

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Уральский государственный педагогический университет»
Институт математики, информатики и информационных технологий
Кафедра высшей математики

**Использование системы компьютерной алгебры GAP для типовой
классификации четырехмерных алгебр**

Выпускная квалификационная работа
по направлению «01.03.02 Прикладная математика и информатика»

Работа допущена к защите
«_____» _____ 2016 г.
Зав. кафедрой _____

Исполнитель: студент группы БП-51z
института математики,
информатики и ИТ Бурков Андрей
Владимирович
подпись _____

Руководитель ОПОП:
Подпись _____ / _____ /

Научный руководитель: к.ф.-м.н.,
доцент кафедры ВМ Коробков
Сергей Самсонович
подпись _____

Екатеринбург – 2016

Оглавление

Введение.....	3
Глава I. Теоретические основы.....	5
1.1. Основные понятия	5
1.2. Пирсовские разложения колец	7
1.3. Изоморфизм алгебр.	8
1.4. Понятие решетки	10
1.5. Диаграммы решеток	11
Глава II. Система компьютерной алгебры GAP	13
2.1. Краткая характеристика системы GAP.....	13
2.2. Язык программирования GAP	13
2.3. Алгебры в GAP.....	14
Глава III. Типовая классификация подалгебр четырехмерной алгебры матриц $M(GF(2),3)$	21
Литература	30
Приложение	31
Приложение 1.	31
Приложение 2.	41
Приложение 3.	45
Приложение 4.	47

Введение

Одним из направлений современной алгебры является описание и классификация ее структур, таких как группы, кольца, поля, алгебры и другие. При изучении решеток подалгебр часто приходится использовать конкретные примеры для того, чтобы проверить те или иные предположения. Удобно, когда имеется большой набор самых разных примеров, к которым можно обратиться и быстро решить возникший вопрос. Для разработки каталога с примерами решеток необходимо произвести их классификацию по какому-либо признаку.

Выпускная квалификационная работа посвящена алгебре A квадратных матриц порядка 3 над полем из двух элементов и ее подалгебрам. Дальнейшие исследования могут быть направлены на решение вопроса о классификации алгебр с точностью до изоморфизма, имеющих один и тот же тип решетки подалгебр.

Цель работы состоит в разработке алгоритмов и компьютерных программ для получения типовой классификации четырехмерных подалгебр алгебры матриц третьего порядка над полем $GF(2)$.

Для достижения основной цели необходимо решить следующие *задачи*:

1. Разработка алгоритма и программы для построения четырехмерных подалгебр алгебры A .
2. Разработка алгоритма и программы для нахождения всех подалгебр для каждой четырехмерной алгебры.
3. Разработка алгоритма и программы для определения отношения покрытия на множестве подалгебр.
4. Построение решеток подалгебр.

Работа состоит из введения, трех глав, списка литературы и приложения. Основное содержание работы изложено в трех главах. Первая глава является теоретической, в ней вводятся понятия алгебраических структур и рассматриваются их основные свойства. Вторая глава посвящена системе компьютерной алгебры GAP. В ней описаны основные команды, представлена

краткая характеристика GAP. Третья глава является практической. В ней приводятся алгоритмы, программы и результаты исследований. В приложениях представлен массив всех элементов алгебры матриц, массивы элементов изученных четырехмерных алгебр (в виде их номеров) и диаграммы решеток подалгебр.

Разработанные алгоритмы и программы проверены на примере алгебры типа $(1, 11, 17, 7, 1)$, при этом исследовано 2 класса подалгебр такого типа (в каждом классе по 14 подалгебр).

Глава I. Теоретические основы

1.1. Основные понятия

Определим основные алгебраические структуры, используемые в работе.

Определение 1. [2] Множество G с бинарной операцией \cdot называется *группой*, если выполняются следующие условия:

- 1) $(\forall a, b, c \in G)(a \cdot (b \cdot c) = (a \cdot b) \cdot c)$;
- 2) $(\exists e \in G)(\forall a \in G)(a \cdot e = e \cdot a = a)$;
- 3) $(\forall a \in G)(\exists a^{-1} \in G)(a \cdot a^{-1} = a^{-1} \cdot a = e)$.

Если, кроме того, операция \cdot коммутативна, то группа G называется абелевой или коммутативной.

Определение 2. *Подгруппой* группы $G = (G, \cdot)$ называется такое подмножество H группы G , которое само является группой относительно бинарной операции \cdot , заданной в G .

Определение 3. Множество K называется *ассоциативным кольцом*, если на нем определены две бинарные операции $+$ (сложение) и \cdot (умножение), обладающие следующими свойствами:

- 1) $(\forall a, b \in K)(a + b = b + a)$;
- 2) $(\forall a, b, c \in K)(a + (b + c) = (a + b) + c)$;
- 3) $(\forall a \in K)(\exists (-a) \in K)(a + (-a) = 0)$;
- 4) $(\forall a, b, c \in K)(a(bc) = (ab)c)$;
- 5) $\begin{cases} (\forall a, b, c \in K)((a + b)c = ac + bc) \\ (\forall a, b, c \in K)(c(a + b) = ca + cb). \end{cases}$

Определение 4. Если для умножения выполняется закон коммутативности $((\forall a, b \in K)(ab = ba))$, то множество K называется *коммутативным кольцом*.

Определение 5. Элемент e кольца K называется *идемпотентным* элементом, если $e^2 = e$.

0 – всегда идемпотентный.

Определение 6. Элемент r кольца K называется *нильпотентным*, если существует такое натуральное число n , для которого произведение любых n элементов кольца равно нулю.

Определение 7. *Поле* называется коммутативное кольцо P , содержащее не менее двух элементов, в котором все ненулевые элементы образуют группу по умножению.

Поле P является конечным, если число элементов в нем конечно. Любое конечное поле характеристики p состоит из p^n элементов для некоторого n . Конечные поля, содержащие p^n элементов, называются полями *Галуа* и обозначаются $GF(p^n)$.

Определение 8. *Характеристикой* поля P называется наименьшее положительное число p , при котором в поле выполнено равенство $p \cdot 1 = 0$.

Определение 9. *Векторным пространством* над полем P называется множество V , если для любых $\alpha, \beta \in P$ и $u, v \in V$ справедливы следующие аксиомы:

- 1) $\alpha(u + v) = \alpha u + \alpha v$;
- 2) $(\alpha + \beta)u = \alpha u + \beta u$;
- 3) $(\alpha\beta)u = \alpha(\beta u)$;
- 4) $1 \cdot u = u$.

Определение 10. [1]. *Алгеброй* над полем P называется множество A , на котором определены две бинарные операции $+$ и \cdot , а также операция умножения элементов из P на элементы из A (то есть отображение $P \times A \rightarrow A$), удовлетворяющее следующим условиям:

- 1) $(A, +, \cdot)$ – кольцо;
- 2) $(A, +)$ – векторное пространство над полем P ;
- 3) $(\forall \alpha \in P)(\forall a, b \in A)((\alpha a)b = \alpha(ab) = a(\alpha b))$.

Определение 11. Подмножество S алгебры A над полем F называется *подалгеброй* алгебры, если относительно операций, определенных в A , S – само является алгеброй над полем F .

Признак подалгебры: непустое подмножество S алгебры A над полем F тогда и только тогда является подалгеброй в A , когда выполнены следующие условия:

- 1) $(\forall a, b \in S)((a - b) \in S)$;
- 2) $(\forall a, b \in S)(ab \in S)$;
- 3) $(\forall \alpha \in F)(\forall a \in S)(\alpha a \in S)$. [5].

1.2. Пирсовские разложения колец

Пусть R – коммутативное кольцо, e – нулевой идемпотентный элемент. Определим два множества:

- 1) $eR = \{ex | x \in R\} \neq \emptyset$.
- 2) $(1 - e)R = \{x - ex | x \in R\} \neq \emptyset$.

Докажем, что eR и $(1 - e)R$ – подкольца в R .

Доказательство: по признаку подкольца (применим к непустым подмножествам).

- 1) $\forall a, b \in S, ((a - b) \in S)$;
- 2) $\forall a, b \in S, (ab \in S)$.

Пусть $S = eR, a = ex_1, b = ex_2$.

- 1) $a - b = e(x_1 - x_2) \in eR$;
- 2) $ab = ex_1ex_2 = e^2x_1x_2 = e(ex_1x_2) \in eR$.

Пусть $S = (1 - e)R, a = (1 - e)x_1, b = (1 - e)x_2$.

- 1) $a - b = x_1 - x_2 - e(x_1 - x_2) = (1 - e)(x_1 - x_2) \in (1 - e)R$;
- 2) $ab = (1 - e)x_1(1 - e)x_2 = (1 - e)((1 - e)x_1x_2) \in (1 - e)R$.

Докажем, что $eR + (1 - e)R = R$.

Пусть $x \in R$. Тогда $x = ex + (1 - e)x = ex + x - ex = x$.

Значит, $R \subseteq eR + (1 - e)R$. Так как $eR, (1 - e)R \subseteq R$, то $eR + (1 - e)R = \{ex + (1 - e)y = ex + y - ey | x, y \in R\} \subseteq R$.

Убедиться в том, что $eR \cap (1 - e)R = \{0\}$.

Пусть $a \in eR \cap (1 - e)R$. Тогда существуют $x, y \in R$ такие, что

$$a = ex = (1 - e)y$$

$$ea = e(ex) = e(1 - e)y = e(y - ey) = ey - ey = 0$$

Получаем $a = 0$.

Обозначим: $eR + (1 - e)R = eR \oplus (1 - e)R$ – прямая сумма двух подколец.

Таким образом, имеем $R = eR \oplus (1 - e)R$ – пирсовское разложение коммутативного кольца R по идемпотенту e .

Для любых $a \in eR$, $ea = a$, e – единичный элемент в подкольце. Для любого $c \in (1 - e)R$, $ec = 0$.

Значит, если $x \in eR$, а $y \in (1 - e)R$, то $e(x + y) = x$, получаем $xy = 0$.

Пусть R – некоммутативное кольцо, e – идемпотентный элемент.

Тогда, если e – не единица, то имеет место двустороннее пировское разложение: $R = eRe \oplus eR(1 - e) \oplus (1 - e)Re \oplus (1 - e)R(1 - e)$,

$$a \in eRe, b \in eR(1 - e), c \in (1 - e)Re, d \in (1 - e)R(1 - e),$$

$$ba = 0, ab \in eR(1 - e),$$

$$ac = 0, ca \in (1 - e)Re,$$

$$ad = da = 0,$$

$$b^2 = 0, c^2 = 0.$$

1.3. Изоморфизм алгебр.

Определение 12. Пусть A и A' – алгебры над полем P . *Изоморфизмом* алгебры A на алгебру A' назовем биективное отображение φ множества A на множество A' , удовлетворяющее следующим условиям:

$$1) (\forall a, b \in A)(\varphi(a + b) = \varphi(a) + \varphi(b));$$

$$2) (\forall a, b \in A)(\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b));$$

$$3) (\forall \alpha \in P)(\forall a \in A) (\varphi(\alpha a) = \alpha(\varphi(a))).$$

Определение 13. Рангом алгебры A называется размерность векторного пространства над полем P .

Теорема 1. Любая алгебра с единицей ранга n над полем P изоморфна некоторой подалгебре алгебры $M_n(P)$.

Доказательство. Пусть A – алгебра ранга n над полем P . Для любого элемента a из A определим отображение $\varphi_a: A \rightarrow A$ следующим образом: $(\forall x \in A)(\varphi_a(x) = xa)$ и докажем, что φ_a – линейное отображение. Действительно:

$$1) (\forall x, y \in A)(\varphi_a(x + y) = (x + y)a = xa + ya = \varphi_a(x) + \varphi_a(y));$$

$$2) (\forall x \in A)(\forall \alpha \in P) (\varphi_a(\alpha x) = (\alpha x)a = \alpha(xa) = \alpha(\varphi_a(x))).$$

Заметим, что $\varphi_{a+b} = \varphi_a + \varphi_b$, $\varphi_{ab} = \varphi_a \varphi_b$ и $\varphi_{\alpha a} = \alpha \varphi_a$.

Пусть Φ_n – алгебра линейных операторов векторного пространства A .

Зададим теперь отображение $\psi: A \rightarrow \Phi_n$ по следующему правилу: $(\forall a \in A)(\psi(a) = \varphi_a)$ и докажем, что ψ – инъективный гомоморфизм. Действительно, пусть $(a, b \in A)$ и $\psi(a) = \psi(b)$. Тогда $\varphi_a = \varphi_b$, то есть $(\forall x \in A)(\varphi_a(x) = \varphi_b(x))$. Это означает, что $xa = xb$. Подставляя в это равенство единичный элемент e алгебры A , получим: $a = b$. Следовательно ψ – инъективное отображение.

Пусть $a, b \in A, \alpha \in P$. Тогда:

$$1) \psi(a + b) = \varphi_{a+b} = \varphi_a + \varphi_b;$$

$$2) \psi(ab) = \varphi_{ab} = \varphi_a \varphi_b;$$

$$3) \psi(\alpha a) = \varphi_{\alpha a} = \alpha \varphi_a.$$

Следовательно, ψ – гомоморфизм. Пусть $\psi(A)$ – гомоморфный образ алгебры A . Тогда, во-первых, $\psi(A) \cong A$, а во-вторых, $\psi(A)$ – подалгебра алгебры Φ_n . Учитывая теперь то, что, $\Phi_n \cong M_n(P)$ получим то, что и требовалось доказать. [5].

1.4. Понятие решетки

Самыми удобными объектами для знакомства с прикладными аспектами алгебры являются решетки. Решетки могут быть определены, как упорядоченные особым образом множества, а их упорядоченность может быть изучена с помощью алгебраических методов.

Определение 14. [4]. Непустое множество с определенным на нем отношением частичного порядка называется *частично упорядоченным множеством*

Определение 15. [4]. Частично упорядоченное множество (P, \leq) называется *линейно упорядоченным* или *цепью*, если \leq – отношение линейного порядка.

Определение 16. *Отношением линейного порядка* называется бинарное отношение \leq на множестве P , если:

- 1) \leq является отношением частичного порядка;
- 2) $(\forall x, y \in P)((x \leq y) \vee (y \leq x))$.

Определение 17. *Решеткой* называется частично упорядоченное множество, в котором каждое двухэлементное подмножество имеет нижнюю и верхнюю грани, то есть имеет наименьший элемент во множестве верхних границ и наибольший элемент во множестве нижних границ.

Определение 18. *Полной решеткой* называется частично упорядоченное множество, в котором каждое подмножество имеет нижнюю и верхнюю грани.

Примечание: любая полная решетка имеет 0 и 1.

Можно сделать вывод, что любая полная решетка является решеткой, но, в тоже время, обратное утверждение неверно. Заметим, что если L – полная решетка, то $\sup L$ – наибольший элемент, а $\inf L$ – наименьший элемент в L .

Если решетку рассматривать, как алгебру, то можно сформулировать еще одно определение, эквивалентное определению 17.

Определение 19. Решеткой называется непустое множество L с определенными на нем двумя бинарными операциями \vee (решеточное объединение) и \wedge (решеточное пересечение), удовлетворяющими условиям идемпотентности, коммутативности, ассоциативности и свойству поглощения соответственно:

- 1) $(\forall a \in L)(a \vee a = a, a \wedge a = a)$;
- 2) $(\forall a, b \in L)(a \vee b = b \vee a, a \wedge b = b \wedge a)$;
- 3) $(\forall a, b, c \in L)(a \vee (b \vee c) = (a \vee b) \vee c, a \wedge (b \wedge c) = (a \wedge b) \wedge c)$;
- 4) $(\forall a, b \in L)(a \vee (a \wedge b) = a, a \wedge (a \vee b) = a)$.

Пусть (L, \wedge, \vee) – произвольная решетка и $a, b, c, d \in L$. Тогда истинны следующие свойства:

- 1) $(a \wedge b \leq a) \& (a \leq a \vee b)$;
- 2) $(a \leq b \Leftrightarrow (a \wedge b = a))$;
- 3) $(a \leq b \Rightarrow (c \wedge a \leq c \wedge b) \& (c \vee a \leq c \vee b))$; – свойство изотонности
- 4) $((a \leq b) \& (a \leq c) \Rightarrow (a \leq b \wedge c) \& (a \leq b \vee c))$;
- 5) $((a \leq c) \& (b \leq c) \Rightarrow (a \wedge b \leq c) \& (a \vee b \leq c))$;
- 6) $((a \leq b) \& (c \leq d) \Rightarrow (a \wedge c \leq b \wedge d) \& (a \vee c \leq b \vee d))$;
- 7) $(a \wedge b < a) \Leftrightarrow (a \vee b > b)$;
- 8) $(a \wedge b = a \vee b) \Leftrightarrow (a = b)$;
- 9) $\left. \begin{array}{l} (a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)) \\ ((a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)) \end{array} \right\}$ – неравенства дистрибутивности;
- 10) $((a \leq c) \Rightarrow (a \vee (b \wedge c) \leq (a \vee b) \wedge c))$ – неравенство модулярности.

1.5. Диаграммы решеток

Рассматривая некоторое частично упорядоченное множество (P, \leq) можно сказать, что элементы a и b будут сравнимыми, если $(a \leq b)$ или $(b \leq a)$. Заметим, что элемент b *покрывает* элемент a , если выполнены следующие условия:

1) $(a < b)$;

2) $(\forall c \in P)((a \leq c) \wedge (c \leq b) \Rightarrow (c = a) \vee (c = b))$.

Для краткости введем следующее условное обозначение: «если b покрывает a », будем записывать в виде $a < b$. [4].

В некоторых случаях частично упорядоченное множество целесообразно изображать на плоскости в виде диаграмм. При этом необходимо учитывать следующие соглашения:

1) Различные элементы множества P изображаются различными точками плоскости;

2) Если $(a, b \in P)$ и b покрывает a , то точки, изображающие эти элементы, соединяются отрезком, причем точка, соответствующая b , располагается выше точки, соответствующей a . [4].

Рассмотрим примеры диаграмм:

Пример 1

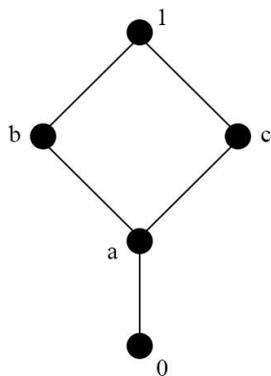


Рисунок 1

Пример 2

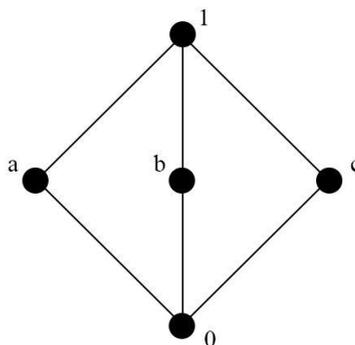


Рисунок 2

Пример 3

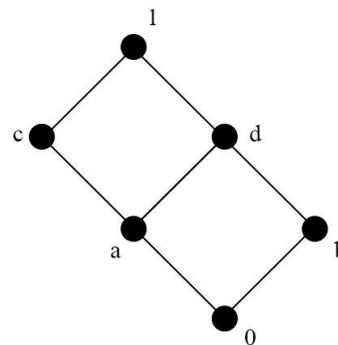


Рисунок 3

Глава II. Система компьютерной алгебры GAP

2.1. Краткая характеристика системы GAP

Разработка системы компьютерной алгебры GAP, название которой расшифровывается как «*Groups, Algorithms and Programming*», была начата в 1986 году. В настоящее время GAP является уникальным всемирным совместным научным проектом, объединяющим специалистов в области алгебры, теории чисел, математической логики, информатики и других наук из различных стран мира.

Система GAP является свободным, открытым пакетом программного обеспечения для вычислений в дискретной алгебре. Система "расширяемая", в ней возможно написание своих собственных программ на языке GAP, и использование их точно так же, как и программ, которые входят в состав системы ("библиотеки").

GAP был задуман как инструмент комбинаторной теории групп – раздела алгебры, изучающего группы, заданные порождающими элементами и определяющими соотношениями. В дальнейшем, с выходом каждой новой версии системы сфера ее применения охватывала все новые и новые разделы алгебры.

2.2. Язык программирования GAP

GAP распознает следующие символы: цифры, буквы (с учетом регистра), пробел, символы новой строки, а также специальные символы, из которых составляют слова для программного кода. Эти слова можно разделить на 5 категорий использования:

Таблица 1

№ п-п	Категории слов	Применение в GAP
1	Ключевые слова	and, do, elif, else, end, fi, for, function, if, in, local, mod, not, od, or, repeat, return, then, until, while, quit, QUIT, break, rec, continue.
2	Идентификаторы	Идентификаторы состоят из букв, цифр, символов

		подчеркивания <code>_</code> , и содержат не менее одной буквы или символа подчеркивания <code>_</code> . При этом регистр является существенным. Примеры идентификаторов: <code>a</code> , <code>world</code> , <code>x100</code> , <code>World</code> , <code>WORLD</code> , <code>100x</code> , <code>_100</code> и т.п.
3	Строки	Последовательность произвольных символов, заключенная в двойные кавычки
4	Целые числа	Последовательность цифр
5	Операторы и ограничители	– операторы сравнения: <code>=</code> , <code><></code> , <code><</code> , <code><=</code> , <code>></code> , <code>>=</code> ; – арифметические операторы: <code>+</code> , <code>-</code> , <code>*</code> , <code>/</code> , <code>mod</code> ; – логические операторы: <code>not</code> , <code>and</code> , <code>or</code> .

2.3. Алгебры в GAP

Пусть F — поле и A — алгебра над F . В GAP операция умножения над алгебрами ассоциативна. Любая алгебра всегда содержит нулевой элемент, который может быть получен, вычитанием произвольного элемента из самого себя. Элементы поля F не рассматриваются как элементы A .

Не все алгебры содержат мультипликативный нейтральный единичный элемент, но если алгебра содержит такой единичный элемент, то он единственен, при этом он не может быть получен из произвольного элемента a алгебры A как частное $\frac{a}{a}$ или как a^0 , так как эти операции могут быть не определены для алгебры A .

Можно инвертировать a или возвести его в нулевую степень, но A может быть не замкнуто относительно этих операций. Например, если a — квадратная матрица в GAP, тогда мы можем считать, что a^0 является единичной матрицей того же самого размера и над тем же самым полем, что и a .

С другой стороны, алгебра может иметь мультипликативный нейтральный элемент, который не равен нулевой степени элементов. Во многих случаях нулевая степень элементов алгебры правильно определена как элемент алгебры. Это справедливо, например, для всех тех матричных алгебр, чьи порождающие элементы являются порождающими элементами конечной группы, поэтому, полезно различить *общие* алгебры и *унитальные* алгебры.

Определение 20. [3]. *Унитальная алгебра* в GAP — алгебра U , которая содержит нулевую степень элементов, и в которой выполнимы все действия с этой степенью.

Не унитальная алгебра A может не содержать нулевые степени элементов или, наоборот содержать их, но тогда в ней невыполнимо какое-нибудь действие с этой степенью.

Итак, возможно рассматривать A как унитальную алгебру, используя $AsUnitalAlgebra(A)$, или используя $AsAlgebra(U)$.

Алгебра A может иметь унитальные подалгебры, и, конечно, алгебра U может иметь подалгебры, которые не являются унитальными. Следующий пример показывает главные различия между алгебрами и унитальными алгебрами.

```
gap> a:=[[1,0],[0,0]];
gap> alg1:= Algebra(Rationals,[a]);
      Algebra(Rationals,[[[1,0],[0,0]])
gap> id:=a^0;
      [[1,0],[0,1]]
gap> id in alg1;
      false
gap> alg2:= UnitalAlgebra(Rationals,[a]);
      UnitalAlgebra(Rationals,[[[1,0],[0,0]])
gap> id in alg2;
      true
gap> alg3:=AsAlgebra(alg2);
      Algebra(Rationals,[[[1,0],[0,0]],[[1,0],[0,1]])
gap> alg3 = alg2;
      true
gap>AsUnitalAlgebra(alg1);Error,<D>is not unital
```

Очевидно, что при необходимости наличия единичной матрицы в алгебре, о которой неизвестно является ли она унитальной, достаточно прибавить ее к порождающим элементам.

GAP различает алгебры и подалгебры алгебр.

Каждая подалгебра принадлежит уникальной основной алгебре, которую называют родителем подалгебры. Алгебраические действия,

совершаемые более чем с одной алгеброй, предполагают, что аргументы имеют общего родителя.

Возьмем, например, `Centralizer`. При этом должно быть два аргумента:

1. алгебра A и алгебра B , где A родительская алгебра и B — подалгебра этой родительской алгебры;
2. A и B — подалгебры общей родительской алгебры P .

В этих случаях `Centralizer` выдает централизатор B в A , который представлен как подалгебра общей родительской алгебры алгебр A и B .

Всякий раз, когда имеется две подалгебры, которые имеют различные родительские алгебры, но имеют и общую супералгебру A , можно использовать `AsSubalgebra` или `AsUnitalSubalgebra` для того, чтобы создать новые подалгебры, которые имеют общую родительскую алгебру A , например:

Algebra

`Algebra(U)` выдает родительскую алгебру A , которая изоморфна родительской алгебре или подалгебре U .

```
Algebra (F, gens)
```

`Algebra (F, gens, zero)` выдает родительскую алгебру над полем F и порожденную элементами алгебры в списке `gens`. Нулевой элемент этой алгебры может быть введен как `zero`; это необходимо всякий раз, когда `gens` пусто.

```
gap> a:=[[1]];
gap> alg:=Algebra(Rationals,[a]);
      Algebra(Rationals,[[[1]]])
gap> alg.name:= "alg";
gap> sub:= Subalgebra(alg,[]);
      Subalgebra(alg,[])
gap> Algebra(sub);
      Algebra(Rationals,[[[0]]])
```

```
gap> Algebra(Rationals, [], 0*a);
      Algebra(Rationals, [[[0]]]);
```

Алгебры, получаемые с помощью `Algebra`, не унитарны. Для построения унитарных алгебр необходимо использовать `UnitalAlgebra`.

Subalgebra

`Subalgebra (A, gens)` выдает подалгебру алгебры A , порожденную элементами в списке `gens`.

```
gap> a:=[[1,0],[0,0]];
gap> b:=[[0,0],[0,1]];
gap> alg:=Algebra(Rationals,[a,b]);
gap> alg.name:="alg";
gap> s:=Subalgebra(alg,[a]);
      Subalgebra(alg,[[[1,0],[0,0]])
gap> s=alg;
      false
gap> s:=UnitalSubalgebra(alg,[a]);
      UnitalSubalgebra(alg,[[[1,0],[0,0]])
gap> s=alg;
      true
```

Помимо вышеперечисленных функций, в GAP к алгебрам можно применять теоретико-множественные функции, например `Intersection` и `Size`, не смотря на то, что они не предназначены к работе исключительно с алгебрами. Рассмотрим некоторые из таких функций:

Таблица 2

Функция	Результат ее применения в алгебре
<code>Elements(A);</code>	вычисляет элементы алгебры A с использованием алгоритма <code>Dimino</code> . Заданная по умолчанию для алгебр функция вычисляет базис линейного пространства в то же самое время.
<code>Intersection(A, H);</code>	выдает пересечение A и H в виде множества элементов или как алгебраическую запись (запись

	алгебры).
<code>IsSubset(A, H);</code> или <code>DomainOps.IsSubset.</code>	Если A и H — алгебры, то <code>IsSubset</code> проверяет являются ли генераторы H элементами A
<code>Random(A);</code>	выдает произвольный элемент алгебры A . Это требует вычисления базиса линейного пространства.

С помощью GAP могут быть проверены некоторые свойства алгебр.

`IsAbelian(A)` выдается *true* если алгебра A абелева и *false* в противном случае.

`IsCentral(A, U)` выдается *true* если алгебра A централизует алгебру U и *false* в противном случае.

`IsFinite(A)` выдается *true* если алгебра A конечна, и *false* в противном случае.

`IsTrivial(A)` выдается *true* если алгебра A состоит только из нулевого элемента, и *false* в противном случае. Если A — унитарная алгебра, то, конечно, она никогда не тривиальна.

Все критерии ожидают родительскую алгебру или подалгебру и выдают *true*, если алгебра имеет свойство и *false* в противном случае. Некоторые функции не могут выполняться, если данная алгебра имеет бесконечное множество элементов. В таких случаях может быть напечатано предупреждение.

```
gap> IsAbelian(FreeAlgebra(GF(2), 2));
false
gap> a:=UnitalAlgebra(Rationals, [[[1, 0], [0, 0]]]);
UnitalAlgebra(Rationals, [[[1, 0], [0, 0]]])
gap> a.name:="a";
gap> s1:=Subalgebra(a, [One(a)]);
Subalgebra(a, [[[1, 0], [0, 1]]])
gap> IsCentral(a, s1);
IsFinite(s1);
true
```

```

false
gap> s2:=Subalgebra(a, []);
Subalgebra(a, [])
gap> IsFinite(s2);
IsTrivial(s2);
true
true

```

В GAP алгебра — линейное пространство, и функции линейного пространства типа Base и Dimension применимы к алгебрам.

```

gap> a:=UnitalAlgebra(Rationals, [[[1,0],[0,0]]]);
UnitalAlgebra(Rationals, [[[1,0],[0,0]]])
gap> Dimension(a);
gap> Base(a);
[[[1,0],[0,1]],[[0,0],[0,1]]] [6].

```

Структура линейного пространства используется также теоретико-множественными функциями.

Алгебраические функции вычисляют некоторые подалгебры данной алгебры, например, Centre вычисляет центр алгебры. Некоторые функции не могут завершиться, если данная алгебра имеет бесконечное множество элементов, в то время как другие функции могут сообщить об ошибке в таких случаях.

В GAP каждая алгебра является или родительской алгеброй или подалгеброй единственной родительской алгебры. Если вычисляется центр C алгебры U с родительской алгеброй A , то C — подалгебра U , но ее родительская алгебра есть A .

Centralizer (A, x) и Centralizer(A, U) выдают централизатор элемента x в A , где x должен быть элементом родительской алгебры A , соответственно централизатор алгебры U в A , где обе алгебры должны иметь общего родителя.

Централизатор элемента x в A определен как множество C элементов c из A , таких, что c и x коммутируют. [7].

Централизатор алгебры U в A определен как множество C элементов c из A , таких, что c коммутирует с каждым элементом U .

```
gap> a:=MatAlgebra(GF(2),2);;
gap> a.name:="a";;
gap> m:=[[1,1],[0,1]]*Z(2);;
gap> Centralizer(a,m);
      UnitalSubalgebra(a,[[[Z(2)^0,0*Z(2)],[0*Z(2),Z(2)
^0]],[[0*Z(2),Z(2)^0],[0*Z(2),0*Z(2)]]])
Centre(A) ## выдает центр A (то есть централизатор A в A)
gap> c:=Centre(a);
      UnitalSubalgebra(a,[[[Z(2)^0,0*Z(2)],[0*Z(2),Z(2)
^0]]])
```

Глава III. Типовая классификация подалгебр четырехмерной алгебры матриц $M(GF(2),3)$

Для классификации подалгебр был создан массив матриц алгебры $A=M(GF(2),3)$, состоящий из всех матриц размером 3×3 , из двух элементов: 0 и 1 [Приложение 1.]. В массиве A всего 512 элементов, из которых 57 являются идемпотентными, 21 элемент является нильпотентным. Выберем два идемпотентных элемента и два нильпотентных элемента. Зададим умножение, основываясь на пирсовское разложение алгебры, найдем в алгебре все подалгебры с заданным базисом и таблицей умножения и проведем исследование полученных подалгебр.

Создадим программу построения четырехмерной подалгебры с заданной таблицей умножения:

	e_i	e_j	r_k	r_l
e_i	e_i	0	r_k	r_l
e_j	0	e_j	0	0
r_k	0	r_k	0	0
r_l	0	0	0	0

Таблица 3

Программа №1, создающая подалгебры	
<code>eerr:=[];</code>	# Создание каталога для размещения подалгебр
<code>Sub:=[];</code> <code>b:=0;</code>	# Создание массива sub и переменной b
<code>ID:=[2,4,6,8,10,17,18,19,22,25,46,49,50,54,55,57,66,74,82,122,145,146,147,152,196,210,217,239,257,258,260,261,266,273,274,275,277,279,281,289,290,293,296,298,317,</code>	# Массив номеров идемпотентных матриц

<pre>321, 337, 345, 361, 385, 386, 388 , 391, 449, 458, 467, 512];</pre>	
<pre>NI := [3, 5, 7, 9, 28, 33, 37, 41, 64 , 65, 73, 129, 131, 193, 220, 326, 366, 433, 439, 456, 505];</pre>	<pre># Массив номеров нильпотентных матриц</pre>
<pre>A := MatAlgebra (GF(2), 3);</pre>	<pre># Построение алгебры матриц четвертого порядка над полем GF(2)</pre>
<pre>E1 := Elements (A);</pre>	<pre># Создание массива элементов алгебры A</pre>
<pre>for i in ID do for j in ID do for k in NI do for l in NI do</pre>	<pre># Начало цикла построения подалгебр</pre>
<pre> if j > i and l > k and E1[i] * E1[j] = E1[1] and E1[j] * E1[i] = E1[1] and E1[i] * E1[k] = E1[k] and E1[k] * E1[i] = E1[1] and E1[i] * E1[l] = E1[1] and E1[l] * E1[i] = E1[1] and E1[j] * E1[k] = E1[1] and E1[k] * E1[j] = E1[k] and E1[j] * E1[l] = E1[1] and E1[l] * E1[j] = E1[1] and E1[l] * E1[k] = E1[1] and E1[k] * E1[l] = E1[1] then</pre>	<pre># Если выполняется, то строится подалгебра B</pre>
<pre> B := Subalgebra (A, [E1[i], E1[j], E1[k], E1[l]]);</pre>	<pre># Записывает подалгебру алгебры A порожденную элементами E1[i], E1[j], E1[k], E1[l] в B</pre>

<code>sub:=Elements(B);</code>	# Кладем в массив sub элементы подалгебры B
<code>AddSet(Sub, sub);</code>	#Присоединение элемента sub к массиву Sub
<code>if Size(Sub) > b then Add(eerr, [i, j, k, l]);</code>	# Сравниваем размер массива Sub с b. Если размер больше, то записываем в массив eerr
<code>b:=Size(Sub);</code>	# Присваиваем b размер массива sub
<code>fi; fi;</code>	#Окончание работы условного оператора
<code>od; od; od; od;</code>	#Конец цикла
<code>Sort(eerr);</code>	# Упорядочиваем элементы массива eerr
<code>PrintTo("nom1.dan", "eerr:=" , eerr, ";", "\n", " eerr =", Size(eerr), "\n");</code>	#Печать результата в файл nom1.dan

Результатом работы этой программы является массив, который находится в файле nom1.dan. Распечатаем этот файл.

```
eerr:= [[2,17,3,5], [2,145,3,7], [2,289,5,7], [10,25,28,37], [10,217,28,64],
[10,289,37,64], [17,66,9,41], [17,261,33,41], [66,145,131,456], [66,361,326,456],
[74,217,220,439], [74,361,366,439], [145,391,433,505], [147,196,220,366]];
```

```
|eerr|=14
```

Любой элемент массива eerr состоит из четверок номеров базисных элементов алгебры. Таких четверок всего получено 14, это значит, что в алгебре A содержится 14 подалгебр изоморфных подалгебре S_1 .

Выполним дальнейшее исследование полученных четверок:

Вычислим тип подалгебры.

Составим программу, которая будет использована для вычисления типа каждой подалгебры.

Программа № 2, определяющая тип на множестве подалгебр алгебры $M(GF(2),3)$	
<code>tip:=function(a,b,c,d)</code>	#Задаем функцию
<code> local</code>	#Создаем локальные переменные
<code> A, El, i, j, k, w, sub,</code> <code> tip, S, s, el, l;</code>	#Имена переменных
<code> sub:=[];</code>	#Задаем пустой массив sub
<code> tip:=[];</code>	#Задаем пустой массив tip
<code> A:=MatAlgebra(GF(2),3);</code>	#Создание алгебры матриц
<code> El:=Elements(A);</code>	#Построение массива элементов
<code> S:=Subalgebra(A,[El[a],El[b]</code> <code>],El[c],El[d]));</code>	#Построение подалгебры
<code> for i in S do</code>	#Начало цикла
<code> for k in S do</code>	#Начало цикла
<code> for j in S do</code>	#Начало цикла
<code> for w in S do</code>	#Начало цикла
<code> s:=Subalgebra(A,[i,j,k,w]);</code>	#Построение подалгебры
<code> AddSet(sub,Elements(s));</code>	#Построение массива элементов и добавление его в массив sub
<code> od;</code>	#Закрытие цикла
<code> for l in [1..Size(sub)] do</code>	#Начало цикла
<code> Add(tip,Size(sub[l]));</code>	#Добавление порядка каждого элемента в массив tip
<code> od;</code>	#Закрытие цикла
<code>tip:=Collected(tip);</code>	#Считаем количество элементов каждого порядка и сохраняем их в tip
<code>PrintTo("tip.txt","a=</code> <code> ",a,";", " b= ",b,";", " c=</code> <code> ",c,";", " d=</code> <code> ",d,"", "\n",tip);</code>	#Распечатываем результаты в файл tip.txt
<code>end;</code>	#Конец функции

Для запуска программы необходимо набрать команду `tip(2,145,3,7)`, где `(2,145,3,7)` – любая из четверок, полученных в программе № 1. GAP сохранит посчитанный файл под названием `tip.txt`.

Результат работы программы № 2 следующий:

`a=2; b=145; c=3; d=7;`

[1,1], [2,11], [4,17], [8,7], [16,1].

Такой тип означает, что в алгебре содержится 1 подалгебра порядка 1 ([1,1]), 11 подалгебр порядка 2 ([2,12]), 17 подалгебр порядка 4 ([4,17]), 7 подалгебр порядка 8 ([8,7]) и 1 подалгебра 16-го порядка ([16,1]).

Определим отношение покрытия.

Таблица 5

Программа № 3 определяющая отношение покрытия на множестве подалгебр алгебры $M(GF(2),3)$	
<code>покр:=function(a,b,c,d)</code>	#Задание функции
<code>local</code>	#Задание переменных
<code>A, El, i, j, k, w, sub, tip, S, s, s1, el, l, l1, m, m1, n, n1, i1;</code>	#Имена переменных
<code>sub:=[];</code>	#Создаем массив sub
<code>for i1 in [1..9] do</code>	#Начало цикла
<code>sub[i1]:=[];</code>	#Создаем в массиве sub 9 пустых массивов
<code>od;</code>	#Конец цикла
<code>покр:=[];</code>	#Создание массива покр
<code>A:=MatAlgebra(GF(2),3);</code>	#Создание алгебры
<code>El:=Elements(A);</code>	#Построение массива элементов
<code>S:=Subalgebra(A,[El[a],El[b], El[c],El[d]]);</code>	#Записывает подалгебру алгебры A порожденную элементами El[a], El[b], El[c] в S
<code>for i in S do</code>	#Начало цикла
<code>for k in S do</code>	#Начало цикла
<code>for j in S do</code>	#Начало цикла
<code>for w in S do</code>	#Начало цикла
<code>s1:=Subalgebra(S,[i,k,j,w]);</code>	#Записывает подалгебру алгебры S порожденную элементами i,k,j в s1
<code>if Size(s1)=1 then</code>	#Проверяет размер. Если равен 1
<code>AddSet(sub[1],Elements(s1));</code>	#Записывает в 1-й массив
<code>fi;</code>	#Закрывает проверку условия
<code>if Size(s1)=2 then</code>	#Если размер равен 2
<code>AddSet(sub[2],Elements(s1));</code>	#Записывает во 2-й массив
<code>fi;</code>	#Закрывает проверку условия
<code>if Size(s1)=4 then</code>	#Если размер равен 4
<code>AddSet(sub[3],Elements(s1));</code>	#Записывает в 3-й массив

fi;	#Закрывает проверку условия
if Size(s1)=8 then	#Если размер равен 8
AddSet(sub[4],Elements(s1));	#Записывает в 4-й массив
fi;	#Закрывает проверку условия
if Size(s1)=16 then	#Если размер равен 16
AddSet(sub[5],Elements(s1));	#Записывает в 5-й массив
fi;	#Закрывает проверку условия
if Size(s1)=32 then	#Если размер равен 32
AddSet(sub[6],Elements(s1));	#Записывает в 6-й массив
fi;	#Закрывает проверку условия
if Size(s1)=64 then	# Если размер равен 64
AddSet(sub[7],Elements(s1));	#Записывает в 7-й массив
fi;	#Закрывает проверку условия
if Size(s1)=128 then	#Если размер равен 128
AddSet(sub[8],Elements(s1));	#Записывает в 8-й массив
fi;	#Закрывает проверку условия
if Size(s1)=512 then	#Если размер равен 512
AddSet(sub[9],Elements(s1));	#Записывает в 9-й массив
fi;	#Закрываем проверку условия
od;	#Закрытие цикла
for m1 in [1..Size(sub)] do	#Открытие цикла
for l1 in [1..Size(sub[m1])] do	#Открытие цикла
do	
for n1 in [1..Size(sub[m1+1])] do	#Открытие цикла
if IsSubset(sub[m1+1][n1],sub[m1][l1]) = true	#Проверяет являются ли генераторы sub[m1][l1] элементами sub[m1+1][n1],
then	#если да, то записывает в pokr
Add(pokr,[[m1,l1],[m1+1,n1]]);	
fi;	#Закрытие проверки условия
od;	#Конец цикла
od;	#Конец цикла
od;	#Конец цикла
PrintTo("pokr.txt",pokr,"\n");	#Распечатываем массив pokr в файл pokr.txt
end;;	#Конец функции

Для запуска программы необходимо набрать команду $\text{rokr}(2,145,3,7)$, где $(2,145,3,7)$ – любая из четверок, полученных в программе № 1. GAP сохранит посчитанный файл под названием rokr.txt .

Результат работы программы № 3 следующий:

[[[1,1],[2,1]], [[1,1],[2,2]], [[1,1],[2,3]], [[1,1],[2,4]], [[1,1],[2,5]], [[1,1],[2,6]],
 [[1,1],[2,7]], [[1,1],[2,8]], [[1,1],[2,9]], [[1,1],[2,10]], [[1,1],[2,11]], [[2,1],[3,1]],
 [[2,1],[3,2]], [[2,1],[3,3]], [[2,1],[3,4]], [[2,2],[3,1]], [[2,2],[3,5]], [[2,2],[3,6]],
 [[2,2],[3,7]], [[2,2],[3,8]], [[2,2],[3,9]], [[2,3],[3,1]], [[2,3],[3,10]], [[2,3],[3,11]],
 [[2,3],[3,12]], [[2,4],[3,2]], [[2,4],[3,5]], [[2,4],[3,10]], [[2,5],[3,2]], [[2,5],[3,6]],
 [[2,5],[3,11]], [[2,5],[3,13]], [[2,6],[3,3]], [[2,6],[3,5]], [[2,6],[3,11]], [[2,6],[3,14]],
 [[2,6],[3,15]], [[2,6],[3,16]], [[2,7],[3,3]], [[2,7],[3,6]], [[2,7],[3,10]], [[2,7],[3,17]],
 [[2,8],[3,4]], [[2,8],[3,7]], [[2,8],[3,14]], [[2,8],[3,17]], [[2,9],[3,4]], [[2,9],[3,8]],
 [[2,9],[3,12]], [[2,9],[3,15]], [[2,10],[3,7]], [[2,10],[3,12]], [[2,10],[3,13]],
 [[2,10],[3,16]], [[2,11],[3,9]], [[2,11],[3,13]], [[2,11],[3,15]], [[2,11],[3,17]],
 [[3,1],[4,1]], [[3,1],[4,2]], [[3,2],[4,1]], [[3,3],[4,1]], [[3,3],[4,3]], [[3,4],[4,2]],
 [[3,4],[4,3]], [[3,5],[4,1]], [[3,5],[4,4]], [[3,5],[4,5]], [[3,6],[4,1]], [[3,6],[4,6]],
 [[3,7],[4,2]], [[3,7],[4,4]], [[3,7],[4,6]], [[3,8],[4,2]], [[3,8],[4,5]], [[3,9],[4,5]],
 [[3,9],[4,6]], [[3,10],[4,1]], [[3,11],[4,1]], [[3,11],[4,7]], [[3,12],[4,2]], [[3,12],[4,7]],
 [[3,13],[4,6]], [[3,13],[4,7]], [[3,14],[4,3]], [[3,14],[4,4]], [[3,15],[4,3]], [[3,15],[4,5]],
 [[3,15],[4,7]], [[3,16],[4,4]], [[3,16],[4,7]], [[3,17],[4,3]], [[3,17],[4,6]], [[4,1],[5,1]],
 [[4,2],[5,1]], [[4,3],[5,1]], [[4,4],[5,1]], [[4,5],[5,1]], [[4,6],[5,1]], [[4,7],[5,1]]]

В данном примере рассматривается подалгебра, порожденная матрицами с номерами 2, 145, 3, 7. Эта подалгебра имеет тип $[[1,1], [2,11], [4,17], [8,7], [16,1]]$. Все подалгебры в решетке распределены по пяти уровням. На каждом уровне алгебры имеют двойные номера, например, номер $[3,9]$ означает, что 3 – номер уровня, а 9 – порядковый номер подалгебры на третьем уровне. Таким образом, запись $[[3,9],[4,7]]$ означает, что подалгебра с номером $[3,9]$ покрывается подалгеброй с номером $[4,7]$ в решетке подалгебр.

Дальнейшее исследование заключается в *построении диаграммы решетки*

Используя полученную ранее информацию, можно выполнить построение диаграммы решетки подалгебры. Построение осуществляется в два шага.

1. Изображение подалгебры алгебры S кружочками (точками).
2. Изображение отношения покрытия, соединяя элементы отрезком.

В результате имеем решетку:

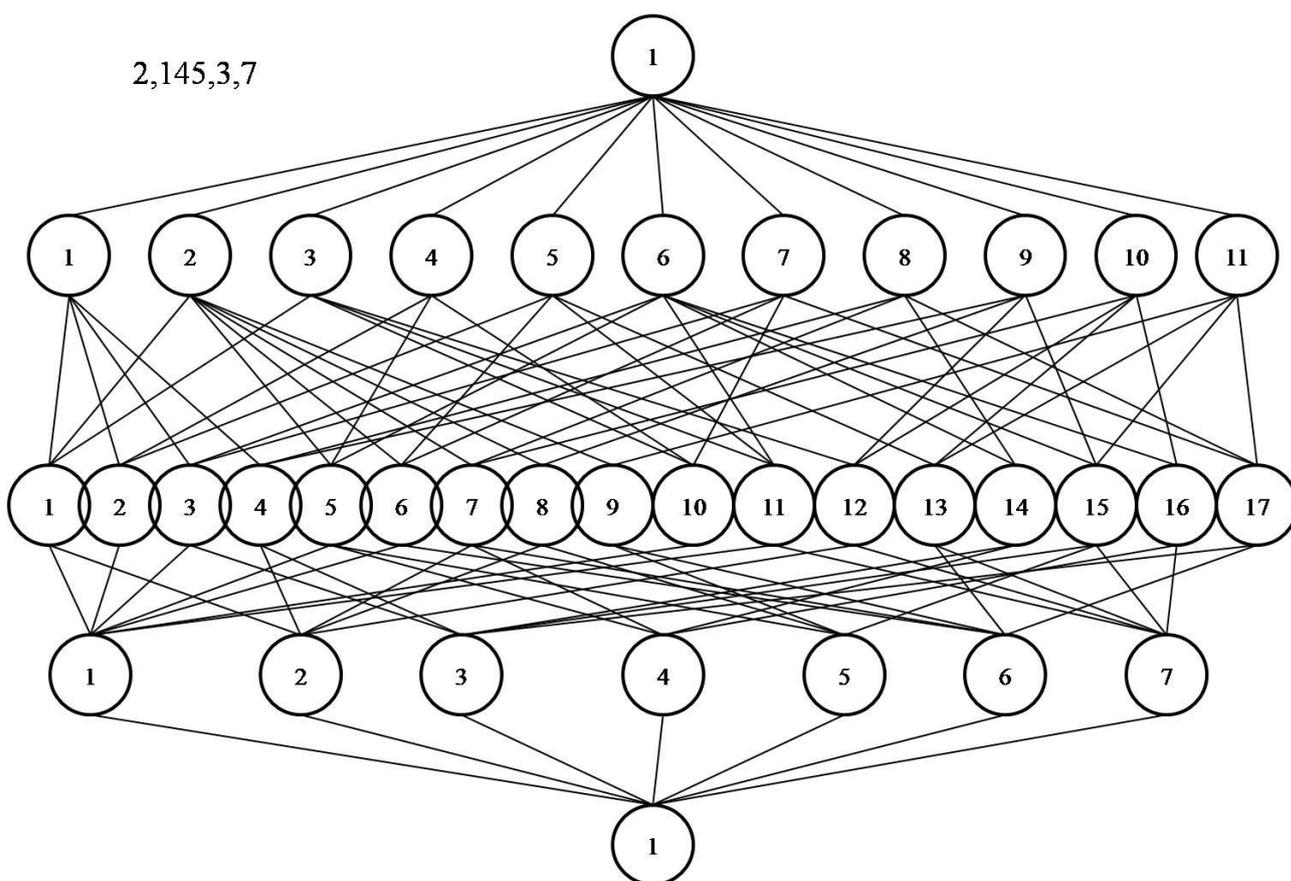


Рисунок 4

Для каждого элемента массива $еегг$ найдено отношение покрытия, построена диаграмма. Результат представлен в таблице 6 [Приложение 2.].

Для дальнейшей классификации необходимо повторить весь этап исследования подалгебр, с теми же массивами ID и NI , но с другой таблицей умножения. Для этого составлена программа № 4, для отыскания других образующих четверок [Приложение 3.].

Результатом работы программы № 4 является массив $eerr = [[2,17,9,65], [2,49,9,73], [2,385,65,73], [4,19,28,193], [4,55,28,220], [4,385,193,220], [6,17,41,326], [6,49,41,366], [6,391,326,366], [8,19,64,456], [8,55,64,505], [8,391,456,505], [17,321,129,131], [49,361,433,439]]$;

$$|eerr|=14$$

Проведем исследование данного массива: найдем покрытие каждой четверки, составим их диаграммы. Результат представлен в таблице 8. [Приложение 4.]

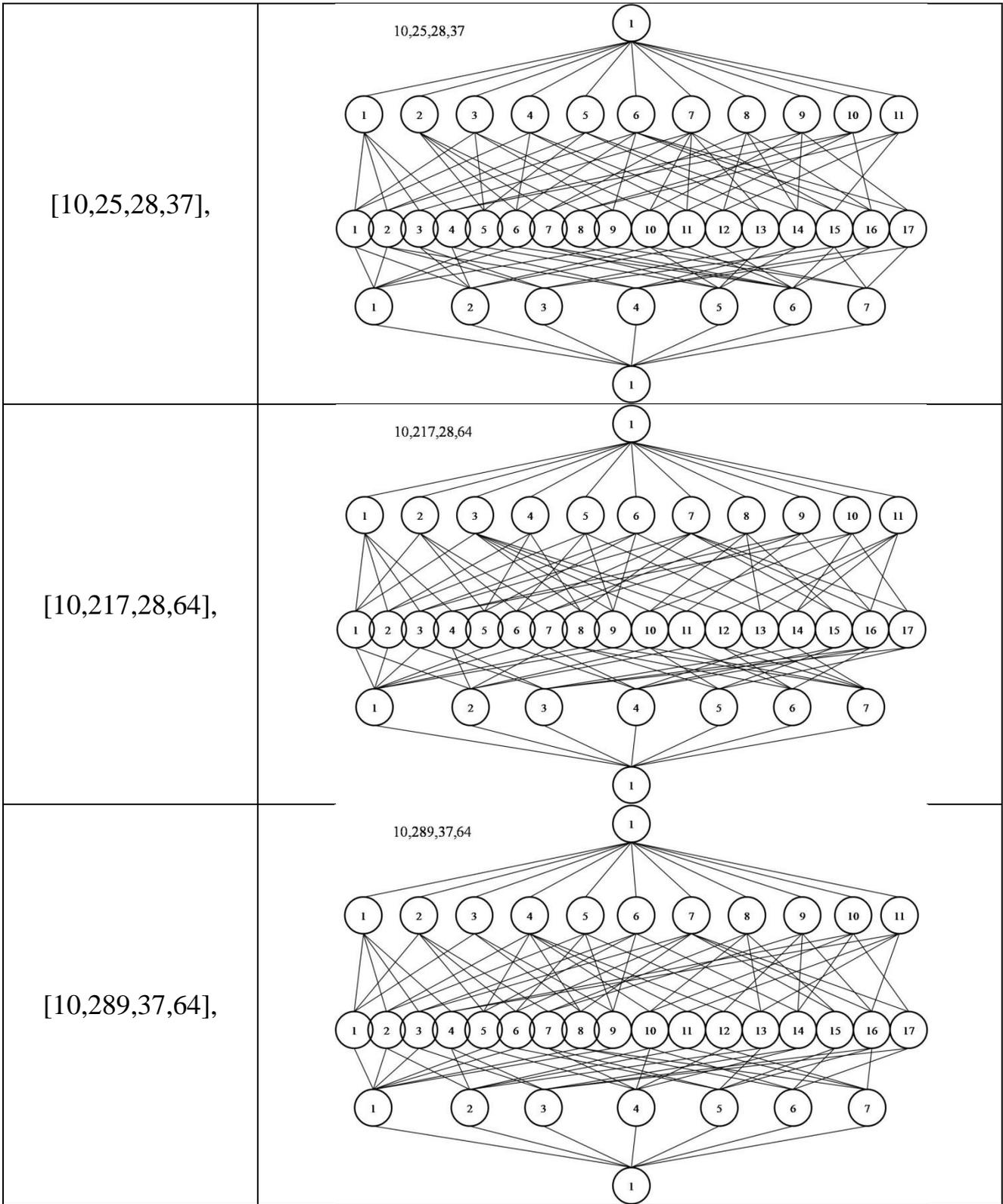
Анализируя результаты двух исследований, очевидно, что все четверки имеют одинаковый тип (1,11,17,7,1), значит, проводить классификацию можно учитывая только отношение покрытия.

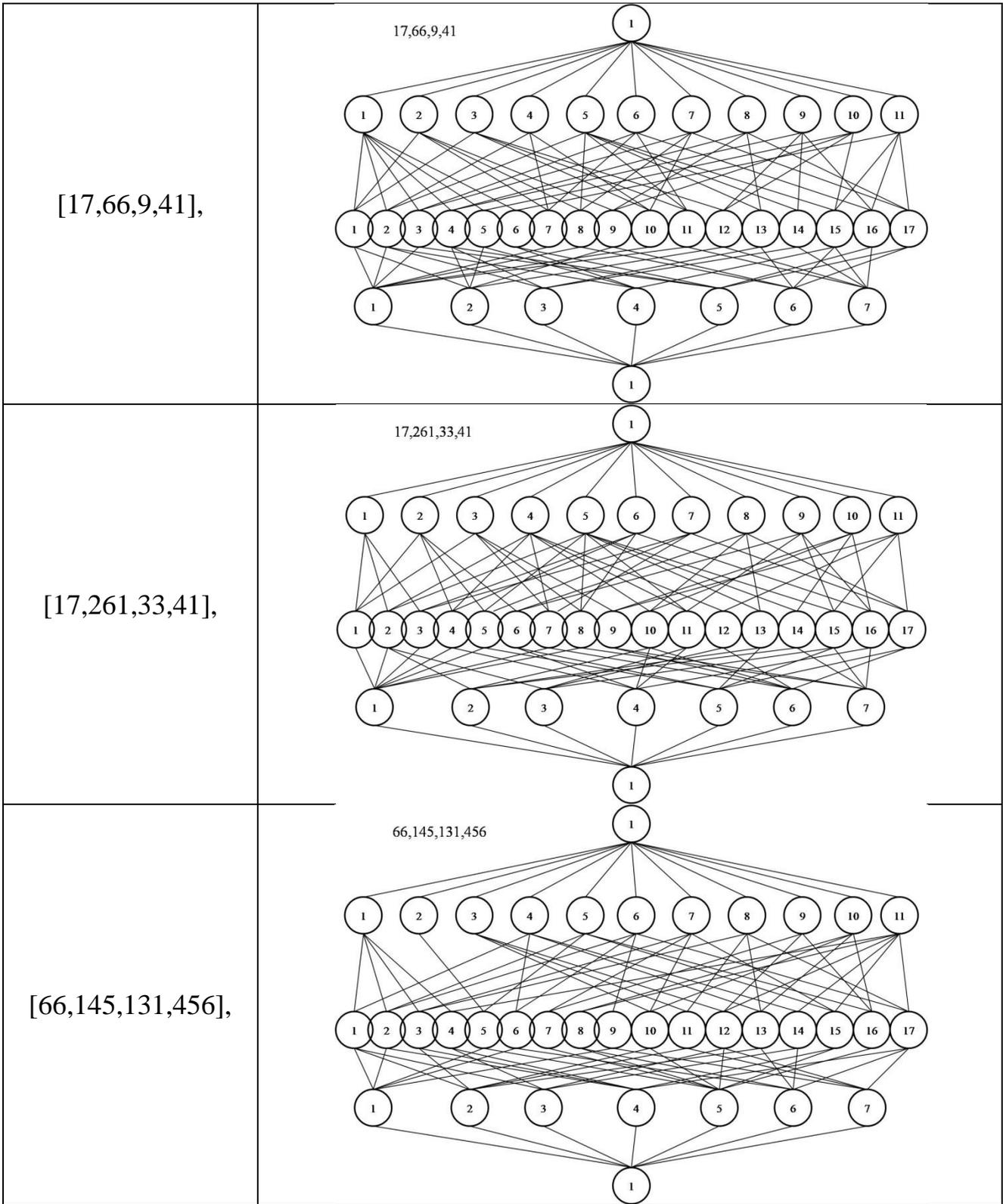
В таком случае необходимо использовать диаграммы четверок. Произведя анализ нарисованных диаграмм можно увидеть среди них одинаковые диаграммы (покрытие полностью совпадает) и похожие диаграммы (покрытие совпадает частично).

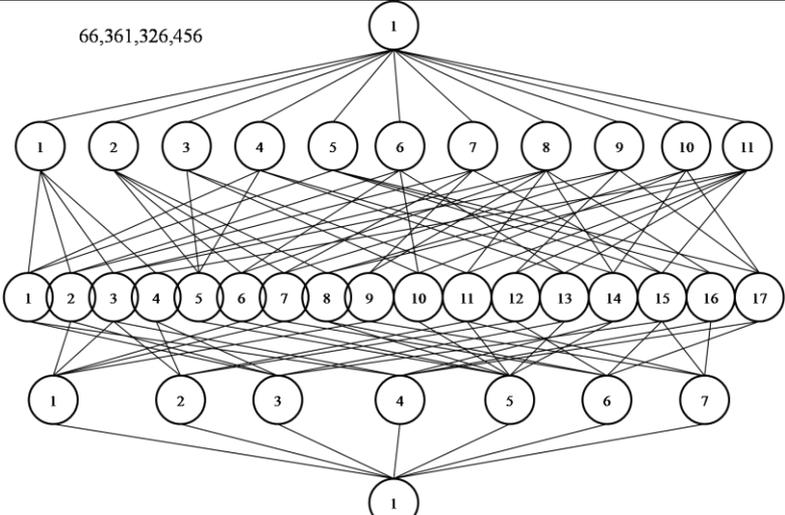
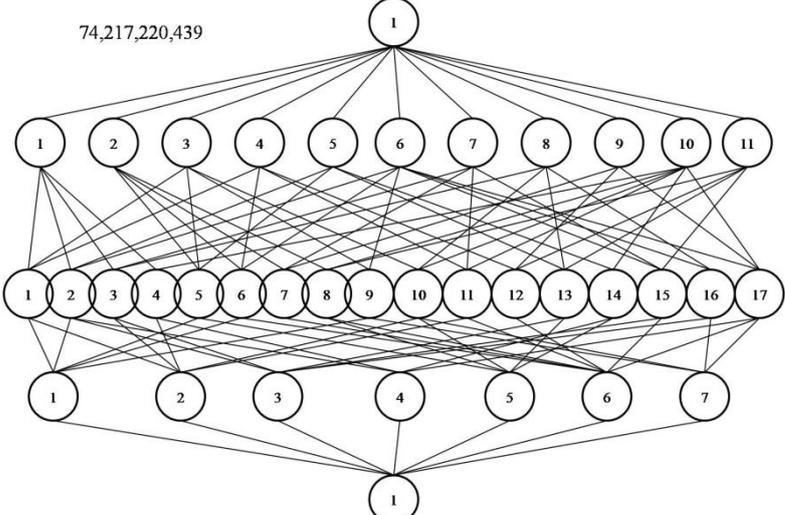
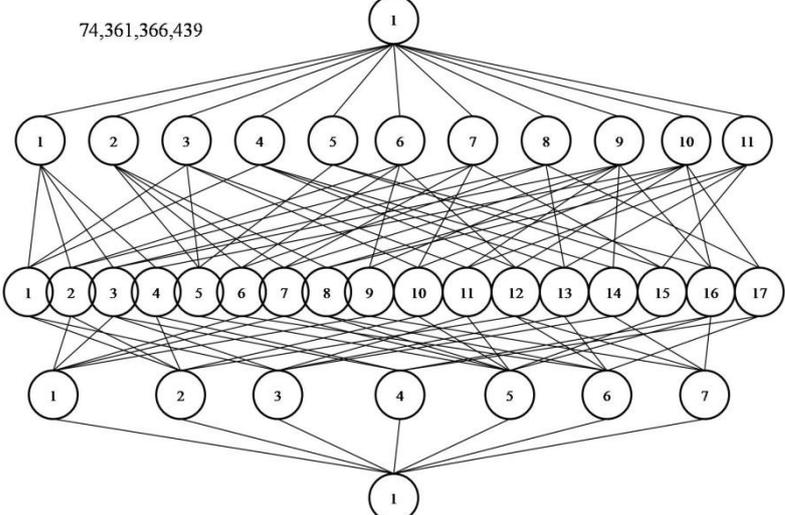
Литература

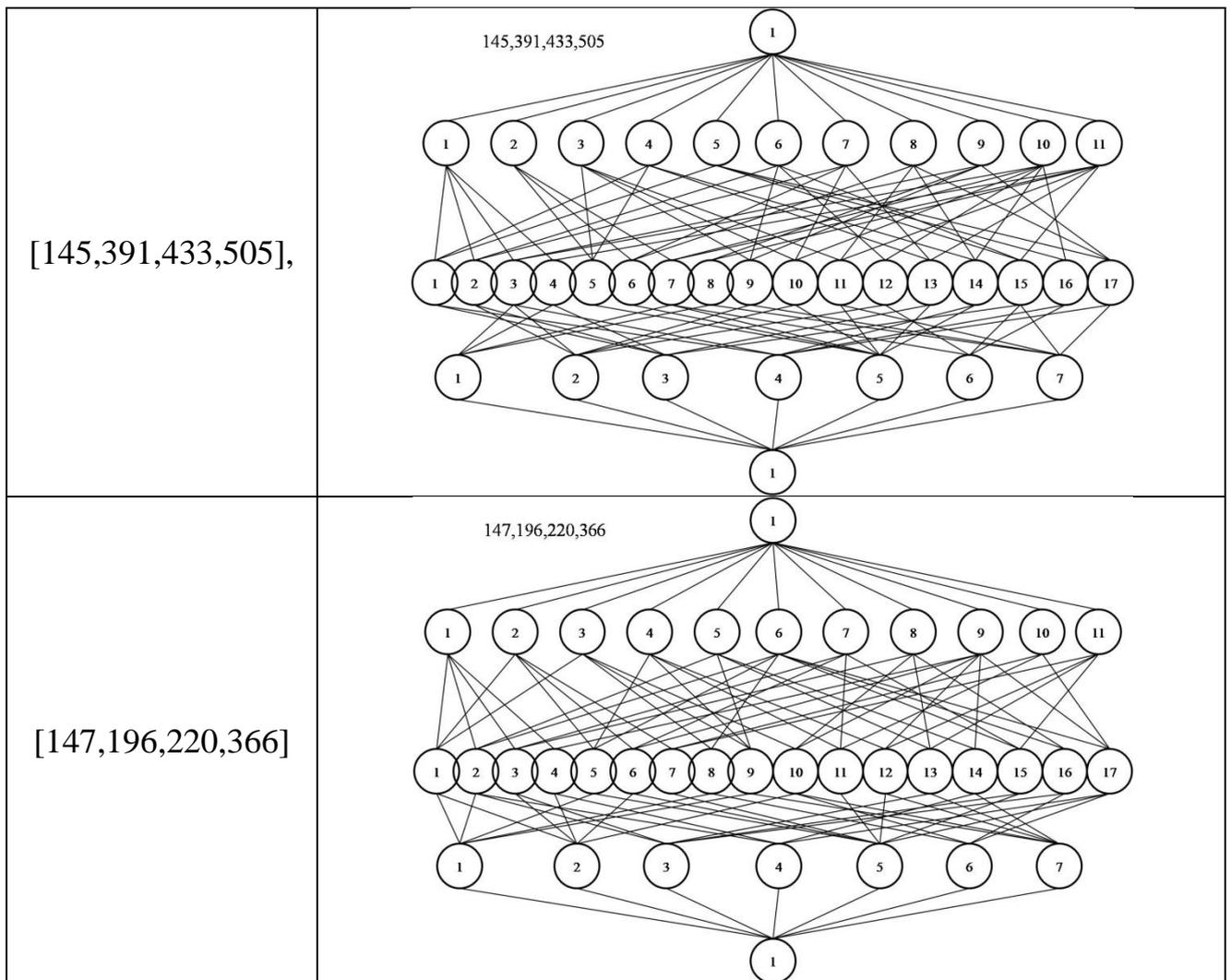
1. Биркгоф Г., Барти Т. К. Современная прикладная алгебра; пер. с англ. Ю. И. Манина. – Изд. 2-е, стер. – М.: Лань, 2005. – 400 с.
2. Зельвенский И. Г. Группы, кольца, поля: Методические указания по дисциплине “Геометрия и алгебра” / СПбГЭТУ.
3. Коновалов А.Б. Система компьютерной алгебры GAP –2009.-87с.
4. Коробков С. С. Вычисления в матричных алгебрах (прикладные аспекты алгебры и информатики) — Екатеринбург: 2014. – 101с.
5. Курош А. Г. Курс высшей алгебры: Учеб. для студентов вузов по спец." Математика", "Приклад. математика". – 13-е изд., стер. – СПб.: Лань, 2004. – 432с.
6. Система компьютерной алгебры GAP – Exponenta. Режим доступа: www.exponenta.ru/soft/others/gap/1.asp
7. GAP Manual. Режим доступа: <http://www.gap-system.org/Doc/manuals.html>

Четверка	Диаграмма
[2,17,3,5],	<p>2,17,3,5</p> <p>The diagram shows a hierarchical structure. At the top is a single node labeled '1'. Below it is a layer of 11 nodes labeled 1 through 11. Below that is a layer of 17 nodes labeled 1 through 17. At the bottom is a layer of 7 nodes labeled 1 through 7. Lines connect the top node to all 11 nodes in the second layer. The 11 nodes in the second layer are connected to the 17 nodes in the third layer. The 17 nodes in the third layer are connected to the 7 nodes in the bottom layer.</p>
[2,145,3,7],	<p>2,145,3,7</p> <p>The diagram shows a hierarchical structure. At the top is a single node labeled '1'. Below it is a layer of 11 nodes labeled 1 through 11. Below that is a layer of 17 nodes labeled 1 through 17. At the bottom is a layer of 7 nodes labeled 1 through 7. Lines connect the top node to all 11 nodes in the second layer. The 11 nodes in the second layer are connected to the 17 nodes in the third layer. The 17 nodes in the third layer are connected to the 7 nodes in the bottom layer.</p>
[2,289,5,7],	<p>2,289,5,7</p> <p>The diagram shows a hierarchical structure. At the top is a single node labeled '1'. Below it is a layer of 11 nodes labeled 1 through 11. Below that is a layer of 17 nodes labeled 1 through 17. At the bottom is a layer of 7 nodes labeled 1 through 7. Lines connect the top node to all 11 nodes in the second layer. The 11 nodes in the second layer are connected to the 17 nodes in the third layer. The 17 nodes in the third layer are connected to the 7 nodes in the bottom layer.</p>





<p>[66,361,326,456],</p>	<p>66,361,326,456</p> 
<p>[74,217,220,439],</p>	<p>74,217,220,439</p> 
<p>[74,361,366,439],</p>	<p>74,361,366,439</p> 



Приложение 3.

Таблица 7

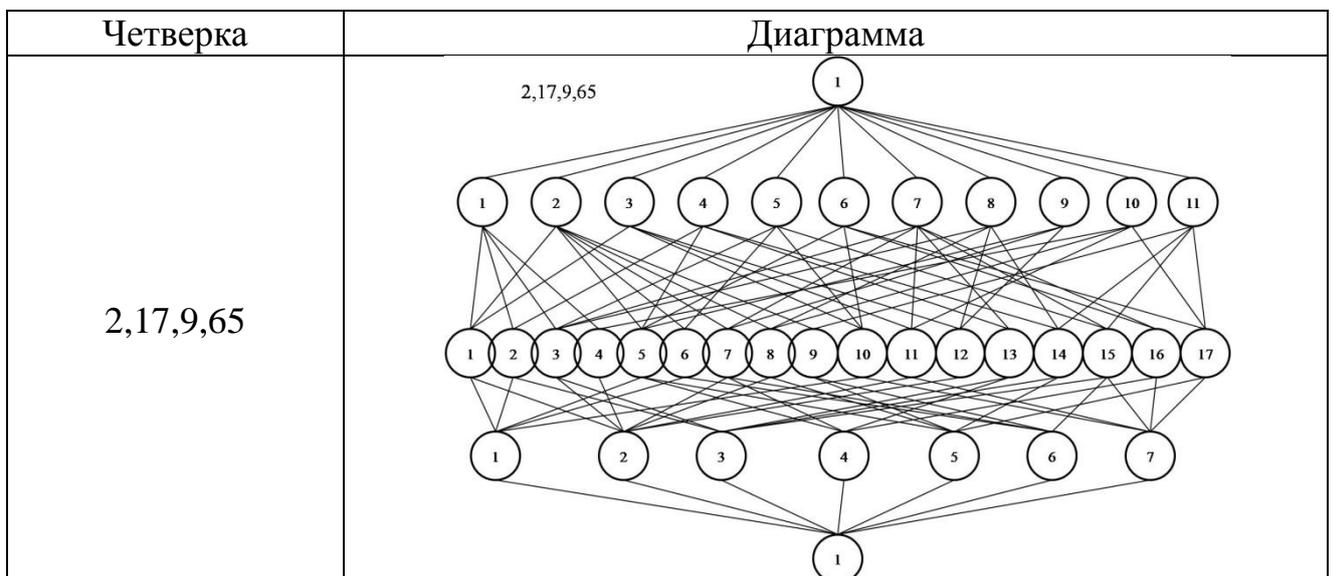
<p>Программа № 4</p>	
<p>eerr:=[];</p>	<p># Создание каталога для размещения подалгебр</p>
<p>Sub:=[]; b:=0;</p>	<p># Создание массива sub и переменной b</p>
<p>ID:=[2, 4, 6, 8, 10, 17, 18, 19, 22, 25, 46, 49, 50, 54, 55, 57, 66, 74, 82, 122, 145, 146, 147, 152, 196, 210, 217, 239, 257,</p>	<p># Массив номеров идемпотентных матриц</p>

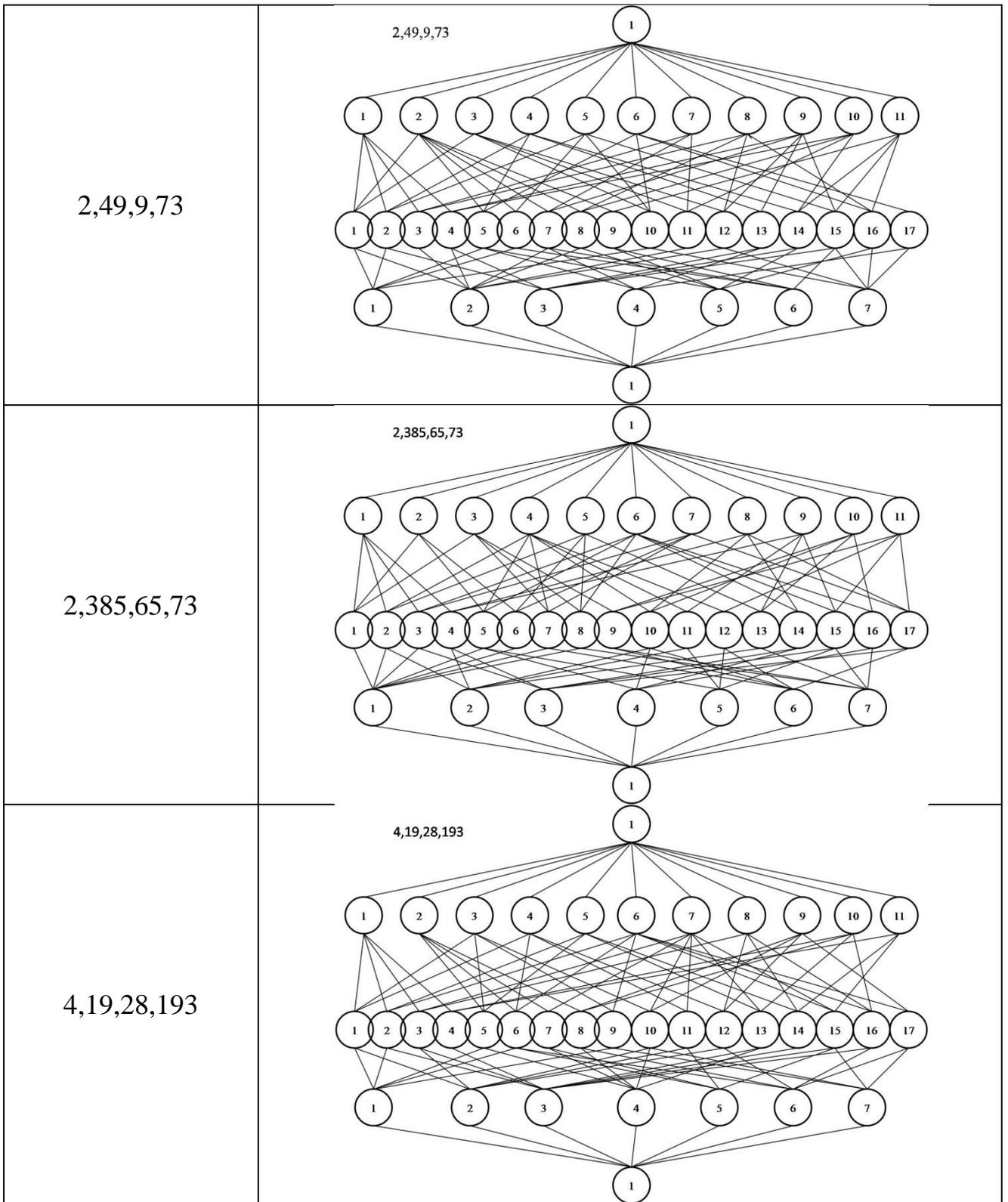
258, 260, 261, 266, 273, 274, 275, 277, 279, 281, 289, 290, 293, 296, 298, 317, 321, 337, 345, 361, 385, 386, 388, 391, 449, 458, 467, 512];	
NI:=[3, 5, 7, 9, 28, 33, 37, 41, 64, 65, 73, 129, 131, 193, 220, 326, 366, 433, 439, 456, 505];	# Массив номеров нильпотентных матриц
A:=MatAlgebra(GF(2),3);	# Построение алгебры матриц четвертого порядка над полем GF(2)
El:=Elements(A);	# Создание массива элементов алгебры A
for i in ID do for j in ID do for k in NI do for l in NI do	# Начало цикла построения подалгебр
if j>i and l>k and El[i]*El[j]=El[l] and El[j]*El[i]=El[l] and El[i]*El[k]=El[l] and El[k]*El[i]=El[k] and El[i]*El[l]=El[l] and El[l]*El[i]=El[l] and El[j]*El[k]=El[k] and El[k]*El[j]=El[l] and El[j]*El[l]=El[l] and El[l]*El[j]=El[l] and El[l]*El[k]=El[l] and El[k]*El[l]=El[l] then	#Если выполняется, то строится подалгебра B

<code>B:=Subalgebra (A,[E1[i],E1[j],E1[k],E1[l]]);</code>	# Записывает подалгебру алгебры A порожденную элементами E1[i], E1[k], E1[j] в B
<code>sub:=Elements(B);</code>	# Кладем в массив sub элементы подалгебры B
<code>AddSet(Sub,sub);</code>	#Присоединение элемента sub к массиву Sub
<code>if Size(Sub) > b then Add(eerr,[i,j,k,l]);</code>	# Сравниваем размер массива Sub с b. Если размер больше, то записываем в массив eerr
<code>b:=Size(Sub);</code>	# Присваиваем b размер массива sub
<code>fi;fi;</code>	#Окончание работы условного оператора
<code>od; od; od; od;</code>	#Конец цикла
<code>Sort(eerr);</code>	# Упорядочиваем элементы массива eerr
<code>PrintTo("eerr-2.dan","eerr:=","eerr,",";" "\n"," eerr =",Size(eerr)," \n");</code>	#Печать результата в файл eerr-2.dan

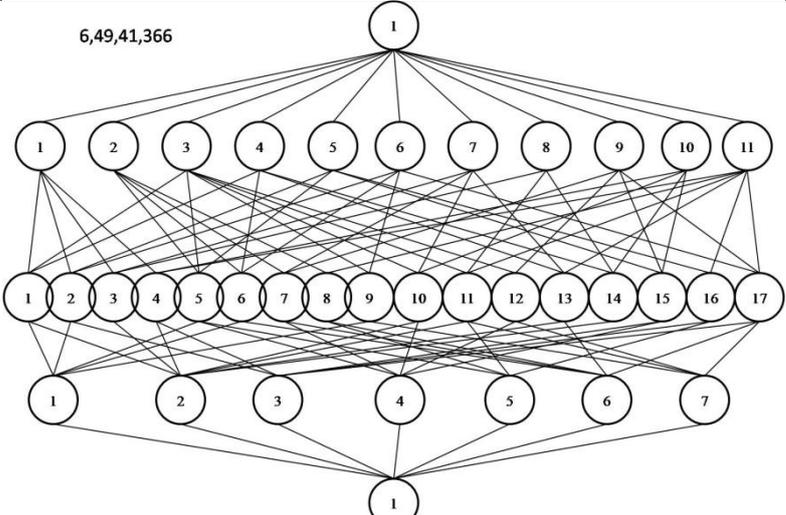
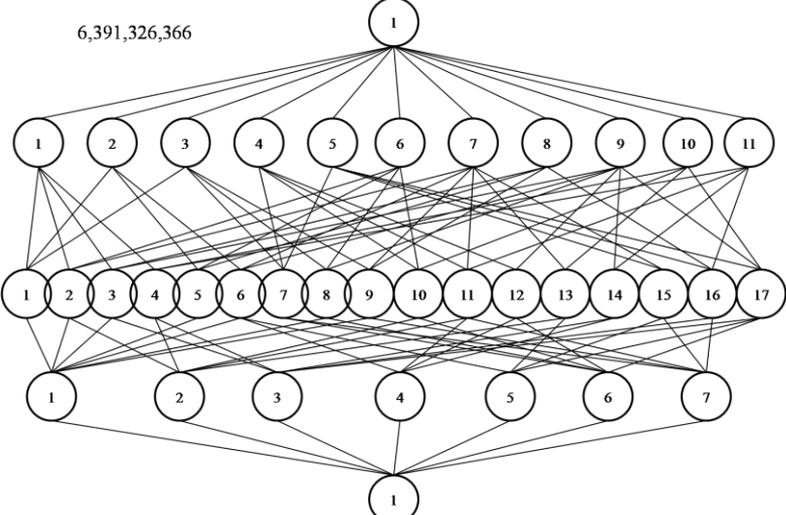
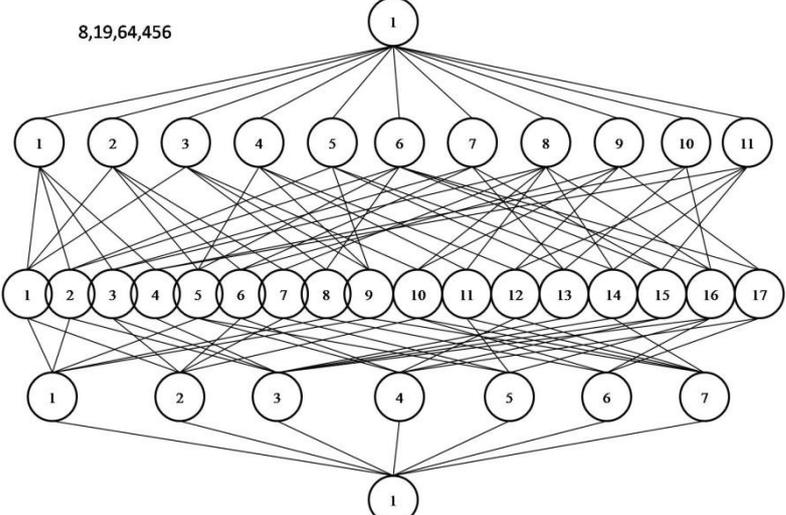
Приложение 4.

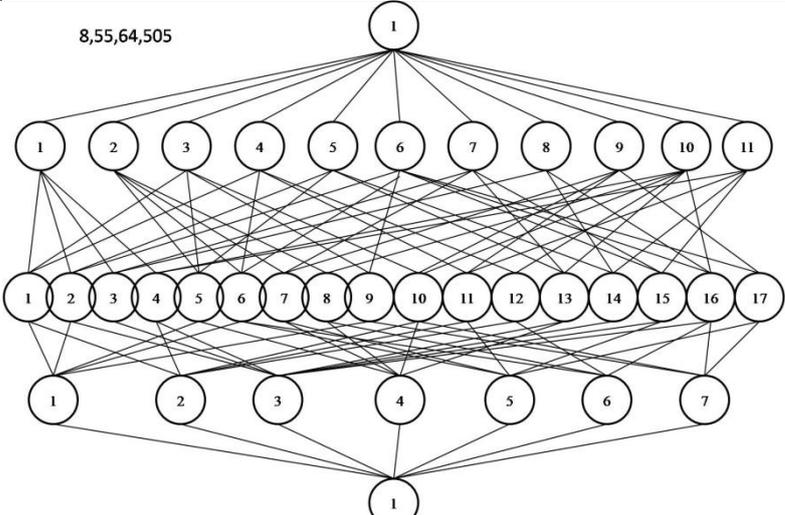
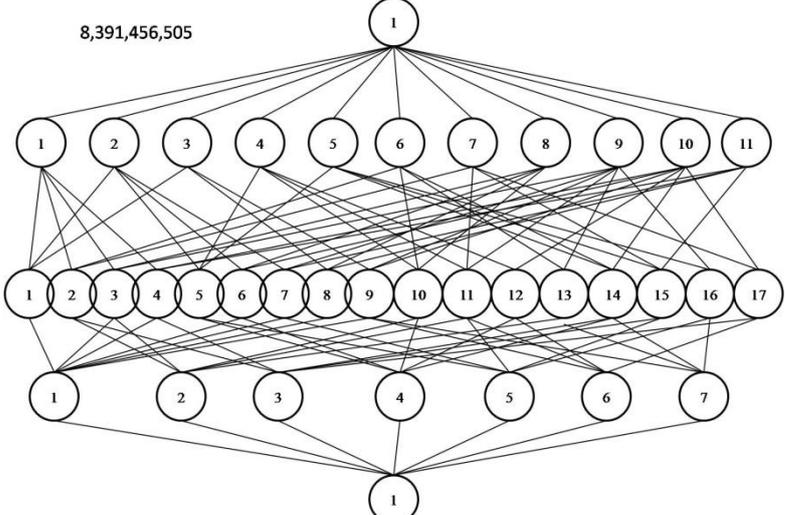
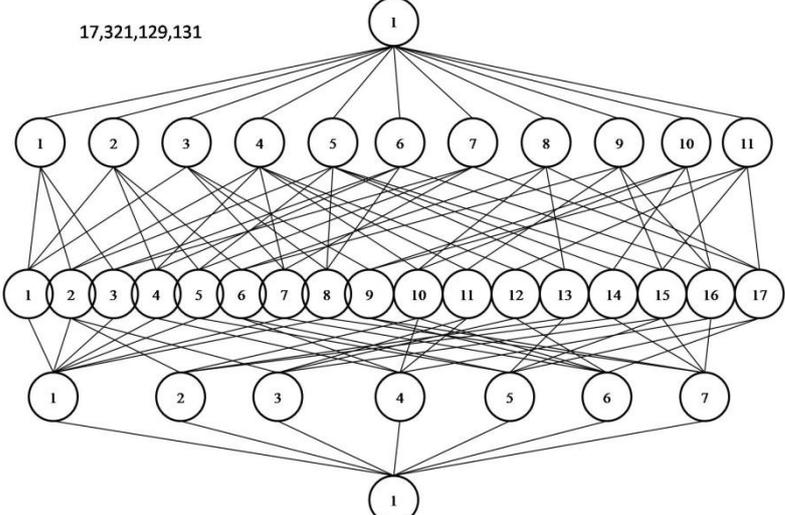
Таблица 8





<p>4,55,28,220</p>	
<p>4,385,193,220</p>	
<p>6,17,41,326</p>	

<p>6,49,41,366</p>	<p>6,49,41,366</p> 
<p>6,391,326,366</p>	<p>6,391,326,366</p> 
<p>8,19,64,456</p>	<p>8,19,64,456</p> 

<p>8,55,64,505</p>	 <p>8,55,64,505</p>
<p>8,391,456,505</p>	 <p>8,391,456,505</p>
<p>17,321,129,131</p>	 <p>17,321,129,131</p>

