a, p)$ oznacza rząd a względem p (patrz kółko o rzędzie, definicja jest zgodna z powyższą) to $$o(a, p) | p-1$$ end{cor} dowod Bezpośrednie skorzystanie z wniosku dla grupy $left{ 1,2, dots, p-1 right}$ z mnożeniem $mod p$. end{enumerate} paragraph{Trochę teorii z * (dużo * na tym kółku :)} begin{enumerate} item begin{lem} Jeżeli grupa G jest skończona i przemienna, to dla dowolnych elementów $a, bin G$ w grupie G istnieje element mający rząd $NWW(o(a), o(b))$. end{lem} dowod begin{enumerate} item Niech $a, cin G$, niech $d = NWD(o(a),o(c))$. Element c^d ma rząd $frac{o(c)}{d}$ (sprawdź to!), więc $NWD(o(c^d), o(a)) = 1$, $NWW(o(c^d), o(a)) = NWW(o(a), o(c))$.\ Oznaczam $b:=c^d$. Udowodnię, że element ab ma szukany rząd $NWW(o(a), o(b))$. item Na początek udowodnię, że $$gen{a} cap gen{b} = 1$$ Niech $gin gen{a} cap gen{b}$. Z wniosku z tw. Lagrange $$o(g) | |gen{a}| = o(a)$$ $$o(g) | |gen{b}| = o(b)$$ a więc $o(g) | NWD(o(a), o(b)) = 1$. Tym samym $g = g^1 = g^{o(g)} = 1$.\ Oczywiście $1in gen{a} cap gen{b}$ (dlaczego?). item Niech dla zwięzłości $O := o(ab)$, więc $(ab)^O = 1$. Skoro grupa jest przemienna, to $$1 = (ab)^O = a^Ob^O$$ Popatrzmy na element a^O. $a^Oin gen{a}$ oraz $a^O = (b^{O})^{-1} = b^{-O} in gen{b}$. A

więc $$a^Oin gen{a}capgen{b} hbox{ stąd } a^O = 1 hbox{ więc } o(a) | O$$ Analogicznie $o(b) | O$, stąd $$NWW(o(a), o(b)) | O$$ item Obliczam $$(ab)^{NWW(o(a),o(b))} = a^{NWW(o(a),o(b)}b^{NWW(o(a),o(b)} = 1ast 1 = 1$$ stąd wynika $O = o(ab) | NWW(o(a),o(b))$, co w połączeniu z $$NWW(o(a), o(b)) | O$$ daje $O = NWW(o(a), o(b))$, czyli tezę. end{enumerate} item begin{thm}[Istnienie generatora] Jeżeli p jest liczbą pierwszą, to grupa $$left{ 1,2,dots, p-1 right}$$ z mnożeniem $mod p$ jest grupą generowaną przez pewien element g, innymi słowy istnieje takie g, że liczby $left{ g,g^2,dots, g^{p-1} right}$ dają parami różne reszty z dzielenia przez p. end{thm} dowod begin{enumerate} item Grupa $G:=left{ 1,2,dots,p-1 right}$ ma skończenie wiele elementów, weźmy element a największego rzędu M. Jeżeli udowodnimy, że $M = p-1$, to grupa cykliczna $gen{a}$ będzie miała $p-1$ elementów, więc będzie równa grupie G. item Weźmy dowolny element $bin G$. Jeżeli $o(b) not| o(a)$, to z lematu istnieje takie $gin G$, że $$o(g) = NWW(o(a), o(b)) > o(a)$$ sprzeczność z określeniem a jako elementu o największym rzędzie. Tak więc $$hbox{ dla każdego }bin G o(b) | o(a)=M$$ $$hbox{ dla każdego }bin G b^M = 1.$$ item Chciałbym teraz zdefiniować, co to jest wielomian o współczynnikach w $mathbb{Z}_p := left{ 0, 1, dots, p-1 right}$. Niestety do tego potrzeba mi jeszcze trochę definicji.\ item begin{defn} Zbiór F z działaniami $+$ i $cdot$ taki, że begin{enumerate} item F jest grupą przemienną ze względu na działanie $+$. Będziemy oznaczać działanie tej grupy w konwencji dodawania, tj. element neutralny oznaczymy 0 itd. item $Fbackslashleft{ 0 right}$ jest grupą przemienną ze względu na $cdot$. item Zachodzą prawa rozdzielności: $$a(b+c) = ab+ac$$ $$(b+c)a = ba+ca$$ end{enumerate} nazywamy textbf{ciałem}. end{defn} Liczby rzeczywiste są ciałem, liczby wymierne są ciałem. item begin{lem} Dla dowolnej liczby pierwszej p zbiór $$mathbb{Z}_p = left{ 0, 1, dots, p-1 right}$$ z działaniami $+ mod p$ i $cdot mod p$ jest ciałem. end{lem} dowod Udowodniliśmy, że $mathbb{Z}_p$ z działaniem $+$ jest grupą, oraz $mathbb{Z}_pbackslashleft{ 0 right}$ 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. item 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 $mathbb{Z}_p$. item begin{thm}[B'ezout] 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. end{thm} dowod Identyczny jak w klasycznym twierdzeniu.

item begin{cor}[Langange] Wielomian $W(x)$ stopnia n może mieć co najwyżej n pierwiastków, licząc z krotnościami. end{cor} dowod Jest to wniosek z tw. B`ezout, dowód analogiczny jak dla wielomianów nad $mathbb{R}$. item textbf{Dokończenie dowodu} Przypominam: $G = left{ 1,2,dots, p-1 right}$ i $$hbox{ dla każdego }bin G b^M = 1.$$ Wielomian $W(x):=x^M -1$ o współczynnikach z ciała $mathbb{Z}_p$ ma pierwiastki $1, 2, dots, p-1$. Z tw. Lagrange wynika, że $$M =operatorname{deg} W(x) geq p-1$$ co było do udowodnienia. end{enumerate} end{enumerate} end{document}