Методическая разработка

для проведения лекции

Занятие 3. Алгебраические структуры

Учебные вопросы занятий:
1. Группы
2. Кольца
3. Поля
Заключительная часть

Содержание занятия:

Введение

В рамках различных задач обеспечения информационной безопасности, в частности криптографии, требуется, чтобы были заданы множества целых чисел и операции, определенные для них. Комбинация множеств и операций, которые могут быть применены к элементам множества, называются алгебраической структурой. Рассмотрим три общих алгебраических структуры: группы, кольца, поля.

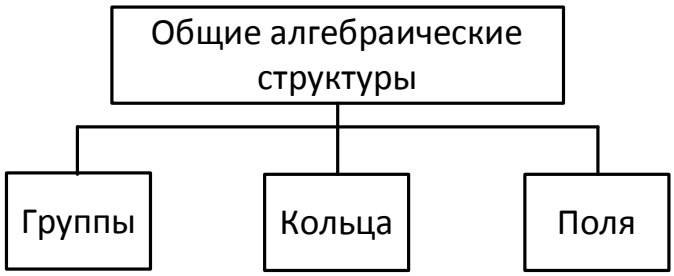

Рисунок 1. Алгебраические структуры

1. Группы

Группа G – набор элементов с бинарной операцией «*», обладает четырьмя свойствами (или удовлетворяет аксиомам), представленным далее.

Коммутативная группа, также называемая абелева, - группа, в которой оператор обладает теми же четырьмя свойствами для групп плюс дополнительным – коммутативностью:

1) *замкнутость:* для каждой пары a и b из множества G элемент $c = a * b$ принадлежит этому множеству;

2) *ассоциативность:* для всех a, b и c из множества G выполняется равенство

$$a*(b*c) = (a*b)*c;$$

3) *существование нейтрального элемента (единицы):* в множестве G существует элемент *e* называемый *нейтральным (единичным) элементом* и такой, что

$$a * e = e * a = a$$

для любого элемента *a* этого множества;

4) *существование обратных элементов (инверсии):* для любого *a* из множества G существует некоторый элемент $b = a^{-1}$ из этого множества, называемый обратным *элементу a* и такой, что

$$a * b = b * a = e.$$

Если группа G содержит конечное число элементов, то она называется *конечной группой,* а число элементов в G – *порядком* G.

5) *коммутативность: д*ля любых *a* и *b* из группы G

$$a * b = b * a.$$

В случае абелевых групп групповая операция может обозначаться символом + и называться сложением (даже тогда, когда она не является обычным арифметическим сложением). В этом случае единичный элемент называется нулем и обозначается 0, а обратный элементу a элемент записывается в виде $-a$, так что

$$a + (-a) = (-a) + a = 0.$$

Иногда групповая операция обозначается символом · и называется умножением (даже тогда, когда она не является обычным арифметическим умножением). В этом случае единичный элемент называется единицей и обозначается 1, а обратный элементу a элемент записывается в виде a^{-1}, так что

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Хотя группа включает единственный оператор, свойства, присущие каждой операции, допускают использование пары операций, если они – инверсии друг друга. Например, если определенный выше оператор – сложение, то группа поддерживает и сложение, и вычитание, так как вычитание и сложение – аддитивно инверсные операции. Это также верно для умножения и деления. Однако группа может поддерживать только сложение/вычитание или умножение/деление, но не оба сочетания операторов одновременно.

Пример 1.

Множество целых чисел, входящих в вычет с оператором сложения $G =< Z_n, + >$ является коммутативной группой. Мы можем выполнить сложение и вычитание на элементах этого множества, не выходя за его пределы.

Проверим свойства

1. Замкнутость удовлетворяется. Результат сложения двух целых чисел в Z_n - другое целое число в Z_n.
2. Ассоциативность удовлетворяется. Например, результат 4+(3+2) тот же самый, что и в случае (4+3)+2.
3. Коммутативность удовлетворяется. Например, 3+5=5+3.
4. Нейтральный элемент – 0. Имеем 3+0=0+3=3.

5. Каждый элемент имеет аддитивную инверсию или дополнение. Например, инверсия 3 – это -3 и наоборот. Инверсия позволяет выполнять вычитание на множестве.

Пример 2.

Множество Z_n с оператором умножения $G =< Z_n, * >$ также является абелевой группой. Мы можем выполнять умножение и деление на элементах этого множества, не выходя за его пределы. Это обеспечивает проверку первых трех свойств. Нейтральный элемент равен 1. Каждый элемент имеет инверсию, которая может быть найдена согласно расширенному алгоритму Евклида.

Пример 3.

Несмотря на то, что обычно мы представляем группу как множество чисел с обычными операторами, такими как сложение или вычитание, определения группы позволяют нам определять любое множество объектов и операций, которые удовлетворяют рассмотренным свойствам. Определим множество $G =< \{a, b, c, d\}, * >$ и операцию, представленную с помощью таблицы 1.

Таблица1.

	a	*b*	*c*	*d*
a	*a*	*b*	*c*	*d*
b	*b*	*c*	*d*	*a*
c	*c*	*d*	*a*	*b*
d	*d*	*a*	*b*	*c*

Это множество – абелева группа, так как все пять свойств удовлетворены.

1. Замкнутость. Применение оператора на любой паре элементов дает в результате другой элемент этого множества.
2. Ассоциативность. Чтобы доказать наличие этого свойства, необходимо проверить его для любой комбинации из трех элементов. Например, $(a + b) + c = a + (b + c)$.
3. Операция коммутативна. Имеем $a + b = b + a$.
4. Группа имеет нейтральный элемент, которым является *a*.
5. Каждый элемент имеет инверсию. Обратные пары могут быть найдены по таблице.

Пример 4.

В группе элементами множества не обязательно должны быть числа или объекты. Ими могут быть правила, отображения, функции или действия. Один из вариантов – группа перестановок. Множество всех перестановок и оператор является композицией: применение одной перестановки за другой. На рисунке 2 показан пример композиции двух перестановок, которые перемещают три входных сигнала, чтобы создать три выходных сигнала.

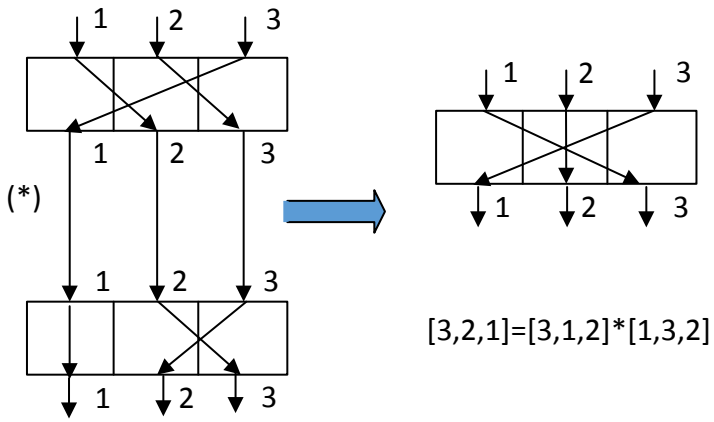

Рисунок 2. Пример композиции перестановок

Входные и выходные сигналы могут быть символами или битами. Каждая перестановка представлена прямоугольником, внутри которого показано, где исходящий входной сигнал, а индекс (1,2,3) определяет выходной сигнал. Композиция состоит из двух последовательно выполняемых перестановок. При трех входных сигналах и трех выходных сигналах может быть 3!=6 различных перестановок. Таблица 2 определяет содержание этого оператора. Первая строка – первая перестановка, первый столбец – вторая перестановка. Результат содержится на пересечении.

В этом случае удовлетворены только четыре свойства, поэтому группа – не абелева.

1. Свойство замкнутости соблюдается.
2. Ассоциативность соблюдается. Для доказательства необходимо проверить свойство для любой комбинации из трех элементов.
3. Свойство коммутативности не выполняется.
4. Множество имеет нейтральный элемент [1,2,3] – перестановка отсутствует.
5. Каждый элемент имеет инверсию. Обратные пары могут быть найдены, если использовать нейтральный элемент.

	[1,2,3]	[1,3,2]	[2,1,3]	[2,3,1]	[3,1,2]	[3,2,1]
[1,2,3]	[1,2,3]	[1,3,2]	[2,1,3]	[2,3,1]	[3,1,2]	[3,2,1]
[1,3,2]	[1,3,2]	[1,2,3]	[2,3,1]	[2,1,3]	[3,2,1]	[3,1,2]
[2,1,3]	[2,1,3]	[3,1,2]	[1,2,3]	[3,2,1]	[1,3,2]	[2,3,1]
[2,3,1]	[2,3,1]	[3,2,1]	[1,3,2]	[3,1,2]	[1,2,3]	[2,1,3]
[3,1,2]	[3,1,2]	[2,1,3]	[3,2,1]	[1,2,3]	[2,3,1]	[1,3,2]
[3,2,1]	[3,2,1]	[2,3,1]	[3,1,2]	[1,3,2]	[2,1,3]	[1,2,3]

В данном примере показано, что множество перестановок с композицией операций – группа. Поэтому использование двух последовательно выполняемых перестановок не могут усилить безопасность шифра. Всегда есть

возможность найти перестановку, которая может реализовать эту же операцию, используя свойство замкнутости.

Подгруппы.

Подмножество H группы G – это подгруппа G, если само H – группа относительно операции на G. Другими словами, если $G =< S, \bullet >$ - группа, а $H =< T, \bullet >$ - группа для той же самой операции, и T – непустое подмножество S, то H – подгруппа G.

Указанное определение подразумевает, что

1. если a и b – члены обеих групп, то $c = a \bullet b$ - также элемент обеих групп;
2. для группы и подгруппы имеется один и тот же нейтральный элемент;
3. если этот элемент принадлежит обеим группам, инверсия a – также элемент обеих групп;
4. группа, полученная с помощью нейтрального элемента G, $H =< \{e\}, \bullet >$, является подгруппой G;
5. каждая группа – подгруппа самой себя.

Пример 5.

Проверим, является ли группа $H =< Z_{10}, + >$ подгруппой группы $H =< Z_{12}, + >$.

В ходе проверки выясняется, что не является. Несмотря на то, что H – подмножество G, операции, определенные для этих двух групп, различны. Операция в H – сложение по модулю 10, операция в G – сложение по модулю 12.

Циклические подгруппы.

Если подгруппа группы может быть сгенерирована путем возведения в степень какого-либо элемента, то такая подгруппа называется циклической подгруппой. Термин «возведение в степень» означает многократное применение к элементу групповой операции: $a^n = a \bullet a \bullet ... \bullet a (n\ раз)$.

Пример 6.

Из группы $G =< Z_6, + >$ могут быть получены четыре циклические подгруппы. Это $H_1 =< \{0\}, + >$, $H_2 =< \{0,2,4\}, + >$, $H_3 =< \{0,3\}, + >$, $H_4 = G$. Следует отметить, что в случае использования операции сложения a^n означает умножение n на a. Следует отметить также, что во всех этих группах операция – это сложение по модулю 6. Далее покажем, каким образом можно найти элементы этих циклических подгрупп.

1. Циклическая подгруппа, сгенерированная из 0, - это H_1, имеет только один элемент (нейтральный элемент).

   $0^0 \bmod 6 = 0$ (процесс завершен, далее все повторяется).
2. Циклическая подгруппа, сгенерированная на основе 1, - это H_4, которая есть сама группа G.

   $1^0 \bmod 6 = 0$

$1^1 \bmod 6 = 1$

$1^2 \bmod 6 = (1+1) \bmod 6 = 2$

$1^3 \bmod 6 = (1+1+1) \bmod 6 = 3$

$1^4 \bmod 6 = (1+1+1+1) \bmod 6 = 4$

$1^5 \bmod 6 = (1+1+1+1+1) \bmod 6 = 5$ (процесс завершен, далее все повторяется).

3. Циклическая подгруппа, сгенерированная на основе 2, - это H_2, имеет три элемента: 0, 2 и 4.

   $2^0 \bmod 6 = 0$

   $2^1 \bmod 6 = 2$

   $2^2 \bmod 6 = (2+2) \bmod 6 = 4$ (процесс завершен, далее все повторяется).

4. Циклическая подгруппа, сгенерированная на основе 3, - это H_3, имеет два элемента: 0 и 3.

   $3^0 \bmod 6 = 0$

   $3^1 \bmod 6 = 3$ (процесс завершен, далее все повторяется).

5. Циклическая подгруппа, сгенерированная на основе 4, - это H_2, не новая подгруппа.

   $4^0 \bmod 6 = 0$

   $4^1 \bmod 6 = 4$

   $4^2 \bmod 6 = (4+4) \bmod 6 = 2$ (процесс завершен, далее все повторяется).

6. Циклическая подгруппа, сгенерированная на основе 5, - это H_4, которая есть сама группа G.

   $5^0 \bmod 6 = 0$

   $5^1 \bmod 6 = 5$

   $5^2 \bmod 6 = 4$

   $5^3 \bmod 6 = (5+5+5) \bmod 6 = 3$

   $5^4 \bmod 6 = (5+5+5+5) \bmod 6 = 2$

   $5^5 \bmod 6 = (5+5+5+5+5) \bmod 6 = 1$ (процесс завершен, далее все повторяется).

Пример 7.

Из группы $G = < Z_{10}, \times >$ можно получить три циклические подгруппы. G имеет только четыре элемента: 1, 3, 7, 9. Циклические подгруппы - $H_1 = < \{1\}, \times >$, $H_2 = < \{1,9\}, \times >$ и $H_3 = G$. Далее покажем, как находятся элементы этих подгрупп.

1. Циклическая подгруппа, сгенерированная на основе 1, - это H_1. Подгруппа имеет только один элемент (нейтральный элемент).

   $1^0 \bmod 10 = 1$ (процесс завершен, далее все повторяется).
2. Циклическая подгруппа, сгенерированная на основе 3, - это H_3, которая есть сама группа G.

   $3^0 \bmod 10 = 1$

   $1^1 \bmod 10 = 3$

   $3^2 \bmod 10 = 9$

   $3^3 \bmod 10 = (3 \times 3 \times 3) \bmod 10 = 7$ (процесс завершен, далее все повторяется).
3. Циклическая подгруппа, сгенерированная на основе 7, - это H_3, которая есть группа G.

   $7^0 \bmod 10 = 1$

   $7^1 \bmod 10 = 7$

   $7^2 \bmod 10 = 9$

   $7^3 \bmod 10 = 3$ (процесс завершен, далее все повторяется).
4. Циклическая подгруппа, сгенерированная на основе 9, - это H_2. Подгруппа имеет только два элемента.

   $9^0 \bmod 10 = 1$

   $9^1 \bmod 10 = 9$ (процесс завершен, далее все повторяется).

Циклические группы.

Циклическая группа – группа, которая является собственной циклической подгруппой. В примере 6 группа G имеет циклическую подгруппу $H_4 = G$. Это означает, что группа G – циклическая группа. В этом случае элемент, который генерирует циклическую подгруппу, может также генерировать саму группу. Этот элемент далее именуется «генератор». Если g – генератор, элементы в конечной циклической группе могут быть записаны как

$\{e, g, g^2, ..., g^{n-1}\}$, где $g^n = e$.

Следует отметить, что циклическая группа может иметь много генераторов.

Пример 8.

1. Группа $G =< Z_6, + >$ - циклическая группа с двумя генераторами g=1 и g=5.
2. Группа $G =< Z_{10}, \times >$ - циклическая группа с двумя генераторами g=3 и g=7.

Теорема Лагранжа.

Теорема Лагранжа показывает отношение порядка группы к порядку ее подгруппы. Предположим, что G – группа и H – подгруппа G. Если порядки G и H – это $|G|$ и $|H|$, соответственно, то согласно этой теореме $|H|$ делит $|G|$. В

примере 6 $|G|=6$. Порядок подгруппы - $|H_1|=1$, $|H_2|=3$, $|H_3|=2$, $|H_4|=6$. Очевидно, все эти значения есть делители 6.

Теорема Лагранжа имеет важное приложение. Когда дана группа G и ее порядок $|G|$, могут быть легко определены порядки потенциальных подгрупп, если могут быть найдены делители. Например, порядок группы $G=<Z_{17},+>$ равен 17. Делители 17 есть 1 и 17. Это означает, что группа может иметь только две подгруппы – нейтральный элемент и $H_2=G$.

Порядок элемента.

Порядок элемента в группе $ord(a)$ является наименьшим целым числом n, таким, что $a^n=e$. Иными словами, порядок элемента – порядок группы, которую он генерирует.

Пример 9.

1. В группе $G=<Z_6,+>$ имеют место следующие значения порядка элементов: $ord(0)=1$, $ord(1)=6$, $ord(2)=3$, $ord(3)=2$, $ord(4)=3$, $ord(5)=6$.
2. В группе $G=<Z_{10},\times>$ имеют место следующие значения порядка элементов: $ord(1)=1$, $ord(3)=4$, $ord(7)=4$, $ord(9)=2$

2. Кольца

Кольцо – абстрактное множество, обозначенное $R=\{...\},\bullet,\perp$, которое является абелевой группой и наделено дополнительной структурой. Оно является алгебраической структурой с двумя операциями. Первая операция должна удовлетворять всем пяти свойствам, требуемым для абелевой группы. Вторая операция должна удовлетворять только первым двум свойствам абелевой группы. Кроме того, вторая операция должна быть распределена с помощью первой. Дистрибутивность означает, что для всех *a, b* и *c* элементов из R мы имеем $a\perp(b\bullet c)=(a\perp b)\bullet(a\perp c)$ и $(a\bullet b)\perp c=(a\perp c)\bullet(b\perp c)$. Коммутативное кольцо – кольцо, в котором коммутативное свойство удовлетворено и для второй операции.

Если обобщить, то кольцо включает две операции. Однако вторая операция может не соответствовать третьему и четвертому свойствам. Другими словами, первая операция фактически соответствует паре операций, таких как сложение и вычитание; вторая операция предполагает единственную операцию, например умножение, но не предполагает деления.

Определение. Кольцом R называется множество с двумя определенными на нем операциями (первая может быть *сложением* (обозначаем +), вторая – *умножением* (обозначаем ×)), причем имеют место следующие аксиомы или свойства:

1) относительно сложения *R* является абелевой группой;
2) *замкнутость:* произведение $a\times b$ принадлежит *R* для любых *a* и *b* из *R;*
3) выполняется *закон ассоциативности:*
   $a\times(b\times c)=(a\times b)\times c$;
4) выполняется *закон дистрибутивности:*

$a\times(b+c)=(a\times b)+(a\times c)$, $(a+b)\times c=(a\times c)+(b\times c)$.

Сложение в кольце всегда коммутативно, а умножение не обязательно должно быть коммутативным. *Коммутативное кольцо* – это кольцо, в котором и умножение коммутативно, т. е. $a\times b = b\times a$ для всех a и b из R.

Закон дистрибутивности в определении кольца связывает операции сложения и умножения. Этот закон имеет несколько непосредственных следствий, как, например, приведенная ниже теорема.

Теорема 1. Для произвольных элементов a и b *в кольце* R

1. $a0 = 0a = 0$;
2. $a(-b) = (-a)b = -(ab)$.

Операция сложения в кольце имеет единичный элемент, называемый нулем. Операция умножения не обязательно имеет единичный элемент, но если он есть, то является единственным. Кольцо, обладающее единственным элементом относительно умножения, называется *кольцом с единицей.* Этот единичный элемент называется единицей и обозначается символом 1. Тогда для всех a из R имеет место равенство $1a = a1 = a$.

Относительно операции сложения каждый элемент кольца имеет обратный. Относительно операции умножения элемент, обратный данному элементу, не обязательно существует, но в кольце с единицей обратные элементы могут существовать. Это означает, что для данного элемента a может существовать элемент b, такой, что $ab = 1$. Если это так, то b называется *правым обратным к* a. Аналогично если существует элемент c, такой, что $ca = 1$, *то* c называется *левым обратным к* a.

Теорема 2. В кольце с единицей

1) *единица единственна;*

2) *если элемент* a *имеет как правый обратный* b, *так и левый обратный* c, *то элемент* a *называется обратимым, причем обратный ему элемент является единственным (и обозначается через* a^{-1});

3) $\left(a^{-1}\right)^{-1} = a$.

Пример 10.

Множество Z с двумя операциями – сложением и умножением – является коммутативным кольцом, которое обозначается R=Z,+,×. Сложение удовлетворяет всем пяти свойствам, умножение удовлетворяет только трем свойствам. Умножение дистрибутивно с помощью сложения. Например, 5×(3+2)=(5×3)+(5×2)=25. Мы можем выполнить на этом множестве сложение и вычитание и умножение, но не деление. Деление не может применяться в этой структуре, потому что оно приводит к элементу из другого множества. Результат деления, например, 12 на 5 равен 2,4. Этот элемент не находится в заданном множестве.

3. Поля

Поле, обозначенное $F=\{\ldots\}$, $\bullet,\perp$ – коммутативное кольцо, в котором вторая операция удовлетворяет всем пяти свойствам, определенным для первой операции, за исключением того, что нейтральный элемент первой операции (иногда называемый нулевой элемент) не имеет инверсии относительно второй операции. Таким образом, поле – это структура, которая поддерживает две пары операций, используемые в математике: сложение/вычитание и умножение/деление. При этом не разрешено деление на нуль.

Определение. Полем называется множество с двумя определенными на нем операциями – *сложением* и *умножением,* причем имеют место следующие аксиомы:

1) множество образует абелеву группу по сложению;

2) поле замкнуто относительно умножения, и множество ненулевых элементов образует абелеву группу по умножению;

3) выполняется закон дистрибутивности: $(a+b)c=ac+bc$ для любых a, b, c из поля.

Единичный элемент относительно сложения принято обозначать через 0 и называть нулем, аддитивный обратный элементу a элемент – через $-a$; единичный элемент относительно умножения обозначать через 1 и называть единицей, мультипликативный обратный к элементу a элемент – через a^{-1}. Под вычитанием $(a-b)$ понимается $a+(-b)$, под делением (a/b) понимается $b^{-1}a$.

Конечные поля

Конечное поле – поле с конечным числом элементов – является очень важной структурой в теории кодирования и криптографии. Галуа показал, что поля, чтобы быть конечными, должны иметь число элементов p^n, где p – простое, а n – положительное целое число. Поэтому конечные поля обычно называют полями Галуа и обозначают как $GF(p^n)$.

Поля GF(p)

Когда n=1, мы имеем поле GF(p). Это поле может быть множеством Z_p, (0, 1, …, p-1) с двумя арифметическими операциями (сложение и умножение). Любой элемент в этом множестве имеет аддитивную инверсию, и элементы, отличные от нуля, имеют мультипликативную инверсию.

Пример 11.

Очень распространенное поле в этой категории - GF(2) с множеством {0,1} и двумя операциями, сложением и умножением:

Сложение

+	0	1
0	0	1
1	1	0

Умножение

×	0	1
0	0	0
1	0	1

Инверсия

a	0	1	*a*	0	1
-a	0	1	a^{-1}	-	1

Есть несколько моментов, которые следует отметить в определении этого поля. Первый: множество имеет только два элемента, которые являются двоичными цифрами или битами. Второй: операция сложения – фактически Исключающее ИЛИ (XOR), операция, которую мы используем с двоичными цифрами. Третий: операция умножения – AND, также операция, которую мы используем с двоичными цифрами. Четвертый: сложение и вычитание – те же самые (операция XOR). Пятый: умножение и деление – те же самые (операция AND).

Пример 12.

Мы можем определить GF(5) на множестве Z_5 с операторами сложения и умножения, представленными ниже.

Для нахождения мультипликативных инверсий элементов поля можно использовать расширенный алгоритм Евклида, но проще составить таблицу умножения и находить каждую пару, произведение которой равно 1. Это (1,1), (2,3), (3,2), (4,4). Также на этом множестве можно применить вычитание и умножение/деление (за исключением запрещенного деления на 0).

Сложение

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Умножение

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Аддитивная инверсия

a	0	1	2	3	4
-a	0	4	3	2	1

Мультипликативная инверсия

a	0	1	2	3	4
a^{-1}	-	1	3	2	4

Поля GF(p^n)

В дополнение к полям *GF(p)* в различных практических приложениях широко используются поля *GF(p^n)*. Однако, рассмотренные ранее примеры не удовлетворяют требованиям полей указанного вида. Поэтому необходимо определить новые множества и новые операции на этих множествах.

Выводы:

Таким образом, построение эталонных описаний в рассматриваемом случае параметрического обучения сводится к выражению значений неизвестных параметров через выборочные моменты $\overline{a}_1, \overline{a}_2, ..., \overline{a}_M$, которые легко вычисляются по обучающей неклассифицированной выборке, и подстановке их в суммарное M -модальное распределение.

Заключительная часть.

Подвожу итоги занятия.

Контрольные вопросы

1. Определите алгебраическую структуру и назовите три алгебраические структуры, обсужденные в этой лекции.
2. Определите группу и приведите различия между группой и *коммутативной* группой.
3. Определите кольцо и приведите различия между кольцом и *коммутативным* кольцом.
4. Определите поле и приведите различия между бесконечным полем и конечным полем.
5. Покажите число элементов в поле Галуа для простого числа.
6. Дайте один пример группы, использующей множество вычетов (операций по модулю).
7. Дайте один пример кольца, использующего множество вычетов (операций по модулю).
8. Дайте один пример поля, использующего множество вычетов (операций по модулю).