Когда все групповые коды некоммутативной группы абелевы (вычислительный подход)?

К. ГАРСИА-ПИЛЬЯДО
Университет Овьедо, Испания

С. ГОНСАЛЕС
Университет Овьедо, Испания

В. Т. МАРКОВ
Московский государственный университет им. М. В. Ломоносова

К. МАРТИНЕС
Университет Овьедо, Испания

А. А. НЕЧАЕВ
Московский государственный университет им. М. В. Ломоносова
e-mail: alexnechaev@inbox.ru

УДК 519.725+512.552.7

Ключевые слова: групповые коды, абелевы коды, групповое кольцо, компьютерная алгебра.

Аннотация

Пусть G — конечная группа, F — поле. Любой линейный код над полем F, перестановочно эквивалентный коду, определённому некоторым идеалом группового кольца FG, назовём G-кодом. Теория таких «абстрактных» групповых кодов была развита в 2009 году. Код был назван абелевым, если он является A-кодом для некоторой абелевой группы A. Были приведены некоторые условия, при которых все G-коды для заданной группы G абелевы, но ни одного примера неабелева группового кода в это время не было известно. С помощью системы компьютерной алгебры GAP мы показываем, что все G-коды над любым полем F являются абелевыми, если $|G| < 127$ и $|G| \notin \{24, 48, 54, 60, 64, 72, 96, 108, 120\}$, но для $F = \mathbb{F}_5$ и $G = \mathrm{S}_4$ существуют неабелевы G-коды над F. Показано также, что существование левого неабелева группового кода для заданной группы зависит, вообще говоря, от выбора поля коэффициентов; для (двусторонних) групповых кодов соответствующий вопрос остаётся открытым.

Abstract

C. García Pillado, S. González, V. T. Markov, C. Martínez, A. A. Nechaev, When are all group codes of a noncommutative group Abelian (a computational approach)?, Fundamentalnaya i prikladnaya matematika, vol. 17 (2011/2012), no. 2, pp. 75—85.

Let G be a finite group and F be a field. Any linear code over F that is permutation equivalent to some code defined by an ideal of the group ring FG will be called a G-code. The theory of these "abstract" group codes was developed in 2009. A code is called Abelian if it is an A-code for some Abelian group A. Some conditions were given that all

Фундаментальная и прикладная математика, 2011/2012, том 17, № 2, с. 75—85.

G-codes for some group G are Abelian but no examples of non-Abelian group codes were known at that time. We use a computer algebra system GAP to show that all G-codes over any field are Abelian if $|G| < 128$ and $|G| \notin \{24, 48, 54, 60, 64, 72, 96, 108, 120\}$, but for $F = \mathbb{F}_5$ and $G = \mathrm{S}_4$ there exist non-Abelian G-codes over F. It is also shown that the existence of left non-Abelian group codes for a given group depends in general on the field of coefficients, while for (two-sided) group codes the corresponding question remains open.

Введение

Пусть F — поле. Рассмотрим естественное действие симметрической группы S_n на n-мерном пространстве F^n, определённое перестановками координат:

$$\sigma(a_1, \ldots, a_n) = \big(a_{\sigma(1)}, \ldots, a_{\sigma(n)}\big) \quad \text{для всех} \quad (a_1, \ldots, a_n) \in F^n.$$

Напомним, что два кода $\mathcal{C}_1, \mathcal{C}_2 \subseteq F^n$ *перестановочно эквивалентны*, если $\mathcal{C}_2 = \sigma(\mathcal{C}_1)$ для некоторой перестановки $\sigma \in \mathrm{S}_n$. Для данного кода $\mathcal{C} \subseteq F^n$ пусть $\mathrm{PAut}(\mathcal{C})$ — группа всех перестановок $\sigma \in \mathrm{S}_n$, таких что $\sigma(\mathcal{C}) = \mathcal{C}$.

Пусть $G = \{g_0 = e, g_1, \ldots, g_{n-1}\}$ — конечная группа. Любой (левый) идеал L группового кольца FG определяет (левый) групповой код $\mathcal{K}(L)$ длины n над F по правилу

$$(a_0, a_1, \ldots, a_{n-1}) \in \mathcal{K}(L) \iff a_0 g_0 + a_1 g_1 + \ldots + a_{n-1} g_{n-1} \in L.$$

Любой линейный код над полем F, перестановочно эквивалентный коду вида $\mathcal{K}(L)$ для некоторого (левого) идеала L кольца FG, называется (*левым*) *G-кодом*.

Код называется *абелевым*, если он является A-кодом для некоторой абелевой группы. В [3] было показано, что существуют неабелевы левые групповые коды, но не было представлено ни одного примера неабелева группового кода.

В этой заметке мы показываем, как можно использовать систему компьютерной алгебры GAP [4] для описания некоторых групп, для которых все групповые коды являются абелевыми, а также для построения примера неабелева группового кода и для доказательства того, что все левые групповые коды в $\mathbb{F}_2\mathrm{Q}_8$ абелевы.

Для любых подмножеств A и B группы G обозначим через AB множество всех произведений ab, где $a \in A$ и $b \in B$. Мы будем говорить, что группа G *имеет абелево разложение*, если существуют абелевы подгруппы A, B группы G, такие что $G = AB$. Это условие было введено в [3], где было доказано, что если группа G имеет абелево разложение, то любой G-код является абелевым групповым кодом [3, теорема 3.1]. Мы покажем, что все группы G порядка меньше 128, кроме таких, что $|G| \in \{24, 48, 54, 60, 64, 72, 96, 108, 120\}$, имеют абелевы разложения. Мы также приведём полный список групп порядка $2^6 = 64$, не имеющих абелева разложения. Некоторые из них дают отрицательный ответ на следующий естественный вопрос: имеет ли абелево разложение любая группа ступени нильпотентности 2? Затем мы докажем существование неабелевых

S_4-кодов над $\mathbb{F}_5$. Наконец, мы покажем, что все левые идеалы группового кольца $\mathbb{F}_2Q_8$ являются двусторонними и являются, таким образом, абелевыми кодами, хотя в [1] было показано, что что в кольце $\mathbb{F}_4Q_8$ имеются левые $[8,3,5]$-коды, но не существует A-кодов над $\mathbb{F}_4$ с теми же параметрами ни для какой абелевой группы A порядка 8 (во избежание недоразумений следует отметить, что в [1] левые групповые коды были названы групповыми кодами).

1. Абелевы разложения

Следующая лемма — лёгкое упражнение из элементарной теории групп.

Лемма 1.1.

1. *Если A, B — две подгруппы группы G, то*
$$|AB| = \frac{|A|\,|B|}{|A \cap B|}.$$
2. *Если $G = AB$ для некоторых подгрупп A, B, то для любой подгруппы A', сопряжённой с A, существует подгруппа B', сопряжённая с B, такая что $G = A'B'$.*

Значит, можно использовать следующую простую функцию GAP, чтобы определить, имеет ли данная группа G абелево разложение.

```
HasAbelianDecomposition:=function(G)
local lat, A, x, xx, y, z, n, flag;
n:=Size(G);
lat:=LatticeSubgroups(G);
#GAP вычисляет структуру всех подгрупп
A:=Filtered(ConjugacyClassesSubgroups(lat),
x->IsAbelian(Representative(x)));
#A - список классов сопряжённости абелевых подгрупп
flag:=0;
for xx in A do x:=Representative(xx);
#берётся произвольный представитель данного класса
for y in A do for z in AsList(y) do
#проверяются все абелевы подгруппы в G
if Size(x)*Size(z)/Size(Intersection(x,z))=n
then return true; fi;
od; od;
od;
return false;
#функция возвращает true, если абелево разложение найдено,
#и false в противном случае
end;
```

Следующий код — пример использования этой функции.

```
for n in [2..127] do cnt:=0; for G in
AllSmallGroups(Size,n,IsAbelian,false) do
if not HasAbelianDecomposition(G) then cnt:=cnt+1; fi; od;
if cnt>0 then Print(n, " ", cnt, "\n"); fi; od;
```

Этот код выдаёт следующую таблицу.

```
24 2
48 6
54 1
60 1
64 19
72 7
96 26
108 4
120 6
```

Существуют чисто алгебраические доказательства того, что любая группа порядка $p^i q^j$, где p, q — простые числа (необязательно различные) и $0 \leqslant i, j \leqslant 2$, имеет абелево разложение, также как любая группа порядка $32 = 2^5$. Эти доказательства будут опубликованы позже. Также имеется конструкция группы порядка p^5, не имеющей абелева разложения, где $p > 2$ — простое число. Приведённая выше таблица показывает, что эти результаты нельзя усилить.

Мы видим, что две группы порядка 24 не имеют абелева разложения. Одна из них может быть идентифицирована следующим образом.

Предложение 1.2. *Симметрическая группа* S_4 *не имеет абелева разложения.*

Доказательство. Выполнение следующей строки в GAP

```
HasAbelianDecomposition(SymmetricGroup(4));
```

выдаёт результат `false`. □

Заметим также, что существует достаточно много групп порядка 64, не имеющих абелева разложения. Таблица 1 содержит индексы всех этих групп в библиотеке GAP, их экспоненты и ступень нильпотентности.

Можно указать более красивое описание этих групп. Например, первая из них, имеющая индекс GAP [64, 73], может быть определена следующим образом. Рассмотрим элементарную абелеву 2-группу N с тремя образующими z_1, z_2 и z_3, а также элементарную абелеву 2-группу H с тремя образующими $\bar{x}_1$, $\bar{x}_2$ и $\bar{x}_3$. Легко показать, используя теорему Шрайера [2, теорема 15.1.1], что существует расширение G с $N = Z(G)$ и $G/N \cong H$, такое что для некоторых прообразов x_1, x_2, x_3 элементов $\bar{x}_1$, $\bar{x}_2$, $\bar{x}_3$ выполняются следующие соотношения:

$$x_i^2 = z_i^2 = e, \quad i = 1, 2, 3; \quad [x_i, z_j] = [z_i, z_j] = e, \quad i, j = 1, 2, 3;$$
$$[x_i, x_j] = z_{i+j-2}, \quad i, j = 1, 2, 3, \quad i < j.$$

Таблица 1. Группы порядка 64, не имеющие абелева разложения

Индекс GAP	Экспонента	Ступень нильпотентности
[64, 73]	4	2
[64, 74]	4	2
[64, 75]	4	2
[64, 76]	4	2
[64, 77]	4	2
[64, 78]	4	2
[64, 79]	4	2
[64, 80]	4	2
[64, 81]	4	2
[64, 82]	4	2
[64, 149]	8	3
[64, 150]	8	3
[64, 151]	8	3
[64, 170]	8	3
[64, 171]	8	3
[64, 172]	8	3
[64, 177]	8	3
[64, 178]	8	3
[64, 182]	8	3

Требуемые автоморфизмы $a \mapsto a^h$ группы N являются тождественными, а система факторов имеет вид

$$(\bar{x}_1^{k_1}\bar{x}_2^{k_2}\bar{x}_3^{k_3}, \bar{x}_1^{r_1}\bar{x}_2^{r_2}\bar{x}_3^{r_3}) = z_1^{r_1k_2}z_2^{r_1k_3}z_3^{r_2k_3} \quad \text{для всех} \quad k_i, r_j \in \mathbb{F}_2, \quad i,j = 1,2,3.$$

2. Неабелевы групповые коды в $\mathbb{F}_5\mathrm{S}_4$

Разумеется, из предложения 1.2 не следует, что существуют неабелевы S_4-коды над какими-либо полями. Однако мы приводим ниже такие примеры. До конца раздела положим, что $F = \mathbb{F}_5$ и $G = \mathrm{S}_4$ реализована как группа подстановок множества $\{0,1,2,3\}$.

Наше изучение групповой алгебры FG основано на применении функции GAP `DirectSumDecomposition(A)`, дающей разложение полупростого конечномерного кольца A в прямую сумму минимальных идеалов. В нашем случае

R — полупростое кольцо по классической теореме Машке, так что следующий код GAP выдаёт пять минимальных идеалов в R.

```
G:=SymmetricGroup(4);
F:=GF(5);
R:=GroupRing(F,G);
D:=DirectSumDecomposition(R);;
List(D,Dimension);
```

Этот фрагмент выдаёт список `[ 9, 9, 4, 1, 1 ]`, т. е. имеется два идеала размерности 1, два идеала размерности 9 и один идеал размерности 4.

Теорема 2.1. *Коды, соответствующие минимальным идеалам в R размерности 9, не являются абелевыми.*

Доказательство. Прямое вычисление групп перестановочных автоморфизмов для данных кодов заняло бы слишком много времени, поэтому мы использовали следующий «обходной манёвр».

Сначала мы нашли распределение весов для каждого из этих двух идеалов, используя следующую GAP-функцию.

```
WeightDistribution:=function(I,R)
local wlist, k, j, d, x, V, B, mf;
mf:=Size(LeftActingDomain(R))-1;
wlist:=List([0..Dimension(R)],x->0);
wlist[1]:=1;
d:=Dimension(I);
B:=BasisVectors(Basis(I));
for j in [1..d] do
V:=SubspaceNC(R,B{[(j+1)..d]});
for x in V do
k:=Size(CoefficientsAndMagmaElements(B[j]+x))/2+1;
wlist[k]:=wlist[k]+mf;
od;
od;
return wlist;
end;
```

Она была использована следующим кодом.

```
WD1:=WeightDistribution:=function(D[1],R);
WD2:=WeightDistribution:=function(D[2],R);
```

Два распределения весов оказались одинаковыми, и их можно описать следующей таблицей.

Вес d	Число слов веса d	Вес d	Число слов веса d
0	1	17	190080
8	324	18	320640
10	144	19	365184
12	5520	20	437952
13	2304	21	245760
14	23808	22	158400
15	23328	23	47232
16	111840	24	20608

Затем мы проверили все абелевы коды длины 24 над $\mathbb{F}_5$. Оказалось, что эта часть вычислений занимает больше всего времени, так что мы применили следующие простые наблюдения:

1) действие автоморфизмов группы можно продолжить до автоморфизма группового кольца, сохраняющего вес элементов;
2) если при вычислении распределения весов оказывается, что для некоторого веса w число уже найденных слов веса w превышает число таких слов в известном распределении весов WD1, то распределение весов для этого идеала не может совпадать с WD1, и в этот момент вычисление распределения весов можно остановить.

Были использованы следующие функции GAP.

1. Техническая функция, преобразующая автоморфизмы группы в автоморфизмы группового кольца.

```
StandardIsomorphismsOfAGroupRing:=function(R,HH)
local H, h, f, x, y, B1, B2, C, n;
H:=[];
B1:=BasisVectors(Basis(R));
n:=Size(B1);
C:=List(B1, x->(CoefficientsAndMagmaElements(x)[1]));
for h in HH do
B2:=List([1..n], x->B1[Position(C,Image(h,C[x]))]);
#Print(B2, "\n");
Add(H, AlgebraHomomorphismByImagesNC( R, R, B1, B2 ));
od;
return H;
end;
```

2. Функция, выдающая список идеалов заданной размерности k. Каждый из этих идеалов определён как сумма минимальных левых идеалов, размерности которых перечислены в списке l.

```
CombinationsOfGivenSum:=function(l,k)
local AllCombList, n, s; n:=Size(l);
```

```
AllCombList:=Combinations([1..n]);
return Filtered(AllCombList, x->(Sum(List(x, i->l[i]))=k));
end;
```

3. Функция, перечисляющая перестановки на множестве минимальных идеалов, индуцируемые множеством H автоморфизмов группы.

```
PermutationsOfComponents:=function(R,H,DSD)
local x, y, h, HH, PL, l, B, I, II, pl;
l:=Size(DSD);
PL:=[[1..l]]; #identity permutation must present
HH:=StandardIsomorphismsOfAGroupRing(R,H);
for h in HH do
pl:=[];
for I in DSD do
B:=BasisVectors(Basis(I));
II:=Ideal(R,List(B,y->Image(h,y)));
Add(pl,Position(DSD,II));
od;
if not pl in PL then Add(PL,pl); fi;
od;
return PL;
end;
```

4. Функция, проверяющая, переводит ли некоторая перестановка из заданного списка PL заданное множество минимальных идеалов в лексикографически меньшее. При поиске идеалов с заданным распределением весов достаточно рассматривать только идеалы, соответствующие лексикографически минимальным множествам минимальных идеалов.

```
IsMinimalCombination:=function(L, PL)
local x, i;
for x in PL do
for i in L do
if x[i]>i then break; else if x[i]<i then return false;
fi; fi;
od;
od;
return true;
end;
```

5. Функция, сравнивающая распределение весов данного идеала с заданным распределением весов.

```
EqualWeightDistribution:=function(I, R, WD)
local wlist, k, j, d, x, V, B, mf;
mf:=Size(LeftActingDomain(R))-1;
```

```
wlist:=List([0..Dimension(R)],x->0);
wlist[1]:=1;
d:=Dimension(I);
B:=BasisVectors(Basis(I));
for j in [1..d] do
V:=SubspaceNC(R,B{[(j+1)..d]});
for x in V do
k:=Size(CoefficientsAndMagmaElements(B[j]+x))/2+1;
wlist[k]:=wlist[k]+mf;
if wlist[k]>WD[k] then return false; fi;
od;
od;
return true;
end;
```

Теперь приведём код GAP, проверяющий утверждение теоремы.

```
G:=SymmetricGroup(4);
F:=GF(5);
R:=GroupRing(F,G);
D:=DirectSumDecomposition(R);;
WD1:=WeightDistribution(D[1],R);
allab:=AllSmallGroups(Size,24,IsAbelian,true);;
for A in allab do
R:=GroupRing(F,A);;
dsd:=DirectSumDecomposition(R);;
dsddim:=List(dsd,Dimension);;
CL:=CombinationsOfGivenSum(dsddim,9);;
H:=AutomorphismGroup(G);;
dsdperm:=PermutationsOfComponents(R,H,dsd);;
RCL:=Filtered(CL, x->IsMinimalCombination(x,dsdperm));;
for C in RCL do I:=Sum(List(C, x->dsd[x]));;
if EqualWeightDistribution(I,R, WD1) then
Print("Equal weight distribution found\n");; break;
fi;
od;
od;
```

Выполнение этого кода потребовало нескольких часов работы компьютера, но не было найдено ни одного абелева кода с распределением весов, записанном в `WD1`. □

Замечание 2.2. В следующей статье мы дадим чисто алгебраическое доказательство того, что `D[3]`, `D[4]` и `D[5]` определяют абелевы коды. Однако авторам неизвестно чисто алгебраическое доказательство теоремы 2.1.

3. Замена основного поля

Вообще говоря, неизвестно, зависит ли для заданной группы G существование неабелевых кодов в FG от поля коэффициентов F.

В следующей статье будут доказаны следующие два утверждения.

Предложение 3.1. *Пусть F — подполе поля E и G — группа. Если все G-коды над E абелевы, то все G-коды над F абелевы.*

Предложение 3.2. *Пусть F — подполе поля E и G — группа. Допустим, сверх того, что F — поле разложения для группы G, т. е.*

$$FG \cong \bigoplus_{i=1}^{k} \mathrm{M}_{d_i}(F)$$

(*групповая алгебра — прямая сумма матричных алгебр над F, откуда, в частности, следует, что* $\operatorname{char} F \nmid |G|$). *При этих условиях, если все G-коды над F абелевы, то все G-коды над E абелевы.*

Здесь же мы подчеркнём различие между случаями групповых кодов и левых групповых кодов: имеется достаточно простой пример, показывающий, что аналогичное свойство левых групповых кодов, вообще говоря, не переносится на расширения поля.

Теорема 3.3. *Пусть $F = \mathbb{F}_2$, $E = \mathbb{F}_4$ — расширение поля F и G — группа кватернионов Q_8. Тогда все левые G-коды над F абелевы, но существуют левые неабелевы G-коды над E.*

Доказательство. Вторая часть утверждения следует из уже упомянутого результата [1, таблица 6]: существуют левые $[8, 3, 5]$-коды в кольце $\mathbb{F}_4\mathrm{Q}_8$, но не существует A-кодов с теми же параметрами над $\mathbb{F}_4$ для любой абелевой группы A порядка 8.

Для доказательства первой части утверждения достаточно проверить, что любой левый идеал кольца FG является двусторонним. Действительно, любой Q_8-код над произвольным полем абелев согласно [3, теорема 3.1] и результатам раздела 1.

Мы снова представим программу GAP, проверяющую это утверждение, хотя чисто алгебраическое доказательство известно и будет опубликовано в другой работе.

Конечно, достаточно рассмотреть только главные левые идеалы, поскольку любой левый идеал — сумма главных. Приведённый ниже код не оптимален по скорости выполнения, но представляется наиболее простым.

```
List(AllSmallGroups(Size,8), StructureDescription);
[ "C8", "C4xC2", "D8", "Q8", "C2 x C2 x C2" ]
Q:=AllSmallGroups(Size,8)[4];;
F:=GF(2);; R:=GroupRing(F,Q);;
for x in R do I:=LeftIdeal(R,[x]);
```

```
for y in R do
if not (x*y in I) then
Print(x,"*",y," not in Rx\n"); break;
fi;
od;
od
```

Мы включили вывод первой строки программы, поскольку его использование представляется наиболее простым способом определить группу кватернионов в сессии GAP. Выполнение этого кода занимает несколько секунд. Он ничего не выводит, значит, приведённое утверждение верно. □

Литература

[1] Коусело Е., Гонсалес С., Марков В., Нечаев А. Групповые коды и их неассоциативные обобщения // Дискрет. мат. — 2004. — Т. 16, № 1. — С. 146—156.

[2] Холл М. Теория групп. — М.: Изд. иностр. лит., 1962.

[3] Bernal J. J., del Río Á., Simón J. J. An intrinsical description of group codes // Designs, Codes and Cryptography. — 2009. — Vol. 51, no. 3. — P. 289—300.

[4] http://www.gap-system.org/.