УДК 512.542

Коновалов О.Б., Пилявська О.С., Шатохіна Ю.В.

Дослідження властивостей циклічних підгруп 2-груп малих порядків за допомогою системи комп'ютерної алгебри GAP.

Розглядається наступна задача: «Нехай p-група G задовольняє умові: якщо Z - циклічна підгрупа групи G, то або $Z \le Z(G)$, *або* $Z \cap Z(G) = \{1\}$. *Класифікувати всі такі групи». Раніше Пилявська і Шатохіна довели, що регулярні p-групи, що задовольняють вказаній умові вичерпуються абелевими группами та группами експоненти p. В даній роботі ми розглядаємо неабелеві 2-групи як мінімальний приклад нерегулярних груп і досліджуємо їх за допомогою системи комп'ютерної алгебри GAP. Одержано: 1) кожна група, порядок якої менший за* 2^7, *має циклічну підгрупу, що не міститься в центрі і має з ним нетривіальний перетин; 2) існують дві групи порядку* 2^7 *і вісім груп порядку* 2^8, *у яких кожна циклічна підгрупа або міститься в центрі або має з ним нетривіальний перетин. Вказано задання знайдених груп за допомогою твірних та визначаючих співвідношень.*

Konovalov A., Pyliavska O., Shatokhina Iu.

Investigation of cyclic subgroups of 2-groups of small order using the computational algebra system GAP.

Y. Berkovich proposed the next problem:"Suppose that p-group G satisfies the following condition: if Z is a cyclic subgroup of G, then either $Z \le Z(G)$ *or* $Z \cap Z(G) = \{1\}$. *Classify all such groups". Earlier Pyliavska and Shatokhina have proved that all regular p-groups satisfying this condition are either abelian p-groups or p-groups with exponent p. We used the computational algebra system GAP to search for examples of non-abelian non-regular 2-groups with the same property. We obtained that: 1) each non-abelian group of order smaller than* 2^7 *has a cyclic subgroup which is not contained in the center of the group and has a non-trivial intersection with it; 2) there are exactly two non-regular groups of order* 2^7 *and eight non-regular groups of order* 2^8 *which satisfy the condition from the Berkovich's problem.*

1. Постановка задачі

Я.Беркович в своїй книзі [1] сформулював наступну проблему: “Нехай р-група *G* задовольняє умові: якщо *C* є циклічною підгрупою групи *G*, то або $C \le Z(G)$, або $C \bigcap Z(G) = \{1\}$. Класифікувати всі такі групи”. Надалі *p*-групу *G*, що задовольняє даній умові, будемо називати ZC-групою.

В роботі [2] авторами було доведено, що абелеві *p*-групи та групи експоненти *p* вичерпують всі регулярні *p*-групи, які задовольняють цій умові. Спроби знайти приклади ZC-груп серед нерегулярних груп порядку $2^3, 2^4$ дали негативний результат. Виникло природне питання: чи існують групи, що задовольняють вказаній умові, крім абелевих груп та груп експоненти *p*? Такі групи надалі будемо називати нетривіальними ZC-групами.

Нагадаємо, що *p*-група *G* називається регулярною, якщо для будь-яких елементів $g, h \in G$ має місце співвідношення $g^p h^p = (gh)^p \prod_i s_i^p$, де s_i є елементом комутанта групи $\langle g, h \rangle$, породженої елементами *g, h*. Відомо (див. [3], [4]), що кожна *p*-група, клас нільпотентності якої менше, ніж *p*, або порядок якої менше, ніж p^{p+1}, є регулярною, а всі неабелеві групи порядку 2^n є нерегулярними. Для пошуку прикладів нерегулярних ZC-груп було використано систему комп’ютерної алгебри GAP [5]. Одним з її компонентів є спеціальна мова, за допомогою якої можна створювати власні програми і розширювати систему GAP. Нами було створено програму, яка дозволяє для кожної *p*-групи знайти всі циклічні підгрупи і дослідити їх перетин з центром.

Задача «розглянути всі *p*-групи заданого порядку і виділити серед них групи з певними властивостями» вирішується значно легше, якщо не будувати кожну групу окремо, а користуватись списками всіх неізоморфних груп заданого порядку. Як відомо, проблема ізоморфізму груп у загальному випадку є алгоритмічно нерозв’язною, тобто неможливо побудувати алгоритм, за допомогою якого для двох довільних груп, заданих твірними і визначальними співвідношеннями, можна було б визначити, чи є ці групи ізоморфними, чи ні [6]. Існують методи [7] побудови всіх неізоморфних *p*-груп даного порядку, що мають ітеративний характер, тобто для побудови груп більшого порядку необхідна інформація про будову груп меншого порядку, а також їх груп автоморфізмів. Отже, практичне застосування їх можливо тільки для «груп малих порядків». Для $p = 2$ такими групами на даний час є групи, порядок яких не перевищує 2^9 ([8-11]) і для $p \geq 3$ - групи, порядок яких не перевищує p^7 ([5, 12-17]).

Зрозуміло, що разом з порядком групи різко зростає не тільки кількість груп даного порядку, але і складність будови кожної групи. А отже і час, що потрібен на побудову як самої групи, так і на побудову решітки її підгруп. Цей час значно скорочується, якщо користуватися стандартними бібліотеками груп, що входять до складу GAP, зокрема бібліотекою `SmallGroups` [18-19]. Бібліотека `SmallGroups` містить всі групи, порядок яких не перевищує 2000, за винятком груп порядку 2^{10}. Нерегулярні p-групи з цього списку можуть мати лише такі порядки: 3^n ($n = 5,6$) і 2^n ($n = 3,...,9$).

Кожна група з бібліотеки має своє позначення для її типу ізоморфізму, яке має вигляд `[n1, n2]`, де `n1` - порядок групи, `n2` - її номер у списку груп порядку `n1`. Групу, яка має тип ізоморфізму `[n1, n2]`, можна викликати з бібліотеки за допомогою функції `SmallGroup`, наприклад: `S:=SmallGroup(16,8);`

2. Алгоритм

В даній роботі ми зосередимось на властивостях груп, порядок яких є степенем 2. Пошук ZC-груп здійснювався за наступним алгоритмом:

1. Вибираємо по черзі групу заданого порядку 2^n. Оскільки для абелевих груп та груп експоненти p проблема вирішена, вилучаємо їх із рогляду.
2. Для неабелевої групи з експонентою більше p досліджуємо всі циклічні підгрупи групи G, порядок яких більше p. Щоб зменшити обсяг перевірки, розбиваємо множину всіх підгруп групи на класи спряжених елементів. Оскільки всі підгрупи, що належать одному класу, мають однаковий тип і однаковий перетин з центром, то досить вибрати один представник цього класу, і перевіряти умову тільки для нього.
3. Вибираючи по одному елементу з множини представників, перевіряємо, чи є це циклічна підгрупа. Якщо так, то визначаємо її перетин з центром. Якщо хоча б одна циклічна підгрупа групи G не міститься в центрі, але має з ним нетривіальний перетин, то переходимо до наступної групи. Якщо ж для всіх циклічних підгруп групи G, які не містяться в центрі, одержуємо, що вони мають з центром тривіальний перетин, то виводимо на екран повідомлення,

що у даної групи немає циклічних підгруп, які мають нетривіальний перетин з її центром. Переходимо до наступної групи.

3. Реалізація

Цей алгоритм було реалізовано на мові GAP. Для його реалізації та тестування було створено такі функції:

1) Функція `PrintRelations(G)`, яка виводить на екран для візуального контролю визначальні співвідношення групи *G*.

Наприклад:

```
gap> G:=SmallGroup(16,4);
     # Стандартна функція, що викликає з  бібліотеки SmallGroups
     # групу, яка має номер 4 у списку груп порядку 16.
          <pc group of size 16 with 4 generators>
gap> PrintRelations(G);
          g1 ^ 2 = g4
          g2 ^ 2 = g3
          g3 ^ 2 = id
          g4 ^ 2 = id
          g2 ^ g1 = g2*g3
```

При цьому група порядку p^n задається n твірними і визначаючими співвідношеннями як поліциклічна група, тобто як n–кратне розширення n циклічних груп простого порядку. Для обчислення визначаючих співвідношень поліциклічна група (pc-group) G має бути задана як поліциклічно-представлена група (pcp-group). В системі GAP можливість виконання дій над певним алгебраїчним об’єктом сильно залежить від способу його представлення.

Функція `IsGoodZCGroup`, яка для p-групи *G* порядку *size*, що має номер *i* у списку `SmallGroups`, видає значення *false*, якщо група *G* має хоча б одну циклічну підгрупу, яка не міститься в центрі, але має з ним нетривіальний перетин, і значення *true*, якщо всі підгрупи групи G або містяться в центрі групи, або мають в перетині з центром тільки одиничний елемент.

Наприклад:

```
gap>IsGoodZCGroup(8,3); # група Діедра порядку 8
          false
gap>IsGoodZCGroup(128,36);
          true
```

Зауваження . В роботі [20] доведено, що група (128, 36) є мініальною 2-породженою нерегулярною 2-групою, в якій всі циклічні підгрупи мають тривіальний перетин з центром. Отже, на вказаних прикладах функція працює коректно.

3) Функція `ZCGroups`, яка для груп заданого порядку 2^n повертає список номерів нетривіальних ZC-груп або видає повідомлення, що нетривіальних ZC-груп вказаного порядку не існує.

4. Текст програми

Функція `PrintRelations`.

```
PrintRelations:=function(G) # G - група, задана як pc-група
local f1,H;
     # Для даної групи будується ізоморфна pcp-група
f1:=IsomorphismPcpGroup(G); H:=Image(f1);
PrintPcpPresentation(H);
end;
```

Функція `IsGoodZCGroup`.

```
     # Функція, що за номером p-групи в списку SmallGroups
     # визначає, чи має вона підгрупи
     # з нетривіальним перетином з центром.
     # Повертає значення true , якщо такі підгрупи є,
     # і false в протилежному випадку.

IsGoodZCGroup := function( size, nr )
local b, G, cc, cl, c;
G := SmallGroup( size, nr );
     # За заданим номером вибираємо групу  зі списку  SmallGroups.
if IsAbelian(G) then  return false;
     # Відкидаємо неабелеві групи
elif Exponent(G)=PrimePGroup(G) then
     # і групи простої експоненти, оскільки відомо,
     # що вони завжди є ZC-групами.
  return false;
else
  cc := ConjugacyClassesSubgroups(G);
     # Стандартна функція,
     # що обчислює класи спряжених підгруп  групи G.
  for cl in cc do
    c := Representative(cl);
     # Стандартна функція,
     # що з кожного класу вибирає представника.
     if IsCyclic(c) then
          # Стандартна функція,
          # що перевіряє, чи є дана підгрупа циклічною.
          if not IsSubgroup( Center(G), c ) then
```

```
            # Стандартна функція, що перевіряє,
            # чи є дана підгрупа c підгрупою центру.
               if Size( Intersection( Center(G), c ) ) > 1 then
                 # Якщо підгрупа  c не міститься в центрі,
                 # то обчислюємо # порядок її перетину з центром.
                 # Якщо порядок  більше 1, то групу  G відкидаємо.
                   return false;
               fi;
          fi;
     fi;
  od;
  Print("The group [", size,", ", nr,
"] is non-regular ZC-group", "\n");
  return true;
fi;
end;
```

Функція ZCGroup.

```
     #Функція для дослідження 2-груп заданого порядку
ZCGroup:=function(n)
local size, # порядок груп, які досліджуються;
      i,    # номер досліджуваної групи у списку груп
            # заданого порядку в бібліотеці SmallGroups;
      k,    # кількість нетрівіальних ZC-груп серед груп
            # заданого порядку;
      L,    # список номерів груп заданого порядку в бібліотеці
            # SmallGroups, які є нетривіальними ZC-групами;
      G;    # група, що досліджується;
size:=2^n;
k:=0; L:=[];
     # створюємо порожній список L
for i in [1..NumberSmallGroups(size)] do
          if IsGoodZCGroup(size,i)=true  then
               # перевіряємо, чи є група з номером (size,i)
               # ZC-групою
               # Якщо так, то додаємо номер ZC-групи до списку L
            k:=k+1; L[k]:=i;
          fi;
od;
if k=0 then
     Print("Non-regular ZC-groups of order 2^",n,);
     Print(" do not exist \n");
else Print(k," non-regular ZC-groups are found \n", L, "\n");
fi;
return L;
end;
```

5. Результати

Продемонструємо роботу з програмою.

```
     gap> l:=ZCGroup(3);
```

```
Non-regular ZC-groups of order 2^3 do not exist
 [  ]
gap> l:=ZCGroup(4);
Non-regular ZC-groups of order 2^4 do not exist
 [  ]
```

Як і при безпосередньому обрахунку, одержуємо, що серед груп порядку 8 та 16 нетривіальних ZC-груп немає.

```
gap> l:=ZCGroup(5);
Non-regular ZC-groups of order 2^5 do not exist
 [  ]
gap> l:=ZCGroup(6);
Non-regular ZC-groups of order 2^6 do not exist
 [  ]
```

Отже, серед груп порядку 32 і 64 нетривіальних ZC-груп також немає. Чи існують взагалі набелеві 2-групи, що задовольняють вказаній умові?

```
gap> l:=ZCGroup(7);
The group G=[ 128, 36 ] is non-regular ZC-group
The group G=[ 128, 836 ] is non-regular ZC-group
2  ZC-groups are found
[36,836]
```

Отже, знайдено 2 групи порядку 128, які є ZC-групами. Це групи, які в бібліотеці `SmallGroups` мають відповідно номери [128,36] і [128,836]. Визначальні співвідношення для цих груп одержимо за допомогою функції `PrintRelations(G)`.

```
gap> G1:=SmallGroup(128,36);
<pc group of size 128 with 7 generators>
gap> PrintRelations(G1);
g1 ^ 2 = g4, g2 ^ 2 = g5, g3 ^ 2 = id, g4 ^ 2 = id,
g5 ^ 2 = id, g6 ^ 2 = id, g7 ^ 2 = id, g2 ^ g1 = g2*g3,
g3 ^ g1 = g3*g6, g3 ^ g2 = g3*g7,g4 ^ g2 = g4*g6,
g5 ^ g1 = g5*g7
gap> G2:=SmallGroup(128,836);
<pc group of size 128 with 7 generators>
gap> PrintRelations(G2);
g1 ^ 2 = g4*g5*g6, g2 ^ 2 = g4*g5, g3 ^ 2 = g4,
g4 ^ 2 = id, g5 ^ 2 = id, g6 ^ 2 = id, g7 ^ 2 = id,
g2 ^ g1 = g2*g4, g3 ^ g1 = g3*g5, g3 ^ g2 = g3*g6,
g4 ^ g1 = g4*g7, g5 ^ g1 = g5*g7, g5 ^ g3 = g5*g7,
g6 ^ g2 = g6*g7
```

Для груп порядку 256 одержали:

```
gap> l:=ZCGroup(8);
The group G=[256, 337] is non-regular ZC-group
```

```
The group G=[256, 414] is non-regular ZC-group
The group G=[256, 1087] is non-regular ZC-group
The group G=[256, 1089] is non-regular ZC-group
The group G=[256, 3678] is non-regular ZC-group
The group G=[256, 3679] is non-regular ZC-group
The group G=[256, 4306] is non-regular ZC-group
The group G=[256, 16834] is non-regular ZC-group
8  non-regular ZC-groups are found

[337, 414, 1087, 1089, 3678,
3679, 4306, 16834]
```

Вивчаючи визначальні співвідношення знайдених груп, легко можна побачити, що групи (256,1087) та (256,16834) є прямим добутком циклічної групи порядку 2 і групи (128, 36) та групи (128, 836) відповідно. Визначальні співвідношення вказаних груп 128-го порядку наведені вище. Отже, задля економії місця, ми наведемо тільки визначальні співвідношення інших 6-ти груп порядку 256.

```
gap> G1:=SmallGroup(256,337);
<pc group of size 256 with 8 generators>
g1 ^ 2 = g4, g2 ^ 2 = g7, g3 ^ 2 = id, g4 ^ 2 = g6,
g5 ^ 2 = id, g6 ^ 2 = id, g7 ^ 2 = id, g8 ^ 2 = id,
g2 ^ g1 = g2*g3, g3 ^ g1 = g3*g5, g3 ^ g2 = g3*g8,
g4 ^ g2 = g4*g5, g4 ^ g3 = g4*g7, g5 ^ g1 = g5*g7,
g5 ^ g4 = g5*g8, g6 ^ g2 = g6*g8, g7 ^ g1 = g7*g8
gap> G2:=SmallGroup(256,414);
<pc group of size 256 with 8 generators>
gap> PrintRelations(G2);
g1 ^ 2 = g4, g2 ^ 2 = g5, g3 ^ 2 = g6*g7, g4 ^ 2 = id,
g5 ^ 2 = id, g6 ^ 2 = id, g7 ^ 2 = id, g8 ^ 2 = id,
g2 ^ g1 = g2*g3, g3 ^ g1 = g3*g5, g3 ^ g2 = g3*g6,
g4 ^ g2 = g4*g5*g6*g7, g4 ^ g3 = g4*g7, g5 ^ g1 = g5*g7,
g5 ^ g3 = g5*g8, g6 ^ g1 = g6*g8, g6 ^ g2 = g6*g8,
g7 ^ g2 = g7*g8
gap> G3:=SmallGroup(256,1089);
<pc group of size 256 with 8 generators>
gap> PrintRelations(G3);
g1 ^ 2 = g5, g2 ^ 2 = g6, g3 ^ 2 = id, g4 ^ 2 = id,
g5 ^ 2 = id, g6 ^ 2 = id, g7 ^ 2 = id, g8 ^ 2 = id,
g2 ^ g1 = g2*g4, g3 ^ g1 = g3*g7, g4 ^ g1 = g4*g7,
g4 ^ g2 = g4*g8, g5 ^ g2 = g5*g7, g6 ^ g1 = g6*g8.
gap> G4:=SmallGroup(256, 3678);
gap> PrintRelations(G4);
g1 ^ 2 = g4*g5*g6, g2 ^ 2 = g4*g5, g3 ^ 2 = g4, g4 ^ 2 = id,
g5 ^ 2 = id, g6 ^ 2 = id, g7 ^ 2 = id, g8 ^ 2 = id,
g2 ^ g1 = g2*g4, g3 ^ g1 = g3*g5, g3 ^ g2 = g3*g6,
g4 ^ g1 = g4*g7, g4 ^ g2 = g4*g8, g5 ^ g1 = g5*g7*g8,
```

```
 g5 ^ g2 = g5*g8, g5 ^ g3 = g5*g7, g6 ^ g1 = g6*g8,
g6 ^ g2 = g6*g7, g6 ^ g3 = g6*g8.
     gap> G5:=SmallGroup(256, 3679);
     <pc group of size 256 with 8 generators>
     gap> PrintRelations(G5);
 g1 ^ 2 = g4*g5*g6*g7, g2 ^ 2 = g4*g5, g3 ^ 2 = g4,
 g4 ^ 2 = id, g5 ^ 2 = id, g6 ^ 2 = id, g7 ^ 2 = id,
 g8 ^ 2 = id, g2 ^ g1 = g2*g4, g3 ^ g1 = g3*g5,
 g3 ^ g2 = g3*g6, g4 ^ g1 = g4*g7, g4 ^ g2 = g4*g8,
 g5 ^ g1 =  g5*g7*g8, g5 ^ g2 = g5*g8, g5 ^ g3 = g5*g7,
 g6 ^ g1 = g6*g8, g6 ^ g2 = g6*g7, g6 ^ g3 = g6*g8.
     gap> G6:=SmallGroup(256, 4306);
     <pc group of size 256 with 8 generators>
     gap> PrintRelations(G6);
 g1 ^ 2 = g7, g2 ^ 2 = g4*g5, g3 ^ 2 = g4, g4 ^ 2 = id,
 g5 ^ 2 = id, g6 ^ 2 = id, g7 ^ 2 = idg8 ^ 2 = id,
 g2 ^ g1 = g2*g4,  g3 ^ g1 = g3*g5, g3 ^ g2 = g3*g6,
 g4 ^ g1 = g4*g8, g4 ^ g2 = g4*g8, g5 ^ g2 = g5*g8,
 g5 ^ g3 = g5*g8, g6 ^ g1 = g6*g8, g6 ^ g2 = g6*g8,
 g6 ^ g3 = g6*g8, g7 ^ g2 = g7*g8.
```

6. Подяка

Автори висловлюють щиру подяку проф. З. Янку та проф. В.Чепулічу, які звернули нашу увагу на цю задачу.

Bibliography

1. *Berkovich Y.* Groups of prime power order. - (In preparation)

2. *Pylyavska O., Shatohina Iu.* The *p*-groups satisfying the condition: each cyclic subgroup is contained in the center or has a trivial intersection with it // Наукові записки НаУКМА. – Т.51. Фізико-математичні науки. – 2006. – С.3-4.

3. *Холл М.* Теория групп. – М.: ИЛ, 1962. – 468 с.

4. *Huppert B.* Endliche Gruppen, I. – Springer-Verlag, Berlin-Heidelberg-New York. – 1967. – p.794.

5. The GAP Group, GAP -- Groups, Algorithms, and Programming, Version 4.4.10; 2007. http://www.gap-system.org

6. Новиков П.С. Об алгоритмической неразрешимости проблемі тождества слов в теории групп // Тр. Математического ин-та АН СССР. - М., 1955. - т.44.

7. *Newman M.F.* Determination of groups of prime-power order // Group Theory (Canberra, 1975), Lecture Notes in Mathematics, Vol. 573, P. 73-84. Springer-Verlag, Berlin-Heidelberg-New York, 1977.

8. *Hall M.Jr, Senior J.K.* The Groups of order 2^6 $(n \leq 6)$. – Macmillan, New York, 1964.

9. *James R, Newman M.F., and O'Brien E.A.* The groups of order 128 // J. Algebra 129, 1990, P.136 – 158.

10. *O'Brien E.A.* The groups of order 256 // J. Algebra 143, 1991, P.219 – 235.

11. Eick B., O'Brien E. A. The groups of order 512 // Proceedings of the Abschlusstagung zum DFG Schwerpunkt Algorithmische Algebra und Zahlentheorie, Springer, 1998, P. 379 – 380.9.

12. *James R.* The Groups of Order p^6 (p and Odd Prime). // Mathematics of Computation*,* Vol. 34, No. 150 (Apr., 1980), P. 613-637.

13. *Пилявская О.С.* Классификация групп порядка p^6 (p>3). – Рук. деп. в ВИНИТИ, №1877-83 Деп. – Рук. – с. 63.

14. *Пилявская О.С.* Применение матричных задач к классификации групп порядка p^6, p>3. – В кн.: Линейная алгебра и теория представлений. – Киев, Ин-т математики АН УССР, 1983. – С. 86 – 99.

15. *Newman M. F., O'Brien E. A., and Vaughan-Lee M. R.* Groups and nilpotent Lie rings whose order is the sixth power of a prime // Journal of Algebra, V.278, 2003, P.383 – 401.

16. *O'Brien E.A., Vaughan-Lee M.R.* The groups with order p^7 for odd prime p // Journal of Algebra, Vol. 292, 2005, P.243 – 258.

17. *Eick B. O'Brien E.A.* Enumerating p-groups // J. Austral. Math. Soc., Vol. 67, 1999, P.191 – 205.

18. *Besche H., Eick B., O'Brien E. A*. The groups of order at most 2000 // Electronic research announcements of the American Mathematical Society. February 12, 2001. S1079-6762(01)00087-7. Volume 7, P.1–4.

19. The Small Groups Library // http://www.tu-bs.de/~beick/small/small.html

Відомості про авторів.

Коновалов Олександр Борисович, кандидат фізико-математичних наук.

Пилявська Ольга Степанівна, доцент кафедри математики Національного університету “Києво-Могилянська Академія”.

Наукові інтереси: теорія скінченних p-груп.

Шатохіна Юлія Вячеславівна, аспірант Інституту космічних досліджень НАН та НКА України.

Наукові інтереси: теорія груп, символьні обчислення, математичне моделювання, динамічні системи, самоорганізація, біофізика, квантові комп’ютери.