Следствие 2. *Пусть $\mathfrak{F}$ — формация всех p-разложимых групп. Тогда и только тогда любая собственная подгруппа не p-разложимой группы G либо $\mathfrak{F}$-субнормальна, либо $\mathfrak{F}$-абнормальна, когда G — разрешимая группа одного из следующих типов:*

1) $G = G_p \rtimes G_q$, где G_q — циклическая подгруппа Картера группы G и максимальная подгруппа из G_q нормальна в G, а $G_p = G^{\mathfrak{F}}$.

2) $G = G_{p'} \rtimes G_p$, где G_p — циклическая подгруппа Картера группы G и максимальная подгруппа из G_p нормальна в G, а $G_{p'} = G^{\mathfrak{F}}$.

Литература

1. Fattahi A. *Groups with only normal and abnormal subgroups* // J. Algebra. 1974. Vol. 28. № 1. P. 15–19.

2. Ebert G., Bauman S. *A note on subnormal and abnormal chains* // J. Algebra. 1975. Vol. 36. № 2. P. 287–293.

3. Förster P. *Finite groups all of whose subgroups are $\mathfrak{F}$-subnormal or $\mathfrak{F}$-subabnormal* // J. Algebra. 1986. № 1. P. 285–293.

4. Семенчук В. Н. *Строение конечных групп с $\mathfrak{F}$-абнормальными или $\mathfrak{F}$-субнормальными подгруппами* // Вопросы алгебры. Минск: Изд-во "Университетское". 1986. № 2. С. 50–55.

5. Семенчук В. Н., Шевчук С. Н. *Конечные группы, у которых примарные подгруппы либо $\mathfrak{F}$-субнормальны, либо $\mathfrak{F}$-абнормальны* // Известия вузов. Математика. 2011. № 8. С. 46–55.

6. Semenchuk V. N., Skiba A. N. *On one generalization of finite $\mathfrak{U}$-critical groups* // ArXiv. org e-Print archive, arXiv:1412.5469v1, 17 Dec 2014.

КОНЕЧНЫЕ ГРУППЫ С НИЛЬПОТЕНТНЫМИ НОРМАЛЬНЫМИ ПОДГРУППАМИ

И.Л. Сохор

Гомельский государственный университет имени Ф. Скорины
Советская, 104, 246019 Гомель, Беларусь Irina.Sokhor@gmail.com

Рассматриваются только конечные группы. Используемая терминология соответствует [1]. Через $\mathfrak{N}$ обозначается формация всех нильпотентных групп. Формация называется наследственной, если она замкнута относительно подгрупп. Формация называется радикальной, если она является классом Фиттинга. $G^{\mathfrak{N}}$ — $\mathfrak{N}$-корадикал группы G — пересечение всех нормальных подгрупп группы G, фактор-группа по которым нильпотентна; $[A]B$ — полупрямое произведение нормальной подгруппы A и подгруппы B.

Пусть $\mathfrak{F}$ — некоторый класс групп. Группа G называется минимальной не $\mathfrak{F}$-группой, если G не принадлежит $\mathfrak{F}$, а каждая собственная подгруппа из G принадлежит $\mathfrak{F}$. Минимальные не $\mathfrak{N}$-группы называют группами Шмидта и их свойства хорошо известны [2].

Естественно возникает задача изучения свойств группы, в которой классу $\mathfrak{F}$ принадлежат лишь некоторые собственные подгруппы, например, нормальные.

Доказана следующая теорема.

Теорема. *Пусть $\mathfrak{F}$ — некоторая наследственная радикальная формация. Если в разрешимой группе G, не принадлежащей $\mathfrak{F}$, каждая собственная нормальная подгруппа принадлежит $\mathfrak{F}$, то справедливы следующие утверждения:*

1) $G_p^G = G$, где $p = |G : M|$, M — нормальная максимальная подгруппа G;

2) $G/G^{\mathfrak{N}}$ — циклическая p-группа;

3) $G = G^{\mathfrak{N}} < x >$, где $x \in G_p$;

4) $G^{\mathfrak{N}} < x^p > \in \mathfrak{F}$;

5) $G^{\mathfrak{N}} = G'$.

Обратно, если разрешимая группа G удовлетворяет условиям 4)–5), то каждая собственная нормальная подгруппа группы G принадлежит $\mathfrak{F}$.

При доказательстве используется следующая лемма, представляющая самостоятельный интерес.

Лемма. *Пусть $\mathfrak{F}$ — некоторая наследственная формация. Если в разрешимой группе G каждая собственная подгруппа, содержащая коммутант G', принадлежит $\mathfrak{F}$, то каждая собственная нормальная подгруппа группы G принадлежит $\mathfrak{F}$.*

При $\mathfrak{F} = \mathfrak{N}$ получаем обобщение групп Шмидта.

Следствие. *Пусть M — нормальная максимальная подгруппа разрешимой ненильпотентной группы G и $|G : M| = p$. Каждая собственная нормальная подгруппа группы G нильпотентна тогда и только тогда, когда $G = [G^{\mathfrak{N}}] < x >$, где $< x >$ — силовская p-подгруппа группы G и $[G^{\mathfrak{N}}] < x^p >$ нильпотентна.*

Литература

1. Huppert, B. *Endliche Gruppen I.* Berlin-Heidelberg-New York: Springer, 1967.

2. Монахов, В. С. *Подгруппы Шмидта, их существование и некоторые приложения* // Труды Украинского математического конгресса–2001. Киев: Институт математики НАН Украины, 2001. С. 81–90.

АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ ЭЛЕМЕНТОВ ИНКАПСУЛИРОВАННЫХ КОЛЕЦ ВЫЧЕТОВ

А.В. Трепачева

Южный федеральный университет
Большая Садовая 105/42, 344006 Ростов-на-Дону, Россия
alina1989malina@ya.ru

Инкапсулированные (black-box) представления алгебраических структур помогают оценить сложность алгоритмов, которые строятся безотносительно конкретного представления элемента [1, 2, 3].

Практическая ценность инкапсулированных колец состоит в том, что они дают оценки на сложность криптоанализа полностью гомоморфных криптосистем в атаке на основе шифртекстов [4, 5].

Определение 1. *Инкапсулированное кольцо вычетов – это шестерка (n, k, h, F, G, T) в которой $n \in \mathbb{N}$ – определяет количество элементов в кольце, $k \in \mathbb{N}$ – определяет длину битового представления кодировки. Функции h, F, G, T определены следующим образом.*

1. *Функция $h : \{0,1\}^k \to \mathbb{Z}_n$ сопоставляет элемент из кольца каждой k-битной двоичной строке. Функция h сюръективна, т. е. каждый элемент кольца представлен по меньшей мере одной битовой строкой.*

2. *Функции $F, G : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}^k$ выполняют сложение и умножение. Они удовлетворяют следующим соотношениям $h(F(x,y)) = h(x) + h(y)$ и $h(G(x,y)) = h(x)h(y)$.*

3. *Функция $T : \{0,1\}^k \times \{0,1\}^k \to \{\mathtt{true}, \mathtt{false}\}$ проверяет равенство двух инкапсулированных элементов: $T(x,y) = \mathtt{true}$ тогда и только тогда, когда $h(x) = h(y)$.*

Определение 2. *Пусть(n, k, h, F, G, T) – инкапсулированное кольцо вычетов. Обозначим отображение, сопоставляющее элементу x некоторое представление $[x]$ как $[]$. **Проблема инкапсулированного кольца вычетов** состоит в следующем: найти алгоритм $\mathcal{A}$ который по данному n и оракулам $F, G, T, []$ и представлению $\alpha \in \mathbb{Z}_n$ находит α в явном виде.*