Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Удмуртский государственный университет»
Институт математики, информационных технологий и физики

А.С. Мерзляков

АЛГЕБРА - 1

Учебно-методическое пособие

Ижевск
2024

УДК 512.5(075.8)
ББК 22.14р30
М521

Рекомендовано к изданию Учебно-методическим советом УдГУ

Рецензент: канд. физ.-мат. наук, доцент , НПО МКМ Л.И.Романов

Мерзляков А.С.

М521 Алгебра-1 : учеб.-метод. пособие : [Электрон. ресурс] – Ижевск : Удмуртский университет, 2024. – 48 с.

Данное методическое пособие предназначено для самостоятельной работы студентов-бакалавров направления 02.03.01«Математика и компьютерные науки»; 01.03.01 «Математика»; 01.03.02 «Прикладная математика и информатика». Она поможет студенту лучше изучить теоретический материал по некоторым вопросам курса фундаментальной алгебры. В пособии подробно заостряется внимание на тех моментах, которые, наиболее важны, и которые могут неоднозначно трактоваться. В нем также разбираются методы решения некоторых типов задач, которые встречаются в ходе изучения курса и предлагаются упражнения, для более глубокого и полного понимания данного курса. Вместе с пособием «Поле комплексных чисел. Практические занятия», оно, несомненно, будет полезно всем студентам, кто в ходе обучения в ВУЗе изучает основы алгебры.

Работа предназначается для всех студентов, обучающихся по математическим специальностям очной и заочной форм обучения.

УДК 512.5(075.8)
ББК 22.14р30

ВВЕДЕНИЕ

Нужно отметить, что математика сегодня - это не только и не столько наука, (причем это одна из немногих наук, которых нет в природе в «чистом виде»), но это и язык любой науки, так как наука только тогда становится наукой, когда она начинает работать с цифрами, сравнивать и анализировать их.

В математике выделяют фундаментальные области, такие как, математическая логика, алгебра и математический анализ, на основе которых появились и создаются другие разделы и области математики, такие как дифференциальные уравнения, дифференциальная геометрия, дискретная математика, теория вероятностей и т.д.

Алгебра, в том виде, в котором её преподают в ВУЗе, является содержательным предметом, в ней много новых понятий, с которыми не знакомят в школе. По мнению автора, студенту, окончившему 1 курс математического факультета нужно:

а) знать, что такое алгебраические структуры и как они образуются;

б) понимать отличие отображений на множествах от морфизмов на алгебраических структурах;

в) знать, что такое поле комплексных чисел и его основные свойства;

г) иметь представление о конечных полях;

д) знать, что такое кольцо многочленов и основные свойства многочленов;

е) иметь понятие о векторном пространстве, и знать его основные свойства;

ж) иметь представление о линейной зависимости или независимости векторов, а вместе с этим знать, что такое система образующих и базис векторного пространства;

з) иметь понятие о кольце матриц и знать свойства некоторых числовых характеристик матриц, таких как, например, определитель матрицы;

и) иметь понятие о линейном отображении между векторными пространствами и линейном операторе, действующем на одном векторном пространстве, а также понимать взаимосвязь кольца матриц $M_m(K)$ и множества всех линейных операторов, действующем на конечномерном векторном пространстве V_K, размерность которого равна m;

ж) иметь представление о собственных значениях и собственных векторах линейного оператора, соответствующих данному собственному значению, уметь их находить, и понимать, что базис, составленный из собственных векторов данного линейного оператора f позволяет упростить матрицу этого линейного оператора f;

з) иметь представление о корневых векторах высоты h, соответствующих собственному значению линейного оператора f, и уметь их находить, что также в конечном счете позволяет упростить матрицу линейного оператора;

и) иметь представление о жордановой форме матрицы линейного оператора, умения находить её и базис, в котором матрица данного оператора принимает жорданов вид;

к) иметь представление об евклидовых и унитарных векторных пространствах и их основных свойствах;

л) понимать взаимосвязь алгебраических структур и иметь представление, какие практические прикладные задачи могут быть решены с их использованием; и наоборот: если есть какая-то прикладная задача, то иметь представление, какие разделы математики, в частности алгебры, могут быть использованы для её решения.

В данном пособии используется тройная нумерация результатов, которая обозначает номер главы, номер параграфа и номер утверждения в данном параграфе.

ОСНОВНАЯ ЛИТЕРАТУРА

КОСТРИКИН А.И. Введение в алгебру (основы алгебры) - М.Наука, 1994. - 318с.
КУРОШ А.Г. Курс высшей алгебры. (изд.9-е) - М.Наука.1968. - 432с.
ФАДДЕЕВ Д.К. Лекции по алгебре - М.Наука.1984. - 416с.

КОСТРИКИН А.И. Сборник задач по алгебре - М.Наука.1989. - 236с.
КУЛИКОВ Л.Я.,МОСКАЛЕНКО А.И.,ФОМИН А.А. Сборник задач по алгебре и теории чисел - М.Просв.1993.- 288с.
ФАДДЕЕВ Д.К.,СОМИНСКИЙ И.С. Сборник задач по высшей алгебре (1изд.) - ОГИЗ.М.Лен.1945. - 304с.

ВСПОМОГАТЕЛЬНАЯ ЛИТЕРАТУРА

ВЕРЕЩАГИН Н.К., ШЕНЬ А. Начало теории множеств- М.,МЦНМО,1997,-128с.
ДАДАЯН А.А., ДУДАРЕНКО В.А. Алгебра и геометрия.-Минск “Вышейшая школа”. 1989. - 221с.
ПОЙА Д. Математика и правдоподобные рассуждения. - М.:Наука.1975.- 464с.

ОБОЗНАЧЕНИЯ: **N** - натуральные числа; **Z** — целые числа, **Q** — рациональные числа, **R** — вещественные числа, **C** — комплексные числа.

$\exists$ - квантор существования; $\exists!$ – квантор существования и единственности такого существования; $\forall$ - квантор всеобщности.

Будем понимать под записью $\sum_{i=1}^{n} x_i$ - сумму n чисел: $x_1 + x_2 + \ldots + x_n$, а под записью $\prod_{i=1}^{n} x_i$ - их произведение - $x_1 x_2 \ldots x_n$.

ЗАМЕЧАНИЕ. Основная сложность курса общей алгебры, который изучается на 1-м курсе ВУЗа, заключается не в сложности рассматриваемых результатов, а в большом количестве новых понятий, которые не так просто согласовать и связать между собой.

Следует заметить ещё тот факт, что в современной алгебре очень много различий в обозначениях, и нередко в литературе встречаются малосущественные различия и в определениях, так как нет общепризнанной символики и терминологии. Часто все зависит от автора курса и (или) учебника, по которому изучается данный курс.

ГЛАВА 1. МНОЖЕСТВА
§1.1. МНОЖЕСТВА, ПОДМНОЖЕСТВА И ИХ ВИДЫ

ОПР. Под **множеством** A понимают любую совокупность различных объектов, называемых элементами множества.

Обычно для этого используют следующие обозначения: если A – множество, элементами которого являются какие-то объекты a, b, c,… , то это записывается таким образом: A ={a,b,c,...}.

Введем следующие обозначения, которые достаточно широко распространены в курсе всей математики:

$a \in A$ - элемент a лежит в множестве A, как элемент,

$a \notin A$ - элемент a не является элементом множества A.

$B \subset A$ или $B \subseteq A$ множество B лежит в A как подмножество, в первом случае, оно строго меньше множества A, во втором подмножество B может совпадать с A.

ЗАМЕЧАНИЕ. Подробнее об этом см. ниже.

ОПР. Множество, не содержащее элементов, называется **пустым множеством** и обозначается следующим образом **Ø.**

Если введено понятие множества, тогда нужно определить, когда эти множества равны.

ОПР. **Множество A равно множеству B** (или **совпадает с множеством B**), если они состоят из одних и тех же элементов (будем это записывать так **A=B**). В противном случае говорят, что множество **A не равно множеству B** (будем записывать это так $A \neq B$).

ЗАМЕЧАНИЕ. Заметим, что это (множество A не равно множеству B) означает, что найдется элемент a из A, который не лежит в B, или наоборот, найдется элемент b из B, который не лежит в A. Понятно, что возможны и оба случая одновременно.

ОПР. Множество B является **подмножеством множества A**, если любой элемент множества B является элементом множества A. Это обозначается следующим образом: $B \subseteq A$.

На языке введенных символов и кванторов данное определение можно записать таким образом: если $(\forall b \in B \Rightarrow b \in A)$, то $B \subseteq A$.

ЗАМЕЧАНИЕ. Заметим, что если подмножество B строго лежит в A, то в A найдется такой элемент a, который не лежит в B. Этот случай будем записывать так: $B \subset A$.

По определению будем полагать, что пустое множество - **Ø** - входит в число

подмножеств любого множества.

ПРИМЕРЫ. а) числовые множества: $N \subset Z \subset Q \subset R$;

б) множество многочленов с целыми коэффициентами от одной переменной (обозначается так Z[x]);

в) множество матриц из 2 строк и 3 столбцов (обозначается через $M_{2,3}(R)$)

$$M_{2,3}(R)=\left\{\begin{pmatrix} a,b,c \\ d,e,f \end{pmatrix} \text{ a,b,c,d,e,f - вещественные числа}\right\}$$

ОПР. Если число элементов в множестве A конечно, то A называется **конечным множеством**, и число его элементов называется порядком множества A (обозначается через $|A|$ или $\overline{A}$); если число элементов в A бесконечно, тогда множество называется **бесконечным множеством** и говорят уже не о порядке, а о мощности множества: счетное множество, множество мощности континиум, и т.д. (об этом подробнее будет говориться в курсе топологии).

ОПР. Подмножество B называется **собственным подмножеством множества A**, если B не пустое множество и B не совпадает с A.

УПР. Найти все собственные подмножества множества A={1,2,3}.

Докажем один простой, но достаточно важный результат, который почти очевиден, но….всегда полезно уметь доказывать такие «очевидные» утверждения.

ЛЕММА 1.1.1.Если $A \subseteq B$ и $B \subseteq A$, тогда A=B.

Доказательство. Рассмотрим произвольный элемент a из A. По условию, так как $A \subseteq B$, то a лежит и в множестве B.

Рассмотрим произвольный элемент b из B. По условию, так как $B \subseteq A$, то b лежит и в A. Отсюда получаем, по определению, что множества A и B равны между собой, так как все элементы каждого множества являются элементами и другого множества.

Заметим, что верно и обратное равенство, т.е. если A=B, то отсюда следует, что $A \subseteq B$ и $B \subseteq A$. Просто в этом случае A и B несобственные или тривиальные подмножества друг друга.

ЗАМЕЧАНИЕ. Доказательство леммы 1.1.1 показывает, каким образом может происходить доказательство равенства каких-то двух множеств. Оно состоит из двух шагов: сначала показывается, что одно множество входит в состав другого, а затем наоборот, показывается, что второе множество входит в состав первого. И вот тогда, на основании леммы 1.1.1, следует равенство множеств.

ОПР. Если все элементы бесконечного множества A можно перенумеровать с помощью натуральных чисел, тогда такое множество называется **счётным множеством.**

ЗАМЕЧАНИЕ. Для установления счетности множества А вовсе необязательно задать счёт явно, т.е. этот элемент множества А является первым, тот – вторым и т.д. Бывает нередко установить взаимно-однозначное соответствие между множеством А и множеством **N**. Это взаимно-однозначное соответствие и показывает, что данное множество счётно, так как само множество натуральных чисел, очевидно, счётное множество.

ПРИМЕРЫ: а) множество положительных четных чисел —оно счётно.

Каждое чётное число можно записать в виде 2k, где k-некоторое натуральное число. Поставим каждому такому числу в соответствие число k. Получим соответствие между множеством чётных чисел и множеством натуральных чисел. Таким образом мы «перенумеровали» все чётные числа.

б) множество всех целых чётных чисел также является счётным множеством.

Докажем это. Произвольное чётное число имеет вид 2k. Положим, что 0 будет иметь номер 1. Далее, если k>0, то 2k будет соответствовать натуральное число 2k, а если k<0, то 2k будет соответствовать число $2|k|+1$. Как несложно заметить, все чётные числа будут перенумерованы.

в) множество положительных вещественных чисел меньших 1 – не является счётным множеством.

УПР. а) Доказать, что **Q** — счётное множество.

б) Доказать, что множество непересекающихся и не лежащих друг в друге окружностей, центры которых лежат правее некоторой точки на фиксированной прямой является счётным множеством.

§1.2. ПЕРЕСЕЧЕНИЕ, ОБЪЕДИНЕНИЕ МНОЖЕСТВ И ИХ СВОЙСТВА

ОПР. **Пересечением множеств S и T** называется множество элементов, которые лежат и в S и в T (обозначается это множество таким образом: $S \bigcap T$).

ОПР. **Объединением двух множеств S и T** называется множество, элементы которого лежат либо в S либо в T (обозначается это множество таким образом: $S \bigcup T$).

ОПР. **Разностью множеств S и T** называется множество элементов, лежащих в S и не лежащих в T (обозначается разность через S\T (или S-T)). Если T лежит в S, тогда говорят что S\T это **дополнение множества T до множества S**.

По аналогии с этими определениями можно дать определения объединения и пересечения любого конечного числа множеств.

ОПР. **Пересечением множеств $A_1,A_2,...,A_k$** называется множество элементов, которые лежат в каждом из этих множеств (обозначается это множество через $A_1 \quad A_2 \quad ... \quad A_k$ или $\bigcap_{i=1}^{n} A_i$).

ОПР. **Объединением множеств $A_1,A_2,...,A_k$** называется множество, содержащие все элементы, которые лежат в каком-либо из множеств A_i, i=1,2,..,k, (обозначается это через $A_1 U A_2 U ... U A_k$ или $\bigcup_{i=1}^{n} A_i$).

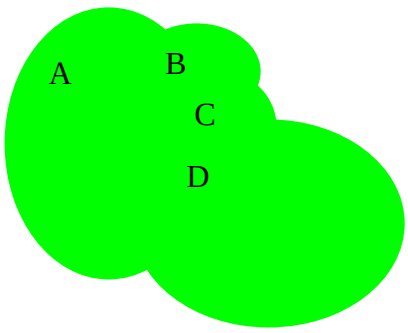


Рис.1

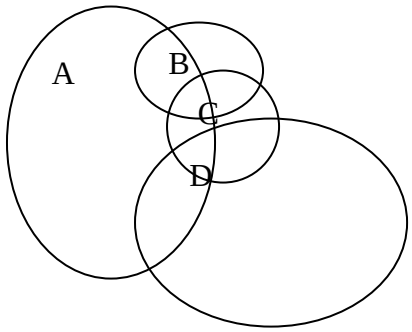


Рис. 2

На рисунке 1 показано объединение четырех множеств A, B, C, D.
На рисунке 2 несложно заметить, что пересечение этих же 4-х множеств образует пустое множество, так как нет общих для всех 4-х множеств точек.

Рассмотрим ряд лемм, о свойствах пересечений и объединений, которые достаточно часто используются и в других разделах математики.

ЛЕММА 1.2.1. (Свойства пересечения)

а) A B=B A; б) A A = A;

в) если A⊆B, то A B=A.

Доказательство. Свойства а) и б) следуют сразу из определения пересечения. Докажем свойство в). Если x∈A, то x∈B (из того, что A подмножество в B). Тогда x∈A B. Отсюда получаем, что A⊆A B.

Пусть x∈A B, тогда x∈A. Отсюда A B⊆A. По лемме 1.1.1 отсюда следует, что множества A и A B равны.

Аналогичные свойства выполняются и для объединения множеств.

ЛЕММА 1.2.2. (Свойства объединения)

а) A∪B=B∪A; б) A∪A = A;

в) если A лежит в B, тогда A∪B=B.

УПР. Доказать справедливость свойств а)-в) леммы 1.2.2.

ЛЕММА 1.2.3. Пусть R, T и S — множества. Доказать, что справедливы формулы:

а) R∪(S T) =(R∪S) (R∪T);

б) R (S∪T) = (R S)∪(R T)

Доказательство а). Пусть x∈R∪(S T). Тогда либо x∈R либо x∈ S T. Если x лежит в R, то x лежит и в (R∪S) (R∪T). Если x∈S T, то x∈S и x∈T. Следовательно, x∈R∪S и x∈R∪T, т.е. x∈(R∪S) (R∪T). Таким образом, мы доказали, что R∪(S T)⊆(R∪S) (R∪T).

Пусть x∈(R∪S) (R∪T). Тогда x∈(R∪S) и x∈(R∪T). Если x∈R, то x∈R∪(S T). Если x∈S\R и x∈T\R, тогда x∈S T. Но тогда x∈ R∪(S T). Получили, что (R∪S) (R∪T)⊆R∪(S T). По лемме 1.1.1 отсюда следует, что два множества равны.

УПР. Доказать свойство б) леммы 1.2.3.

А сейчас мы рассмотрим одно важное множество, которое хорошо известно в курсе математики, но оказывается, что структура его построения имеет большое значение для обоснования метода математической индукции, который играет важную роль во всех областях математики.

§1.3 МНОЖЕСТВО НАТУРАЛЬНЫХ ЧИСЕЛ. АКСИОМАТИКА

В 1893 году итальянский математик Пеано сформулировал аксиомы, которые полностью определяют структуру множества натуральных чисел. Сформулируем их.

1^{o}. На множестве натуральных чисел **N** существует единица, будем обозначать её через 1.

2^{o}.Для каждого элемента a из **N** найдется последующий за ним элемент, будем обозначать его через a', и такой элемент единственный для каждого натурального числа a.

3^{o}. Каждый элемент множества натуральных чисел, кроме 1, является последующим для некоторого другого элемента b из **N.**

4^{o}. Если равны последующие элементы, тогда равны и сами элементы, т.е. если a'=b', то a=b.

5^{o}. Пусть M — некоторое подмножество в **N**, такое, что 1 лежит в M, и из условия, что a лежит в M, следует, что и a' также лежит в M. Тогда M=**N.**

На основе пятой аксиомы Пеано для **N** получается утверждение принципа математической индукции.

ЛЕММА 1.3.1 (Принцип математической индукции) Пусть на множестве натуральных чисел **N** сформулировано некоторое утверждение P(n). Если данное утверждение верно для n=1, и из предположения его истинности для n следует истинность утверждения для n+1, то это утверждение истинно для всех натуральных чисел.

Доказательство: принимаем за M подмножество множества всех натуральных чисел n, для которых утверждение P(n) верно. Последующим n' для n будем считать натуральное число n+1.

Допустим, что P(1) верно. (Если это не так, тогда утверждение P(n) не является истинным для всех натуральных чисел, однако, утверждение принципа математической индукции от этого не перестает быть верным!).

Пусть P(n) верно, т.е. n лежит в M. Тогда по условию и P(n+1) также верно, т.е. и последующее для n число n+1 —также лежит в M. Отсюда по пятой аксиоме Пеано следует, что M=**N,** т.е. утверждение P(n) верно для всех натуральных чисел.

Таким образом, согласно принципу математической индукции, проверка истинности для бесконечного числа утверждений заменяется проверкой двух вещей:

— истинности утверждения P для n=1, т.е. истинно ли P(1); это называется **базой индукции:**

— и истинности P(n+1), в предположении, что P(n) истинно; это называется проверка индукционного шага, а предположение, что P(n) истинно — **индукционной гипотезой.**

ЗАМЕЧАНИЕ. Заметим, что принцип математической индукции действует уже

не просто на множестве натуральных чисел, а на множестве, где заданы операции.

Более подробно о методе математической индукции можно посмотреть в книге Пойа Д. «Математика и правдоподобные рассуждения» М.Наука.1975г.464с.

Разберем пример.

ПРИМЕР: а) Доказать, что сумму первых n натуральных чисел можно вычислить по формуле $1+2+3+...+n = \frac{n(n+1)}{2}$.

1 ШАГ. Проверяем базу, т.е. верна ли формула для n=1.

$$1=\frac{1(1+1)}{2}.$$

Формула верна.

2 ШАГ. Проверяем, верен ли индукционный шаг.

Пусть для n формула верна, докажем, что и для n+1 формула также верна.

Рассмотрим сумму 1+2+3+….+n+(n+1). По индукционному предположению сумму первых n слагаемых можно вычислить по формуле $\frac{n(n+1)}{2}$. Тогда всю сумму можно переписать в виде

$$1+2+3+….+n+(n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)((n+1)+1)}{2}.$$

Отсюда видно, что формула верна и для (n+1)-о слагаемого. Следовательно, по принципу математической индукции, формула верна для любого натурального числа.

Метод математической индукции иногда позволяет не только доказать равенство, но и выдвинуть гипотезу для нахождения нужной формулы, а уже затем доказать, что данная формула верна.

Рассмотрим следующую задачу.

Найти формулу для суммы

$$S_n = 1 + 3 + 5 + 7 + 9 +....+ (2n-1),$$

где n – произвольное натуральное число.

Решение. Применяем формулу для нескольких первых натуральных чисел n=1, 2, 3, и т.п., пока не заметим некоторой закономерности для получения этой суммы.

Итак, рассмотрим n=1. Тогда S=1.

Положим n=2. Тогда S=1+3=4.

Положим n=3. Тогда S=1+3+5=9.

Видим, что сумма первых n нечётных натуральных чисел равна n^2. Выдвигаем гипотезу.

ГИПОТЕЗА. Сумма первых n нечётных чисел равна n^2, т.е.

$$S=1+3+5+… +(2n - 1)= n^2 \qquad (*).$$

Докажем сейчас это утверждение с помощью метода математической индукции.

Проверяем базу. n=1, $S=1=1^2$. Видим, что формула (*) верна.

Предположим, что для всех натуральных, не превосходящих n, формула для

вычисления суммы (*) верна. Докажем, что она выполняется и для суммы (n+1)-го нечётного слагаемого.

Рассмотрим сумму 1 + 3 + 5 +… + (2n-1) + (2n+1). По индукционному предположению для первых n слагаемых формула (*) верна, т.е. 1 + 3 + 5 + … + (2n-1) = n^2. Тогда получаем, что

$$1+3+5+\ldots+(2n-1)+(2n+1) = n^2+2n+1 = (n+1)^2.$$

Таким образом, формула (*) верна и для n+1. А это и требовалось показать. Следовательно, по принципу математической индукции формула (*) выполняется для всех натуральных n.

Позднее, когда мы будем говорить про алгебраические структуры, мы введем операции, которые придают данным (известным) множествам те свойства, которые мы изучали в школе.

УПР. На сколько частей разобьют плоскость n прямых общего положения, т.е. когда никакие две прямые не параллельны, и никакие три не проходят через одну точку?

ЗАМЕЧАНИЕ. Нужно отметить, что базой индукции может быть и другое натуральное число $n_o>1$, если утверждение задачи было сформулировано в таком виде: доказать, что для всех натуральных чисел n, таких, что $n\geq n_o$ справедливо утверждение P(n). Здесь нужно, чтобы истинность утверждения была проверена для этого n_o, а далее все действия проходят совершенно аналогично указанному выше методу математической индукции.

Используя метод математической индукции, можно обобщить результат леммы 1.2.3, что мы сейчас и проделаем.

ЛЕММА 1.3.2. Пусть $R,S_1,S_2,\ldots,S_n$ - множества, тогда для них справедливы следующие равенства:

а) $R\ (S_1 U S_2 U \ldots U S_n)=(S_1 U S_2 U \ldots U S_n)\ R=(R\ S_1)U(R\ S_2)U\ldots U(R\ S_n)$;

б) $RU(S_1\ S_2\ \ldots\ S_n)=(S_1\ S_2\ \ldots\ S_n)UR=(RUS_1)\ (RUS_2)\ \ldots\ (RUS_n)$

Доказательство а) Докажем п. а) на основе леммы 1.2.3 методом математической индукции по n.

Рассмотрим базу при n=1. Понятно, что утверждение леммы верно.

Рассмотрим еще один случай, когда n=2. Но это утверждение леммы 1.2.3, т.е. утверждение а) также верно.

Допустим, что для любого числа множеств, не превосходящего n, утверждение а) верно. Рассмотрим случай, когда множеств n+1, n>1.

Нужно доказать, что

$$R\ (S_1 U S_2 U \ldots U S_n U S_{n+1}) = (R\ S_1)U(R\ S_2)U\ldots U(R\ S_n)U(R\ S_{n+1}).$$

Обозначим $S_1 U S_2 U \ldots U S_n$ через B. Тогда, по лемме 1.2.3 получаем, что $RB(\cap U S_{n+1})=(RB\cap)U(R\cap S_{n+1})$. По предположению индукции отсюда получаем, что $RB(\cap U S_{n+1})=(RB\cap)\ U(R\cap S_{n+1}) = (R\cap S_1)U(R\cap S_2)U\ldots U(R\cap S_n)U(R\cap S_{n+1})$. А это и требовалось доказать.

УПР. Доказать свойство б) леммы 1.3.2.

§1.4. КОМБИНАТОРНЫЕ СВОЙСТВА МНОЖЕСТВ И ИХ ПОДМНОЖЕСТВ

ЗАМЕЧАНИЕ. Нужно отметить, что когда речь идет о комбинаторных свойствах множеств, то обычно подразумевается, что речь идет о конечных множествах, т.е порядки этих множеств и их подмножеств конечны. Однако, методы современной комбинаторики позволяют работать и с бесконечными множествами. Но комбинаторные свойства таких множеств мы в данной брошюре не будем рассматривать.

Ещё раз напомню, что если A конечное множество, то символом |A| обозначается порядок множества A, т.е. количество элементов в нём. Сейчас мы докажем один достаточно важный результат и его обобщение, которые нами будут использоваться в дальнейшем курсе лекций.

ЛЕММА 1.4.1. Пусть $A_1, A_2,.., A_n$ – конечные множества, и пусть $|A_1|, |A_2|,.., |A_n|$ - порядки этих множеств. Тогда для них справедливы следующие утверждения:

а) $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

б) $\left|A_1 \cup A_2 \cup ... \cup A_n\right| = |A_1| + |A_2| + ... + |A_n| - \sum_{1\le i<j\le n}\left|A_i \cap A_j\right| + \sum_{1\le i<j<k\le n}\left|A_i \cap A_j \cap A_k\right| + .. + (-1)^n\left|\bigcap_{i=1}^{n} A_i\right|$

Доказательство. а) Понятно, что общие элементы, которые входят и в A_1 и в A_2 (т.е.элементы, входящие в $A_1 \cap A_2$) будут считаться два раза, когда будем подсчитывать сумму порядков A_1 и A_2, т. е. сумма $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$. Что и требовалось доказать.

б). Для доказательства этого пункта будем использовать метод математической индукции по числу множеств n.

Понятно, что для n=1 и n=2 все очевидно и уже показано в п.а).

Пусть для всех не превосходящих n утверждение верно, докажем, что оно верно и для n+1. $|A_1 \cup A_2 \cup ... \cup A_{n...} \cup A_{n+1}| =$ |обозначим через $B = A_1 \cup A_2 \cup ... \cup A_n$| $= |B| + |A_{n+1}| - |B \cap A_{n+1}| =$ (по предположению индукции для B)

$$= |A_1| + |A_2| + ... + |A_n| + |A_{n+1}| - \sum_{1\le i<j\le n}\left|A_i \cap A_j\right| + \sum_{1\le i<j<k\le n}\left|A_i \cap A_j \cap A_k\right| + ... + (-1)^n\left|\bigcap_{i=1}^{n} A_i\right| -$$

$$- |(A_1 \cup A_2 \cup \ldots \cup A_n) \cap A_{n+1}| = \text{(по п.а Леммы 1.3.2)} =$$

$$= |A_1| + |A_2| + ... + |A_n| + |A_{n+1}| - \sum_{1\le i<j\le n}\left|A_i \cap A_j\right| + \sum_{1\le i<j<k\le n}\left|A_i \cap A_j \cap A_k\right| + ...$$

$$+(-1)^n\left|\bigcap_{i=1}^{n} A_i\right| - |(A_1 \cap A_{n+1}) \cup (A_2 \cap A_{n+1}) \cup ... \cup (A_n \cap A_{n+1})|$$

$$= \text{(по предположению индукции для B (n множеств))} =$$

$$= |A_1| + |A_2| + ... + |A_n| + |A_{n+1}| - \sum_{1\le i<j\le n}\left|A_i \cap A_j\right| + \sum_{1\le i<j<k\le n}\left|A_i \cap A_j \cap A_k\right| + ... + (-1)^n\left|\bigcap_{i=1}^{n} A_i\right| -$$

$$- \left(|A_1 \cap A_{n+1}| + |A_2 \cap A_{n+1}| + \ldots + |A_n \cap A_{n+1}| - \sum_{1\le i<j\le n}\left|A_i \cap A_j \cap A_{n+1}\right| + .. + (-1)^n\left|\bigcap_{i=1}^{n+1} A_i\right|\right) =$$

$$= |A_1| + |A_2| + ... + |A_n| + |A_{n+1}| - \sum_{1\le i<j\le n+1}\left|A_i \cap A_j\right| + \sum_{1\le i<j<k\le n+1}\left|A_i \cap A_j \cap A_k\right| + ... + (-1)^{n+1}\left|\bigcap_{i=1}^{n+1} A_i\right|.$$

Что и требовалось доказать.

Рассмотрим пример использования полученной формулы.

ПРИМЕР: Найти количество натуральных чисел, которые не превышают 100 и делятся на 2 или на 5.

Решение. Положим, что A_2 -натуральные числа, не превосходящие 100 и делящиеся на 2, A_5 - натуральные числа, не превосходящие 100 и делящиеся на 5. Тогда $|A_2| = 50$, $|A_5| = 20$. Количество чисел, делящихся на 2 и на 5, т.е.на 10 , и не превосходящие 100, равно 10 штук. Отсюда по лемме 1.4.1 получаем, что искомое число равно $|A_2 \cup A_5| = |A_2| + |A_5| - |A_2 \cap A_5| = 50 + 20 - 10 = 60$.

Рассмотрим некоторые комбинаторные свойства множеств и их подмножеств.

ОПР. Перенумерация элементов конечного множества A называется **перестановкой множества A**.

ПРИМЕР: A={a,b,c}. Тогда перестановками данного множества будут следующие тройки (a,c,b), (a,b,c) и (c,b,a), в которых указано, какой элемент стоит на каком месте.

ЛЕММА 1.4.2. Число различных перестановок в конечном множестве A из n элементов равно $n!=1\cdot 2\cdot \ldots \cdot n$.

Доказательство. Пусть в A n различных элементов. Тогда покажем это свойство, используя строку из n клеточек, в i-ой из клеток которой будем записывать количество возможных выборов для элемента, стоящего на i-ом месте.

1-е	2-е	3-е		(n-1)-е	n-е
			…….		

Итак, для выбора первого элемента есть ровно n кандидатов, т.е. любой элемент из n. Понятно, что после того, как выбрали один, в любом случае остался n-1 элемент. Значит, для выбора элемента, который расположен на втором месте, всегда будет ровно n-1 элемент. Вновь, после того, как выбрали кандидата на второе место, остаётся n-2 элемента, следовательно, для выбора третьего – всегда n-2 варианта, и т.д.. И для выбора последнего всегда (независимо от выбора оставшихся 1,2,3,…,(n-1)-го) остаётся ровно 1 элемент. Таким образом, получаем, что в таблице будут записаны следующие числа.

1-е	2-е	3-е		(n-1)-е	n-е
n	n-1	n-2	…….	2	1

Следовательно, так как количество выборов следующего кандидата не зависит от выбора предыдущих, получаем, что общее число выборов n кандидатов равно n!

Положим по определению, что 0!=1.

ОПР. Количество выборов k элементов из данных n называется **числом сочетаний из n по k**, обозначается C_n^k.

ЛЕММА 1.4.3 Число сочетаний из n по k элементов, т.е. количество наборов по k элементов из n ($k \le n$) элементов равно $C_n^k = \frac{n!}{k!(n-k)!}$

Доказательство. Для доказательства используем прием со строкой только из k клеток.

n	n-1	n-2	…….	n-(k-2)	n-(k-1)

Таким образом общее количество выборов k элементов из данных n (при условии, что $k \le n$) равно n(n-1)….(n-(k-1)). Однако, как несложно заметить, каждый такой набор повторяется ровно k! раз, так как выбрать одни и те же k элементов можно ровно k! способами. Следовательно, общее число различных подмножеств из k элементов равно $\frac{n(n-1)...(n-(k-1))}{k!}$. Умножим числитель и знаменатель этой дроби на (n-k)! И получим, что данное выражение будет равно

$$\frac{n(n-1)...(n-(k-1))(n-k)!}{k!(n-k)!} = \frac{n!}{k!(n-k)!}$$

Что нам и требовалось доказать.

УПР: вычислить $C_5^2; C_6^5$.

Рассмотрим несколько простейших свойств числа сочетаний. (Заметим, что есть несколько книг по различным свойствам числа сочетаний C_n^k. См., например, брошюру УСПЕНСКИЙ В.А. Треугольник Паскаля. Серия "Популярные лекции по математике" вып.43.М.Наука.1979.48с.)

ЛЕММА 1.4.4. Докажем, что $C_n^k = C_n^{n-k}$.

Доказательство. Доказательство данного утверждения легко получить из леммы 1.4.3, зная, как вычисляется C_n^k.Однако, это доказательство можно получить и из того замечания, что если мы выбираем какие-то k элементов из данных n элементов, то тем самым мы «выбираем» и оставшиеся (n-k) элементов. Причем, понятно, что если остались какие-то (n-k) элементов, то выбрали именно те k элементов, которых в этом множестве нет. Таким образом, мы получили взаимно однозначное соответствие между этими подмножествами: множеством из k элементов и множеством из оставшихся (n-k).

Число сочетаний из n по k широко используются в различных областях математики. Сейчас мы рассмотрим, как число сочетаний из n по k используется при вычислении коэффициентов бинома Ньютона, т.е. нахождения коэффициентов в разложении $(a+b)^n$. (В большинстве литературы C_n^k называются биномиальными коэффициентами).

Рассмотрим коэффициенты при $a^{n-k}b^k$ в разложении степеней выражения $(a+b)^n$

n=0	1	$(a+b)^o$
n=1	1 1	$(a+b)^1$
n=2	1 2 1	$(a+b)^2$
n=3	1 3 3 1	$(a+b)^3$

……

Оказывается, что все полученные результаты можно обобщить в виде теоремы.

ТЕОРЕМА 1.4.5. (Формула Бинома Ньютона)

$$(a+b)^n = C_n^o a^n b^o + C_n^1 a^{n-1}b^1 + C_n^2 a^{n-2}b^2 + .. + C_n^n a^o b^n.$$

Доказательство. Каждое слагаемое в полученном произведении будет иметь вид произведения n элементов: k –элементов a, а остальные (n-k) - элементы b. Это связано с тем, что рассматривается n скобок: (a,b)(a,b)....(a,b). Из каждой скобки выбирается ровно по одному элементу (либо a, либо b), поэтому вид каждого слагаемого в полученной сумме будет иметь вид $a^k b^{n-k}$.

С каким коэффициентом он войдет в формулу бинома?

Как несложно понять этот коэффициент равен C_n^k, так как мы выбираем из n скобок ровно k элементов a (можно считать, что в каждой скобке элемент a «отличен от других»), а все остальные множители b уже заранее предопределены. Поэтому и получаем формулу, которая приведена в условии.

УПР. Исследовать, как будет выглядеть формула $(a+b+c)^n$.

Оказывается, знание бинома Ньютона очень легко позволяет решить ещё одну интересную задачу.

ТЕОРЕМА 1.4.6. (Теорема о числе подмножеств). Число различных подмножеств в конечном множестве A, состоящем из n элементов, равно 2^n.

Доказательство. Каждое подмножество множества A содержит k-элементов, k=0,1,2,…,n, т.е это подмножество входит в одно (и только одно) C_n^k. Поэтому для нахождения количества всех подмножеств данного множества нужно подсчитать сумму

$$C_n^o + C_n^1 + C_n^2 + C_n^3 + .. + C_n^n.$$

Но для этого достаточно в биноме Ньютона подставить в качестве чисел a и b числа, равные 1. Получим необходимое равенство

$$2^n = C_n^o + C_n^1 + C_n^2 + C_n^3 + .. + C_n^n.$$

Формула Бинома Ньютона позволяет считать и некоторые суммы биномиальных коэффициентов.

ПРИМЕР. Найти сумму конечного ряда

$$C_n^o - C_n^1 + C_n^2 - C_n^3 + .. + (-1)^n C_n^n . \qquad (1)$$

Решение. В формуле бинома Ньютона нужно положить a = - b =1. Тогда и получим, что данное выражение (1) равно 0.

Отсюда можно сделать вывод, что сумма биномиальных коэффициентов, где верхний индекс пробегает чётные значения, равен сумме биномиальных коэффициентов, где верхний индекс пробегает все нёчетные значения и равно (в силу т.1.4.6) 2^{n-1}.

ЗАМЕЧАНИЕ. Достаточно часто нахождение сумм биномиальных коэффициентов сводится к подбору нужных чисел a и b, а также к суммированию и (или) преобразованию некоторых полученных выражений.

Более подробно о методе математической индукции и о различных способах вычисления сумм биномиальных коэффициентов также можно найти в книге Пойа Г. «Математика и правдоподобные рассуждения» М.Н.1978.

Глава 2. АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

ЗАМЕЧАНИЕ. Заметим, что рассмотрение алгебраических структур можно вести аналогично рассмотрению множеств и их свойств: множество – подмножества –собственные и не собственные подмножества множества и т.д..

§2.1.ПОЛУГРУППЫ. МОНОИДЫ. ГРУППЫ

ОПР. Отображение (произвольное, но фиксированное) $X \times X \to X$, т.е. каждой паре (a,b), где a и b из X, ставится элемент c из X, называется **бинарной операцией на X.**

ЗАМЕЧАНИЕ. Аналогично можно определить n-арную операцию на множестве X. Для этого берется произвольный набор из n элементов множества X, и ему сопоставляется один элемент множества X.

Нужно также отметить, что если операция не обладает свойством ассоциативности, то n-арную операцию в общем случае нельзя свести к рассмотрению бинарной операции на X. Если же операция ассоциативна, тогда эту операцию можно свести к рассмотрению бинарной операции.

Часто операцию на множестве X обозначают каким-то специальным значком: *, или o, или каким-то другим образом. Будем называть операцию * **умножением.** (Часто умножение обозначается просто приписыванием двух букв друг к другу, без всяких знаков). Особо будем выделять операцию, которая обозначается знаком «+» и будем называть ее **сложением.**

ОПР. Если на множестве X задана бинарная операция *, то говорят, что на множестве X определена **алгебраическая структура**, которая обозначается через (X,*)

ЗАМЕЧАНИЕ. 1) Если на множестве задано несколько операций «*»,… ,«o», тогда обозначение для такой алгебраической структуры имеет вид (X,*,...., o).

2) Нередко, по ходу работы с множеством X, действующая на данном множестве операция очевидна, поэтому вместо алгебраической структуры (X,*) пишут просто X (подразумевая, что на нем рассматривается действующая операция).

ПРИМЕРЫ: а) на **Z** - «+» - операция сложения; б) на **Z** - «×» - операция умножение ; в) на Z операция o: aob = a+b-ab.

ОПР. Бинарная операция * на множестве X называется **ассоциативной**, если (a*b)*c = a*(b*c)=a*b*c для всех a,b,c из X.

ОПР. Операция на множестве X называется **коммутативной**, если a*b = b*a, для любой пары элементов a и b из X.

ЗАМЕЧАНИЕ. В некоторых книгах те же наименования (что и операция), начинает носить и алгебраическая структура, которая образуется с этой операцией на X. Если операция умножение, тогда говорят, что структура – **мультипликативная**, если – сложение, тогда структура – **аддитивная**.

ЗАМЕЧАНИЕ. Заметим также, что требования ассоциативности и коммутативности между собой независимы, т.е. есть структуры, которые ассоциативны, но не коммутативны, и наоборот.

ПРИМЕР: а) на Z рассмотрим операцию: m*n = -m-n. Она коммутативна, но не ассоциативна, (1*2)*3 = (-1-2)*3 = -(-1-2)-3 = 0 ≠ 4 = 1*(2*3) = -1-(-(2+3)).

б) Рассмотрим операцию умножения на множестве квадратных матриц $M_{2,2}(R)$ множество матриц из 2 строк и 2 столбцов $M_{2,2}(R)=\{\begin{pmatrix} a,b \\ c,d \end{pmatrix}$ a,b,c,d, - вещественные числа$\}$. На этом множестве зададим операцию умножения:

$$\begin{pmatrix} a,b \\ c,d \end{pmatrix}\begin{pmatrix} x,y \\ z,t \end{pmatrix} \overset{\Delta}{=} \begin{pmatrix} ax+bz, ay+bt \\ cx+dz, cy+dt \end{pmatrix}.$$

Как несложно проверить, данная операция ассоциативна, но не коммутативна.

ОПР. Элемент e из X называется **единичным** для бинарной операции * на X, если a*e = e*a = a для любого элемента множества X (такой элемент e будем обозначать через $\mathbf{e_X}$ или $\mathbf{1_X}$).

ЗАМЕЧАНИЕ. Особым образом записывается и называется единичный элемент, когда на множестве X задана операция сложения «+». Тогда единичный элемент называется **нулевым** или **нейтральным** и обозначается через $\mathbf{O_X}$.

УПР. Доказать, что если на X существует 1_X, то она единственная.

ОПР. Множество X, с заданной на нем бинарной ассоциативной операцией называется ***полугруппой***. Полугруппу с единичным (нейтральным) элементом называют ***моноидом*** (или полугруппой с единицей). Единицу полугруппы (или моноида) обозначают $\mathbf{1_X}$ или $\mathbf{e_X}$.

ЗАМЕЧАНИЕ. Обычно, если на моноиде M рассматривается операция умножения *, то говорят, что (M,*,e) —**мультипликативный моноид** (и вообще, когда говорят про мультипликативность, как уже отмечено выше, подразумевают операцию умножения), а когда —сложение, то (M,+,0) — **аддитивный моноид**.

ОПР. Пусть (X,*) моноид с единицей e_X. Если для элемента x из этого моноида найдется элемент y из X, такой что, $x*y=y*x=e_X$, то говорят, что элемент **x обратим**, а элемент y называется **обратным к x элементом** (такой элемент y обозначается как $\mathbf{x^{-1}}$).

ПРИМЕРЫ: а) $(Z,+)$, в Z есть нулевой элемент - 0, т.е. – это моноид;
б) $(Z,\times)$, в Z есть и единичный элемент - 1, т.е. и это моноид;

в) в R выбирается произвольный элемент (пусть π) и рассматривается операция * (умножение) $(a,b)\to a*b = a\pi b$.

Покажем, что (R,*) — моноид.

То, что операция ассоциативна следует из того, что операция умножения ассоциативна на вещественных числах.

Какой элемент будет единицей в (R,*)? Понятно, что это $e=\pi^{-!}$. Берем любой элемент a из R. Тогда $a*\pi^{-1} = \pi^{-1}*a = \pi^{-1}\pi a = a$. Значит, (R,*) — моноид.

ОПР. Если полугруппа G конечна и имеет n элементов, то говорят, что G ***имеет порядок*** n.

ОПР. Подмножество S' в S с операцией * называется ***подполугруппой*** в (S,*), если для всех x и y из S' x*y лежит в S'. Говорят, что подмножество S' в S замкнуто относительно операции *.

ОПР. Если $H\subseteq G$, где G – моноид, H относительно операции на G образует моноид, тогда H называется **подмоноидом моноида G.**.

ПРИМЕРЫ: а) $(2Z,+)$ в $(Z,+)$ является подмоноидом.

б) Пусть X - множество диагональных матриц по сложению с нулевыми правыми нижними элементами, т.е. матриц вида: $\begin{pmatrix} a,0 \\ 0,0 \end{pmatrix}$. Положим по определению, что $\begin{pmatrix} a,0 \\ 0,0 \end{pmatrix}+\begin{pmatrix} b,0 \\ 0,0 \end{pmatrix} \stackrel{\Delta}{=} \begin{pmatrix} a+b,0 \\ 0,0 \end{pmatrix}$. Несложно заметить из определения, что сумма двух матриц также является матрицей аналогичного вида, т.е. если A и B лежат в X, то и A+B также лежит в X. Также замечаем, что для этой операции выполняется свойство: $\begin{pmatrix} a,0 \\ 0,0 \end{pmatrix}+\left(\begin{pmatrix} b,0 \\ 0,0 \end{pmatrix} + \begin{pmatrix} c,0 \\ 0,0 \end{pmatrix}\right) = \left(\begin{pmatrix} a,0 \\ 0,0 \end{pmatrix}+\begin{pmatrix} b,0 \\ 0,0 \end{pmatrix}\right) + \begin{pmatrix} c,0 \\ 0,0 \end{pmatrix} = \begin{pmatrix} a+b+c,0 \\ 0, \quad 0 \end{pmatrix}$. Таким образом, ассоциативность сложения выполняется.

В X есть нулевой элемент, а именно, нулевая матрица: $\begin{pmatrix} 0,0 \\ 0,0 \end{pmatrix}$. И для каждой матрицы $\begin{pmatrix} c,0 \\ 0,0 \end{pmatrix}$ есть противоположная матрица: $\begin{pmatrix} -c & 0 \\ 0 & 0 \end{pmatrix}$. Следовательно, (X,+) – подмоноид $(M_2(R),+)$.

ЛЕММА 2.1.1. На полугруппе (A,*) выполнен обобщенный ассоциативный закон, т.е. в произведение могут входить не только три элемента, но и произвольное конечное число элементов, другими словами, для любого фиксированного натурального числа n и любого k ($k \le n$) справедливо равенство:

$$(x_1*x_2*\ldots..*x_k)*(x_{k+1}*\ldots.*x_n) = x_1*x_2*\ldots..*x_k*x_{k+1}*\ldots.*x_n$$

Доказательство. Методом математической индукции по k числу элементов в первой скобке произведения ($k \le n$).

При k=1, тогда

$$x_1*(x_2*\ldots..*x_k*x_{k+1}*_{\ldots.}*x_n) = x_1*x_2*\ldots..*x_k*x_{k+1}*_{\ldots.}*x_n.$$

Можно обозначить через A элемент $x_3*x_4*\ldots..*x_k*x_{k+1}*_{\ldots.}*x_n$. Тогда левая часть будет записана в виде $x_1*(x_2*A) = x_1*x_2*A$, по закону ассоциативности для полугруппы. После этого расписывание A завершает доказательство.

Рассмотрим ещё переход от k=1 до k=2.

$(x_1*x_2)(x_3*\ldots..*x_k*x_{k+1}*_{\ldots.}*x_n)$. Вновь обозначим через $A=x_3*\ldots..*x_k*x_{k+1}*_{\ldots.}*x_n$. Тогда по ассоциативному закону для полугруппы получаем, что

$$(x_1*x_2)*A = x_1*x_2*A=x_1*x_2*x_3*\ldots..*x_k*x_{k+1}*_{\ldots.}*x_n.$$

Это завершает доказательство для k=2.

Допускаем, что для всех $k<m<n$ выполнено. Докажем, что выполнено и для m+1.

Рассмотрим произведение $(x_1x_2\ldots..x_m*x_{m+1})*(x_{m+2}*_{\ldots.}*x_n)$.

Заменяем произведение $x_1*x_2*\ldots..*x_m=A$, $x_{m+2}*_{\ldots.}*x_n =B$. После этого получаем, что рассматриваемое произведение равно (по свойствам операции на полугруппе и предположению индукции)

$$(A*x_{m+1}) *B = A*x_{m+1}*B = x_1*x_2*\ldots..*x_m*x_{m+1}*x_{m+2}*_{\ldots.}*x_n$$

А это завершает доказательство.

ОПР. Моноид (A,*), в котором все элементы обратимы, называется **группой.** Или, другими словами, если на A задана операция *, такая, что

1) она ассоциативна;

2) в A есть e — единица группы относительно этой операции, т.е. такой элемент e, что для любого x из A, x*e = e*x = x;

3) для любого элемента x в A найдется обратный к нему элемент x^{-1}, т.е. такой, что $x^{-1}*x = x*x^{-1} = e$.

ПРИМЕРЫ .а) целые числа по сложению (Z,+);

б) {0;+} или {e,*};

в) (2N,+) не является группой по сложению, так как у любого натурального числа противоположный элемент не лежит в N; кроме того, там нет и нулевого элемента.

Аналогично понятию порядка полугруппы рассматривается понятие порядка группы G.

ОПР. Если группа G конечна и имеет n элементов, то говорят, что G ***имеет порядок*** n.

Аналогично понятию подполугруппы рассматривается понятие подгруппы группы G.

ОПР. Пусть (G,*)-группа, H —подмножество в G. H называется **подгруппой**

группы G, если H замкнута относительно операции *, т.е. для любой пары элементов a и b из H a*b также лежит в H, и (H,*) —является группой относительно той же самой операции *.

ПРИМЕРЫ. 1) G и {e} — **тривиальные подгруппы** в группе G (или несобственные подгруппы в группе G).

2) $(R_+,*)$ положительные числа по умножению. Подгруппы в R_+:

{1};

положительные рациональные числа.

3) группа многочленов по сложению $R_n[x] = \{a_o+a_1x+a_2x^2+..+a_nx^n: a_i \text{ из } R\}$.

Подгруппы в группе многочленов:

многочлены с целыми коэффициентами;

многочлены с рациональными коэффициентами;

многочлены степени не большие n, с вещественными коэффициентами.

ЛЕММА 2.1.2 Все подгруппы в (Z,+) имеют вид dZ, где d некоторое натуральное число.

Доказательство. Рассмотрим наименьший по модулю элемент, который лежит в H, подгруппе Z, и отличный от нуля. Пусть это будет число d (будем полагать, без ограничения общности, что это положительное число, если d<0, тогда вместо d возьмем - d). Тогда любое другое целое число a, лежащее в H можно разделить на d с остатком. Получим, что

$$a = qd+r, \quad 0 \le r < d.$$

(q·d можно трактовать, как сложение d раз числа q). Отсюда видим, что если $a \in H$, $d \in H$, то $r \in H$. Но в силу выбора числа d число r должно лежать в H (иначе модуль r меньше модуля d). Следовательно, d|a.

§2.2 **КОЛЬЦО**

ОПР. **Кольцом** называется множество A с заданными на нем двумя бинарными операциями + (сложение) и *(умножение), удовлетворяющие следующим условиям:

а) (A,+) —коммутативная группа;

б) (A,*) —полугруппа;

в) операции сложения и умножения связаны дистрибутивными законами:

$$(a+b)*c = a*c + b*c;\ c*(a+b) = c*a + c*b.$$

для всех a,b,c из A.

ПРИМЕРЫ: а) (Z,+,*); б) (R[x],+,*) -множество многочленов от одной переменной, с двумя обычными операциями: «+»-сложением и «*» умножением. Это множество, также образует структуру кольца.

УПР. Доказать, что на кольце выполняется и общий закон дистрибутивности: для любых натуральных m, n, если a_i i=1,2,…,n и b_j j=1,2,…,m лежат в кольце A, то справедливо равенство

$$(a_1+a_2+....+a_n)*(b_1+b_2+...+b_m) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i * b_j$$

ОПР. Кольцо называется **коммутативным**, если x*y = y*x, для всех x,y из A.

ОПР. Сумма двух элементов кольца A a и (- b) называется их **разностью**, и обозначается через **a - b**.

ОПР. Если в кольце A есть 1_A (или e_A) – единичный элемент относительно операции умножения, то такое кольцо называют **кольцом с единицей.**

ОПР. Элемент a кольца A с единицей называется **обратимым в кольце A,** если для него в кольце A существует обратный элемент a^{-1}, т.е. такой элемент, что

$$a^{-1}*a=a*a^{-1}=1_A.$$

ОПР. Пусть A —коммутативное кольцо с единицей. Если для любого a из A, $a \neq 0$, в A найдется обратный элемент, тогда данная структура называется **полем**.

В дальнейшем поле будем обозначить через **K**.

Другими словами поле K — это структура, которая

- относительно операции “+”является абелевой группой (эта абелева группа (K,+) называется **аддитивной группой поля K)**;

- относительно операции умножения (без ноля, т.е. $K^*=K\backslash\{0\}$) будет коммутативной группой (эта группа (K^*,*) называется - **мультипликативной группой поля K**).

Z_m-КОЛЬЦО КЛАССОВ ВЫЧЕТОВ ПО МОДУЛЮ m

Рассмотрим пример одного из числовых колец, которое играет большую роль в теории чисел и ее многочисленных приложениях, в частности, в криптографии.

ОПР. Пусть m —произвольное натуральное число. Говорим, что **a сравнимо с b по модулю m**, если a - b делится на m. В противном случае говорят, что два целых числа не сравнимы между собой по модулю m

(Это записывается таким образом $a \equiv b(\mathrm{mod} m)$).

ПРИМЕР. Пусть m=2. Тогда любые два чётных числа сравнимы между собой по модулю 2, также как и любые два нечётные числа.

ОПР. Пусть m некоторое фиксированное натуральное число. Множество всех целых чисел сравнимых между собой по модулю m называется **классом вычетов по модулю m.** Произвольное целое число, которое лежит в этом классе называется **вычетом по модулю m.**

Из рассмотрения определения сравнимости по модулю m сразу возникает несколько вопросов:

- есть ли какие-то явные признаки того, что два числа сравнимы между собой по модулю m;
- как много элементов сравнимых между собой;
- как много наборов сравнимых между собой чисел?

Рассмотрим пример.

ПРИМЕР. Пусть m=3. Возьмем число 0, с чем сравнимо это число по модулю 3? Понятно, что с 3, 6, 9, -3, …, т.е. в одном с 0 классе вычетов, лежат все целые числа, делящиеся на 3. Этот класс обозначим через $\bar{0}$.

Если возьмем 1, тогда получаем, что в одном с 1 классе вычетов лежат числа 4, 7, -2, -5,…, т.е. в этом классе лежат все целые числа, имеющие при делении на 3 остаток равный 1. Обозначим этот класс вычетов через $\bar{1}$.

Если рассмотрим число 2, то получаем, что оно сравнимо с 5, -1, 8, -4, …, т.е. все оставшиеся целые числа образуют класс вычетов (обозначим его через $\bar{2}$), в котором все целые числа при делении на 3 дают в остатке 2.

Итак, получили, что у нас всего 3 класса. Причем каждый класс определяется, по сути, остатком при делении на 3. И эти классы попарно не пересекаются.

Из рассмотрения примера несложно получить ответ на все поставленные вопросы.

Ответ на первый: два целых числа сравнимы между собой по модулю натурального числа m тогда и только тогда, когда имеют одинаковый остаток при делении на m.

УПР. Пусть a, b – целые числа, m –натуральное. Доказать, что $a \equiv b(\mathrm{mod} m)$ $\Leftrightarrow$ остатки при делении на m чисел a и b равны.

Отсюда понятен ответ и на второй вопрос: понятно, что в каждом классе вычетов по модулю m содержится бесконечное множество вычетов (т.е. целых чисел, имеющих одинаковые остатки при делении на m).

Опять же из рассматриваемого примера понятен ответ и на третий вопрос: число классов вычетов по модулю m равно количеству остатков при делении на m, их ровно m штук.

Чтобы получить структуру кольца, на множестве классов вычетов (при некотором фиксированном натуральном числе m) нужно ввести две операции: сложение и умножение с требуемыми свойствами.

Итак, рассмотрим множество всех классов вычетов по модулю m. Их, как замечено выше, ровно m штук. Будем обозначать их через $\{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$. На этом множестве классов вычетов можно с помощью таблиц ввести две операции: «+» сложения и «×» умножения.

ПРИМЕРЫ. Кольцо классов вычетов по модулю 3. Зададим операции умножения и сложения на Z_3 с помощью таблиц.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Аналогично рассмотренному примеру, определим операции «+» и «×» для набора классов вычетов по модулю m (m>2).

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	. .	$\overline{m-1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	. .	. .	$\overline{m-1}$
$\bar{1}$	$\bar{1}$				$\bar{0}$
… …	… …	…	. .	. .	…..
$\overline{m-1}$	$\overline{m-1}$	$\bar{0}$			$\overline{m-2}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	. .	$\overline{m-1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	. .	. .	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$			$\overline{m-1}$
….	..	…	. .	. .	… …
$\overline{m-1}$	$\bar{0}$	$\overline{m-1}$			$\bar{1}$

УПР. Доказать, что полученная структура является кольцом, которое и называется **кольцом классов вычетов по модулю m (**обозначается через $\mathbf{Z_m}$**).**

ЗАМЕЧАНИЕ. Заметим, что все требуемые свойства для операций «+» и «×» будут выполняться, так как это фактически получаются таблицы для операций над множеством остатков при делении целых чисел на натуральное число m; сумма остатков равна остатку от суммы остатков, остаток произведения равен остатку от произведения остатков. А на множестве целых чисел операции «+» и «×» и ассоциативны и коммутативны, а также выполнен и дистрибутивный закон.

ОПР. Взяв от каждого класса вычетов по одному представителю (вычету), получим систему вычетов, которая называется ***полной системой вычетов по модулю m.***

Понятно, что полная система вычетов определяется неоднозначно, так как в каждом классе вычетов можно выбрать произвольный вычет, который можно отправить в полную систему вычетов.

ОПР. Пусть есть полная система вычетов, выбираем из них вычеты, которые взаимно просты с m, отсюда получаем систему вычетов, которая называется ***приведенной системой вычетов по модулю m.***

Несложно заметить, что приведенная система вычетов вновь определяется неоднозначно, но количество элементов в ней не зависит от выбора вычетов из полной системы вычетов, потому, что если какой-то один элемент a взаимно прост с модулем m, то, как несложно видеть, и все остальные вычеты из этого класса также взаимно просты с m.

Верно и обратное: если какой-то вычет не взаимно прост с модулем m, то и любой вычет из данного класса будет не взаимно прост с модулем.

ПРИМЕР. Рассмотрим все классы вычетов по модулю 6. Это будут $\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$. Сейчас в качестве полной системы вычетов по модулю 6 можно взять произвольный набор из 6 чисел, лежащих в попарно различных классах вычетов, например, (6, 13, 20, 3, 28, 5). В качестве приведенной системы вычетов можно взять такой набор вычетов (1, 5) или (7, 17). Во всех других классах вычетов по модулю 6 лежат числа, не взаимно простые с 6.

ОПР. Количество натуральных чисел, не превосходящих m и взаимно простых с m, (m-натуральное) равно значению **функции Эйлера φ(m)**, которая определяется на всем множестве натуральных чисел, и значения которой лежат также в этом множестве.

Положим по определению, что φ(1)=1.

ЗАМЕЧАНИЕ. Как несложно понять, значение функции Эйлера **φ(m)** равно числу элементов в приведенной системе вычетов по модулю m. Число классов равно m, в качестве полной системы вычетов можно взять числа от 1 до m. Если произвольный вычет взаимно прост с модулем, тогда в его классе вычетов есть элемент, лежащий в данной полной системе вычетов {1,2,3…,m}, и, как несложно заметить, он также будет взаимно прост с m.

ПРИМЕР: Если рассмотреть функцию Эйлера φ(6), тогда несложно подсчитать, что она равна 2. И верно, число элементов в приведенной системе вычетов по модулю 6 равно 2, как было показано выше.

Несложно вычислить прямым подсчетом, значения функции Эйлера для ряда натуральных чисел: φ(1)=1, φ(2)=1, φ(3)=2, φ(4)=2, φ(5)=4, и т.д..

А сейчас рассмотрим вопрос о нахождении формулу для вычисления функции Эйлера.

Сначала подумаем о том, как вычислить функцию Эйлера для некоторых частных случаев, например, когда речь идет о простых числах, т.е. найти φ(p). Несложно понять, что все натуральные числа, меньшие простого числа p, взаимно просты с ним. Поэтому φ(p)=p-1. Также несложно подсчитать, что $\varphi(p^2)=p(p-1)$. Это связано с тем, что всего чисел от 1 до p^2 равно p^2 и из них ровно p делится на p: это p,2p,3p,…pp=p^2. Только эти числа и не взаимно просты с p^2. Поэтому всего чисел взаимно простых с p^2 равно p^2-p.

Аналогично находится $\varphi(p^k)$ для произвольной степени простого числа p:

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(k-1).$$

УПР. Доказать, что $\varphi(p_1p_2)=(p_1-1)(p_2-1)$; $\varphi(p_1^2p_2^2)=p_1p_2(p_1-1)(p_2-1)$.

Оказывается справедлива следующая лемма.

ЛЕММА 2.2.1. Функция Эйлера φ(n) мультипликативна, т.е. если (a,b)=1, то φ(ab) = φ(a)φ(b), где a и b —натуральные числа.

Доказательство. Пусть M —множество чисел не меньших ab. Каждое число n из M может быть единственным образом представлено в виде

$$n = bq+r, \text{ где } q = \{0, 1, 2, \ldots, a\}, r = \{0, 1, 2, .., b-1\}.$$

Когда (n,b)=1? Понятно, что это тогда, когда (b,r)=1.

Сколько существует таких r? Ровно φ(b). Рассмотрим какое-то одно $r=r_1$. Тогда числа r_1, r_1+b, r_1+2b,...,$r_1+(a-1)b$ образуют полную систему вычетов по mod a.

Это можно показать, так как если какие-то два элемента сравнимы между собой по модулю a**,** т.е. если $r_1+kb \equiv r_1+tb(moda)$, получаем, что $(k-t)b\equiv 0(moda)$. Однако, (k - t) не могут делиться на a, кроме случая когда k=t, и (a,b)=1. Значит, приходим к противоречию, которое показывает, что числа r_1, r_1+b, r_1+2b,...,$r_1+(a-1)b$ образуют полную систему вычетов по модулю a.

Значит, среди них ровно φ(a) чисел, которые взаимно просты с a.

Отсюда получаем, что каждому числу r_1 соответствует ровно φ(a) чисел, взаимно простых с a чисел. Ещё раз напомним, что среди остатков при делении на b ровно φ(b) взаимно простых с b. Отсюда получаем, что общее число вычетов, взаимно простых с a·b равно φ(a)·φ(b).

И понятно, что других чисел, взаимно простых с ab нет. Значит, утверждение леммы верно.

Отсюда следует следующий результат.

ЛЕММА 2.2.2. Значение функции Эйлера для $n = \prod_{p_i|n} p_i^{a_i}$ вычисляется по формуле $\varphi(n)=\prod_{p_i|n}\varphi(p_i) = \prod_{p_i|n} p_i^{a_i}(p_i-1)$, где p_i — различные простые делители n.

Доказательство. Мы уже научились вычислять $\varphi(p^k)=p^{k-1}(p-1)$. Так как произвольное натуральное n можно разложить в произведение степеней простых, то получаем, что

$$\varphi(p_1^{a_1}\cdot p_2^{a_2}\cdot\ldots\cdot p_s^{a_s}) = \varphi(p_1^{a_1})\cdot\varphi(p_2^{a_2})\cdot\ldots\cdot\varphi(p_s^{a_s}) = \prod_{p_i|n} p_i^{a_i}(p_i-1)$$

УПР. Найти а) φ(10); б) φ(100); с) φ(720).

ЗАМЕЧАНИЕ. Функция Эйлера будет использоваться в дальнейшем не только в алгебре, но и в дискретной математике, теории чисел, криптографии и других курсах.

КОЛЬЦО МНОГОЧЛЕНОВ С ВЕЩЕСТВЕННЫМИ КОЭФФИЦИЕНТАМИ

Построим новое кольцо А, элементами которого являются бесконечные упорядоченные (т.е. перенумерованные) последовательности

$$a = (a_0,a_1,a_2,a_3,\ldots,\ldots)$$

такие, что все a_i - вещественные числа, причем в каждой такой последовательности все, кроме конечного числа a_i, равны 0.

Определим на А аксиому равенства:

I. $(a_o,a_1,a_2,\ldots..) = (b_o,b_1,b_2,\ldots.) \overset{\Delta}{=} a_i=b_i$, для всех i=0,1,2,...

Определим на множестве В операции сложения и умножения, полагая

II. $a+b = (a_o,a_1,a_2,\ldots..) + (b_o,b_1,b_2,\ldots.) \overset{\Delta}{=} (a_o+b_o,a_1+b_1,a_2+b_2,\ldots..)$

III $a\ b = (a_o,a_1,a_2,\ldots..)\ (b_o,b_1,b_2,\ldots.) \overset{\Delta}{=} (\sum_{i+j=0} a_ib_j\ ,\ \sum_{i+j=1} a_ib_j\ ,\ \sum_{i+j=2} a_ib_j\ ,\ldots\ldots,)$

В качестве $\mathbf{0_A}$ можно взять элемент (0,0,...0,..). По определению операции сложения для любой последовательности $a = (a_0,a_1,a_2,a_3,\ldots..,\ldots)$ из А, получаем, что

$$(a_0,a_1,a_2,a_3,\ldots..,\ldots) + (0,0,\ldots,0,\ldots.) = (0,0,\ldots,0,\ldots.) + (a_0,a_1,a_2,a_3,\ldots..,\ldots) = (a_0,a_1,a_2,a_3,\ldots..,\ldots).$$

Несложно заметить, что для любого элемента $a = (a_0,a_1,a_2,a_3,\ldots..,\ldots)$ из А есть противоположный элемент $-a =(-a_0, -a_1,-a_2,-a_3,\ldots..,\ldots)$, который также лежит в А и такой, что

$$a + (-a) = (a_0,a_1,a_2,a_3,\ldots..,\ldots) + (-a_0, -a_1,-a_2,-a_3,\ldots..,\ldots) = (0,0,\ldots,0\ldots) = 0_A.$$

Заметим также, что в силу того, что для вещественных чисел сумма не зависит от порядка слагаемых, операция сложения на множестве А, также не зависит от порядка слагаемых, т.е. для любых двух элементов из А $a=(a_0,a_1,a_2,a_3,\ldots..,\ldots)$ и $b=(b_o,b_1,b_2,\ldots.)$ выполняется

$a+b = (a_0,a_1,a_2,a_3,\ldots..,\ldots)+(b_o,b_1,b_2,\ldots.) = (a_o+b_o,a_1+b_1,a_2+b_2,\ldots..)=(b_o+a_o, b_1+a_1, b_2+a_2,\ldots..)$

и

$$(b_o,b_1,b_2,\ldots.) + (a_0,a_1,a_2,a_3,\ldots..,\ldots) = b + a.$$

Следовательно, относительно операции «+» структура (А,+) - является абелевой группой.

Можно проверить, что относительно операции умножения структура (А,) является полугруппой.

УПР. Доказать, что (А,) – полугруппа.

Также несложно проверить, что для операций “ ” и “+” выполняется дистрибутивный закон, т.е.

$$a\times(b+c) = a\times c + b\times c, \quad \text{для любых элементов a, b, c из A,}$$

что говорит, о том, что данная структура (A, +, ×) определяет кольцо, которое и называется **кольцом многочленов над кольцом A.**

Несложно проверить, что умножение “ ”коммутативно: т.е. для любых двух элементов a и b из A выполняется a b=b a. Это следует из того, что операции сложения и умножения на множестве вещественных чисел коммутативны, поэтому получаем, что данное кольцо будет и **коммутативным кольцом.**

Заметим, что последовательности вида (a,0,0,...) складываются и умножаются так же, как элементы кольца A. Таким образом это подмножество можно отождествить с элементами из A. Таким образом можно считать, что A становится подкольцом кольца многочленов над A.

Причем умножение на элементы из кольца A на произвольный элемент кольца многочленов можно трактовать, как

$$a(x,y,....)$$

т.е. просто a раз взят элемент (x,y,..).

Обозначим (0,1,0,....) через X и назовем X **переменной** (или **неизвестной**) над A. Используя введенную на B операцию умножения, находим, что

$$X^2 = (0,0,1,0,....); \ ....., \ X^n=(0,0,...0,1,0...) \ (1 \text{ на } (n+1)\text{-месте}).$$

Как уже упоминалось ранее $aX=(0,a,0,...)$.

Итак, если a_n - последний ненулевой член последовательности $(a_o,a_1,a_2,...,a_n,0,0,...)$, то в новых обозначениях это можно переписать и так.

$$a = a_o+a_1X+a_2X^2+a_3X^3+...+a_nX^n.$$

ОПР. Введенное выше кольцо B обозначается через A[X] и называется **кольцом многочленов над A от одной переменной, а его элементы — многочленами.**

ЗАМЕЧАНИЕ. Отметим, что X — рассматривается как многочлен f=X, а не как переменная, которая пробегает какое-то множество значений, но это только на время, далее это будет не столь существенно, как рассматривать данный многочлен.

Ещё раз отметим, что произвольный элемент кольца многочленов над кольцом A можно записать так:

$$p(X) = a_o+a_1X+a_2X^2+a_3X^3+...+a_nX^n.$$

ОПР. Элементы $a_i \in A$, $i= 0,1,2,...,n$ —называются **коэффициентами многочлена**, **a_o - постоянный член, a_n - старший коэффициент, n —степень многочлена**.

Нулевой многочлен —это многочлен, у которого все коэффициенты нулевые. Степень нулевого многочлена будем считать равной $-\infty$.

Многочлены степени 1,2,3,.... называются соответственно **линейными, квадратичными (или квадратными), кубичными**, и т.д.

КОЛЬЦО МАТРИЦ

Рассмотрим множество квадратных матриц порядка n, т.е.

$M_n(R) = \{L=\begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ..... & .. & ... & ... \\ a_{n1} & a_{n2} & ... & a_{nn} \end{pmatrix}$, где все $a_{i,j}$ - являются вещественными числами$\}$, и

покажем, что если на этом множестве определить две операции «+» - сложение и «*» умножение, то данная структура будет кольцом.

Мы уже показали выше, что множество квадратных матриц порядка 2 образует абелеву группу по сложению. Определим на множестве $M_n(R)$ (аналогично случаю $M_2(R)$, операцию «+» (сложение):

$$\begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ..... & .. & ... & ... \\ a_{n1} & a_{n2} & ... & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & ... & b_{1n} \\ b_{21} & b_{22} & ... & b_{2n} \\ ..... & .. & ... & ... \\ b_{n1} & b_{n2} & ... & b_{nn} \end{pmatrix} \stackrel{\Delta}{=} \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & ... & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & ... & a_{2n}+b_{2n} \\ ..... & .. & ... & ... \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & ... & a_{nn}+b_{nn} \end{pmatrix}.$$

Совершенно аналогично разобранному выше случаю для $M_2(R)$, проверяется, что и $(M_n(R),+)$ также является абелевой группой. Нулевым элементом в $M_2(R)$, будем считать матрицу, составленная из нулей.

На множестве $M_n(R)$ определим операцию «*» (умножение):

$$\begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ..... & .. & ... & ... \\ a_{n1} & a_{n2} & ... & a_{nn} \end{pmatrix} * \begin{pmatrix} b_{11} & b_{12} & ... & b_{1n} \\ b_{21} & b_{22} & ... & b_{2n} \\ ..... & .. & ... & ... \\ b_{n1} & b_{n2} & ... & b_{nn} \end{pmatrix} \stackrel{\Delta}{=}$$

$$\begin{pmatrix} a_{11}b_{11}+a_{12}b_{21}+...+a_{1n}b_{n1} & a_{11}b_{12}+a_{12}b_{22}+...+a_{1n}b_{n2} & ... & a_{11}b_{1n}+a_{12}b_{2n}+..+a_{1n}b_{nn} \\ a_{21}b_{11}+a_{22}b_{21}+...+a_{2n}b_{n1} & a_{21}b_{12}+a_{22}b_{22}+...+a_{2n}b_{n2} & ... & a_{21}b_{1n}+a_{22}b_{2n}+...+a_{2n}b_{nn} \\ .. & & & .. \\ a_{n1}b_{11}+a_{n2}b_{21}+...+a_{nn}b_{n1} & a_{n1}b_{12}+a_{n2}b_{n2}+...+a_{nn}b_{n2} & ... & a_{n1}b_{1n}+a_{n2}b_{2n}+...+a_{nn}b_{nn} \end{pmatrix}$$

Можно проверить, что умножение является ассоциативной операцией. Это предлагается в качестве упражнения.

УПР. Доказать, что $(M_n(R),*)$ – полугруппа.

Из определения операций несложно показать, что выполняется и дистрибутивный закон: для любых трех матриц $A=(a_{i,j})$, $B=(b_{i,j})$, $C=(c_{i,j})$ из $M_n(R)$ выполняется соотношение

$$(A+B)C = AC+BC.$$

Это соотношение следует из равенств

$$\left(\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots\dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \dots\dots & \dots & \dots & \dots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix}\right)\begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \dots\dots & \dots & \dots & \dots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{pmatrix} =$$

$$\begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \dots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \dots & a_{2n}+b_{2n} \\ \dots\dots & \dots & \dots & \dots \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & \dots & a_{nn}+b_{nn} \end{pmatrix}\begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \dots\dots & \dots & \dots & \dots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{pmatrix} =$$

$$\begin{pmatrix} (a_{11}+b_{11})c_{11}+..+(a_{1n}+b_{1n})c_{n1} & .. & .. & (a_{11}+b_{11})c_{1n}+..+(a_{1n}+b_{1n})c_{nn} \\ (a_{21}+b_{21})c_{11}+..+(a_{2n}+b_{2n})c_{n1} & .. & .. & (a_{21}+b_{21})c_{1n}+..+(a_{1n}+b_{1n})c_{nn} \\ \dots & .. & .. & \dots. \\ (a_{n1}+b_{n1})c_{11}+..+(a_{nn}+b_{nn})c_{n1} & .. & .. & (a_{n1}+b_{n1})c_{1n}+..+(a_{nn}+b_{nn})c_{nn} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11}c_{11}+..+a_{1n}c_{n1} & .. & .. & a_{11}c_{1n}+..+a_{1n}c_{nn} \\ a_{21}c_{11}+..+a_{2n}c_{n1} & .. & .. & a_{21}c_{1n}+\dots+a_{2n}c_{nn} \\ \dots & .. & .. & \dots. \\ a_{n1}c_{11}+..+a_{nn}c_{n1} & .. & .. & a_{n1}c_{1n}+..+a_{nn}c_{nn} \end{pmatrix} + \begin{pmatrix} b_{11}c_{11}+..+b_{1n}c_{n1} & .. & .. & b_{11}c_{1n}+..+b_{1n}c_{nn} \\ b_{21}c_{11}+..+b_{2n}c_{n1} & .. & .. & b_{21}c_{1n}+..+b_{1n}c_{nn} \\ \dots & .. & .. & \dots. \\ b_{n1}c_{11}+..+b_{nn}c_{n1} & .. & .. & b_{n1}c_{1n}+..+b_{nn}c_{nn} \end{pmatrix}$$

§ 2.3. ПОЛЕ. ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ

Ещё раз напомним, что поле K это коммутативное кольцо с единицей, в котором любой элемент a из K, $a \neq 0$, обратим.

Другими словами поле - это структура, которая относительно операции "+" является абелевой группой; относительно операции "*"(без ноля) также является коммутативной группой.

ЗАМЕЧАНИЕ. Полученная структура (K,+) будет абелевой группой относительно операции сложения, и она называется **аддитивной группой поля**, а структура без нулевого элемента (она обозначается через K*), (K^*,*) будет коммутативной группой по умножению. Это так называемая **мультипликативная группа поля**.

ОПР. Пусть A и B – множества. Множество всех пар (a,b), где a из A, и b из B, называется **прямым произведением множеств A и B** (Обозначается A×B).

Замечание. Если A=B, то говорят, что это степень множества A, т.е. A^2.

ПРИМЕР: $R \times R = R^2$ – это множество пар точек (x,y), x и y из R.

ЗАМЕЧАНИЕ. По аналогии с упорядоченными парами (x,y), $x \in X$; $y \in Y$, можно рассмотреть упорядоченные n-ки, т.е. рассмотреть n множеств X_1, X_2,….., X_n и рассмотреть наборы из n элементов $(x_1,x_2,\ldots,x_n)$, где $x_i \in X_i$, i=1,2,..,n. Множество всех таких наборов называется **прямым произведением множеств X_1,…..X_n** и обозначается через $X_1 \times X_2 \times \ldots \times X_n$ или $\prod_{i=1}^{n} X_i$.

Для получения поля комплексных чисел рассмотрим прямое произведение $R \times R = \{(x,y), x,y \text{ из } R\}$.

Образуем на нем алгебраическую структуру, с помощью введения на нём двух операций "+"и "·" (сложения и умножения) по следующим правилам (или аксиомам):

1) сложение: $(a,b) + (c,d) \stackrel{\Delta}{=} (a+c, b+d)$;

2) умножение: $(a,b)\cdot(c,d) \stackrel{\Delta}{=} (a\cdot c - b\cdot d, a\cdot d + b\cdot c)$.

3) $(x,y) = (a,b) \stackrel{\Delta}{=} (x=a)$ и $(y=b)$.

4) Будем полагать, что $(a,0) \stackrel{\Delta}{=} a$, где a - вещественное число, и будет использоваться соответствующая запись.

В дальнейшем знак операции умножения «·» мы будем часто просто опускать, поскольку операции умножения – это обычная операция умножения на вещественных числах.

Проверим, что 4) аксиома не противоречит здравому смыслу, т.е. операции на множестве вещественных чисел можно рассматривать и на подмножестве R×R, которое соответствует множеству вещественных чисел, и они ничем не отличаются

$$(a,0) + (b,0) = (a+b,0) = a+b$$
$$(a,0)(b,0) = (ab,0) = ab$$

Умножение произвольного числа из R×R на произвольное вещественное также вполне понятно:

$$(a,0)(x,y) = (ax,ay) = a(x,y).$$

Если m натуральное число, то получим, что m(x,y) = (mx,my) — это сумма m элементов (a,b), т.е. имеет вполне понятный смысл.

Поэтому нет никаких противоречий со здравым смыслом и с обычными операциями на множестве вещественных чисел. Следовательно, можно считать, что в множестве R×R, с заданными операциями, есть подмножество, совпадающее с множеством всех вещественных чисел.

Сейчас проверим, что введенные операции определяют хорошую структуру на этом множестве.

Проверяем, что обе операции удовлетворяют свойствам ассоциативности и коммутативности, в качестве нулевого элемента (обозначим через **0**) на этом множестве можно взять пару (0,0), а в качестве единицы (обозначим через **1**) можно взять пару (1,0).

Если ассоциативность по сложению почти очевидна, так как сложение в поле вещественных чисел ассоциативно, а вот по умножению эту ассоциативность нужно проверить.

$$((a,b)\cdot(c,d))\cdot(e,f) = (ac - bd, ad + bc)\cdot(e,f) = (ace-bde-adf-bcf, acf-bdf+ade+bce)$$
$$(a,b)\cdot((c,d)\cdot(e,f)) = (a,b)\cdot(ce - df,cf + de) = (ace-adf-bcf-bde,acf+ade+bce-bdf).$$

Как видим, правые части равенств одинаковы. Следовательно, операция умножения также ассоциативна.

Для любого элемента (a,b) из R×R есть противоположный (-a,-b), который также лежит в R×R.

Покажем, что для любого, не равного (0,0), элемента (a,b) из R×R есть обратный элемент, и он также лежит в R×R:

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}; \frac{-b}{a^2+b^2}\right).$$

Докажем, что две введенные операции удовлетворяют и дистрибутивному закону.

$$(a,b)\cdot((c,d)+(e,f)) = (a,b)(c+e,d+f) = (a(c+e)-b(d+f),a(d+f)+b(c+e)) =$$
$$(ac-bd,ad+bc) + (ae-bf,af+be)) = (a,b)(c,d) + (a,b)(e,f).$$

Что и требовалось доказать.

Заметим, что несложно проверить, что операция умножения коммутативна. Следовательно, данная структура является полем, которое называется **полем комплексных чисел** и обозначается как **C**.

Понятно, что алгебраические преобразования в C над парами (x,y) не очень удобны, особенно, когда речь идёт об операции умножения. Поэтому обычно рассматривают две интерпретации таких пар, или две формы записи таких чисел, которые более удобны для выполнения преобразований с ними: а именно, алгебраическая и тригонометрическая форма записи комплексных чисел.

Для первого вида записи введём число *i* (она носит название **"мнимой единицы")**, которая будет иметь вид *i*=(0,1) и обладает свойством, что $i^2 = -1$ (по аксиоме умножения).

Тогда, как несложно проверить, в соответствии с аксиомами, произвольное комплексное число z=(x,y) можно записать так:

$$(x,y) = (x,0) + (0,y) = (x,0) + (0,1)\cdot(y,0) = x + iy.$$

x —называется вещественной частью числа z (обозначается через **Rez), y — мнимая часть числа z (**обозначается через **Imz).**

ОПР. Пусть z = x + *i*y, то число, которое имеет вид x - *i*y, называется **комплексно сопряжённым для z** числом и обозначается $\bar{z}$.

Из аксиомы 3, при рассмотрении z C в алгебраической форме записи, получаем, что из равенства двух комплексных чисел следует, что

$$z_1=a_1+ib_1 = z_2=a_2+ib_2 \overset{\Delta}{=} (a_1=a_2)\&(b_1=b_2),$$

т.е. два комплексных чисел равны тогда и только тогда, когда равны их вещественные и мнимые части.

Также несложно сосчитать, что $z\cdot\bar{z}$, если z = x + *i*y, является вещественным неотрицательным числом и это произведение равно x^2+y^2. Корень квадратный из этого числа называется **модулем комплексного числа z** и обычно обозначается через |z|.

ЛЕММА 2.3.1. Произведение $z\cdot\bar{z}$ и сумма $z+\bar{z}$ двух комплексно сопряжённых чисел являются вещественными числами.

Доказательство. Пусть z = x + *i*y, тогда $\bar{z}$ =x - *i*y и то, что произведение $z\,\bar{z}$ = $x^2 + y^2$ - является вещественным числом, уже показано выше. А то, что сумма $z+\bar{z}$ является вещественным числом, то это также понятно, и следует из записи этой суммы.

ЗАМЕЧАНИЕ. Несложно заметить, что мы рассматривали представление элементов поля комплексных чисел, как множество точек плоскости R^2. Для них легко понять интерпретацию для сопряжённого числа: это число симметричное z относительно оси абсцисс. Понятно, что модулем будет расстояние от точки (x,y) до начала координат точки (0,0).

Эта запись нередко более удобна, когда нужно выполнять сложение комплексных чисел. Для операции умножения комплексных чисел чаще удобнее использовать другую форму записи комплексных чисел, так называемую **тригонометрическую форму записи**.

Эта запись возникает от записи точек плоскости в полярных координатах: положение каждой точки z плоскости однозначно определяется модулем числа (**модуль комплексного числа** обозначается, как обычно, через |z|) и углом φ между радиус-вектором точки плоскости, которая соответствует точке $z \in C$ и положительным направлением вещественной оси oX. Угол φ - называется **аргументом z** и обозначается argz.

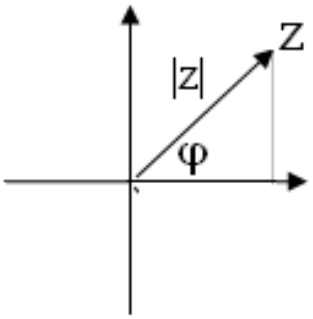
По определению argz может принимать любые значения от $(-\infty,\infty)$, но при заданном модуле $|z|$ углы, отличающиеся на $2\pi k$, k - целое, определяют одно и то же комплексное число (как точку комплексной плоскости).

Также по определению несложно понять, что аргумент нельзя определить для комплексного числа (0,0) (так как модуль этого числа равен 0), поэтому для z=0 нет тригонометрической формы записи.

Поэтому (как несложно выяснить из рисунка), любое комплексное число z (кроме z=**0**) также может быть записано в виде

$$z = |z|(\cos\varphi + i\sin\varphi).$$

Это так называемая **тригонометрическая форма комплексного числа**. Заметим, что в этой форме стоит знак + и аргумент у синуса и косинуса одинаков.



ЗАМЕЧАНИЕ. Во-первых, отметим, что в силу замечания выше (про аргумент для комплексного числа (0,0)), тригонометрическая форма комплексного числа определяется не для всех комплексных чисел. Она определена для всех комплексных чисел, кроме нуля.

Во-вторых, понятно, что аргумент комплексного числа определен не однозначно, а с точностью до $2k\pi$, так как значения синуса и косинуса имеют период 2π.

ПРИМЕРЫ: Найти тригонометрическую форму записи для чисел z C:

а) – 1; б) cos(-x) – *i*·sin(-x).

Решение. а) Заметим, что модуль |-1| = 1, а аргумент равен π, поэтому число – 1 можно записать таким образом (- 1) = cosπ + *i*·sinπ;

б) Здесь видим, что модуль числа равен 1, а аргумент, в силу чётности функции cosx и нечётности функции sinx, равен просто x. Отсюда тригонометрическая форма записи этого числа равна cos(-x) - *i*sin(-x) = cosx+ *i*sinx.

Рассмотрим один несложный, но достаточно важный результат о тригонометрической форме записи чисел.

ЛЕММА 2.3.2. Модуль произведения комплексных чисел z, z’ равен произведению модулей чисел z и z', а аргумент произведения комплексных чисел z, z’ равен сумме их аргументов.

Доказательство. Пусть z=|z|(cosφ+*i*sinφ), z'=|z'|(cosω+*i*sinω).

Тогда z·z' = |z|(cosφ + *i*sinφ)·|z’|(cosω+*i*sinω) = |z|·|z'|·(cosφ+*i*sinφ)·(cosω+*i*sinω) = |zz’|·(cosφ ·cosω - sinφ·sinω + *i*(sinφ·cosω + cosφ·sinω)) = |zz’| (cos(φ+ω)+*i*sin(φ+ω)).

Рассмотрим решение некоторых задач, в том чисел и с использованием данной леммы.

ПРИМЕР: Найти геометрическое место точек на комплексной плоскости z(x,y) таких, что а) |z|=3; б) arg(*i*z) = π/4.

Решение. а) По определению |z|=|x+*i*y| = $\sqrt{x^2+y^2}$ =3. Отсюда получаем, что x^2+y^2 = 9. На плоскости XoY это уравнение является уравнением окружности. Следовательно, искомое ГМТ есть окружность радиуса 3, с центром в начале координат (см.рис.1)

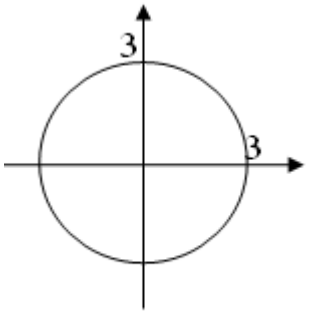


рис.1

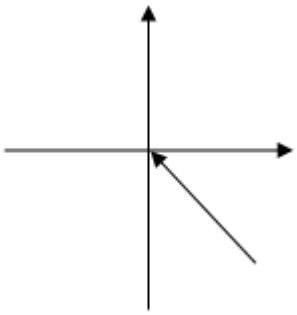


рис.2

б) По лемме 2.3.2. аргумент произведения двух комплексных чисел равен сумме аргументов этих чисел. Поэтому arg(*i*z) = arg*i* + argz = $\frac{\pi}{4}$. Отсюда получаем, что argz = π/4 - arg*i* = $\frac{\pi}{4}$ - $\frac{\pi}{2}$ = - $\frac{\pi}{4}$. Следовательно, искомым ГМТ будет луч без конца, исходящий из точки (0,0) и являющийся биссектрисой четвертого координатного угла (см.рис.2).

в) Рассмотрим один пример использования комплексных чисел для решения некоторых задач тригонометрии.

Найти сумму $\operatorname{artg}\frac{1}{3} + \operatorname{arctg}\frac{1}{4} = \arg(z_1 \cdot z_2) = \arg((3+i)\cdot(4+i)) = \operatorname{arctg}\frac{7}{11}$.

ЗАМЕЧАНИЕ. Нужно отметить, что комплексные числа, в отличие от вещественных, не упорядочены: это очень важное свойство. Именно оно позволяет доказать основную теорему алгебры, о существовании корней у произвольного многочлена ненулевой степени.

Покажем, что операции, которые мы ввели на множестве комплексных чисел, записанных в тригонометрической или алгебраической формах, хорошо согласуются с теми, которые мы давали при определении.

Рассмотрим операцию сложения для чисел в алгебраической форме записи.

$$a+bi + c+di = a + c + (b + d)i.$$

То есть, видим, что все хорошо согласуется: просто складываются вещественные и мнимые части двух комплексных чисел.

Аналогично можно проделать с произведением чисел, которые записаны в алгебраической форме записи.

$$(a+bi)\cdot(c+di) = ac - bd + i(ad + bc).$$

Что также согласуется с введенным выше определенным, и становится понятным, почему в первом числе произведения пар ставится знак «-».

Рассмотрим ещё один вопрос: если число задано в алгебраической форме записи, каким образом можно перевести его в тригонометрическую форму?

Есть вполне определенный метод решения этой задачи.

$z = x + iy = \sqrt{x^2+y^2}\left(\frac{x}{\sqrt{x^2+y^2}} + \frac{y}{\sqrt{x^2+y^2}}\cdot i\right) = |z|(\cos\alpha + i\sin\alpha)$, где α - аргумент комплексного числа $z = x+iy$.

$z=(a+bi)=\sqrt{a^2+b^2}\ \frac{a+bi}{\sqrt{a^2+b^2}} = |z|\ \left(\frac{a}{\sqrt{a^2+b^2}} + \frac{b}{\sqrt{a^2+b^2}}i\right) = |z|(\cos\alpha + i\sin\alpha)$, где α - аргумент комплексного числа z.

Приведем формулу для определения $\alpha = \arg z$:

$$\alpha = \arg z = \begin{cases} arctg\left(\frac{x}{y}\right); a > 0 \\ \pi + arctg\left(\frac{x}{y}\right); a < 0 \\ \frac{\pi}{2}; (a = 0)\ \&\ (b > 0) \\ -\frac{\pi}{2}; (a = 0)\ \&\ (b < 0) \end{cases}$$

Ещё раз отметим, что в силу неопределённости аргумента для z=0, у него нет тригонометрической формы.

Докажем один важный результат.

ТЕОРЕМА 2.3.3. (Формула Муавра) Пусть $z=|z|(\cos\varphi+i\sin\varphi)$— комплексное число. Тогда $z^n=|z|^n(\cos n\varphi + i\sin n\varphi)$, где n произвольное натуральное число.

Доказательство. Проведем доказательство индукцией по n.

Проверяем, что для n=1 формула верна.

Пусть для всех натуральных не превышающих n формула выполняется. Тогда рассмотрим $z^{n+1} = z^n\cdot z$. По предположению индукции, получаем, что

$$z^{n+1}=|z|(\cos n\varphi+i\sin n\varphi)|z|(\cos\varphi+i\sin\varphi) =$$
$$|z|^{n+1}(\cos n\varphi\cdot\cos\varphi - \sin n\varphi\sin\varphi+i(\sin\varphi\cos n\varphi+\cos\varphi\cdot\sin n\varphi)) =$$
$$= |z|^{n+1}(\cos((n+1)\varphi) + i\sin((n+1)\varphi)))$$

Что и требовалось доказать.

УПР. Доказать, что формула Муавра справедлива и для всех целых чисел n, а не только натуральных.

Формула Муавра помогает в счете некоторых сумм с биномиальными коэффициентами, с которыми мы уже сталкивались, когда изучали комбинаторные свойства множеств, а также в вычислении некоторых тригонометрических сумм.

Рассмотрим некоторые примеры.

ПРИМЕРЫ: 1) Найти формулу для подсчета сумм биномиальных коэффициентов

$$C_{2n}^0+C_{2n}^4...+C_{2n}^{4n}$$

2) Найти формулу для подсчета суммы $\sin x + \sin 2x + \sin 3x +...+ \sin nx$.

Решение. 1). Для начала запишем $(1 + i)^{2n}$ в двух формах

$$(1+ i)^{2n} = C_{2n}^0 + iC_{2n}^1 - C_{2n}^2 - iC_{2n}^3 + C_{2n}^4 +\ldots. \qquad (1)$$

С другой стороны, эта сумма по формуле Муавра может быть подсчитана и таким образом:

$$(1 + i)^{2n}=(\sqrt{2}\,(\cos\frac{\pi}{4}+ i\sin\frac{\pi}{4}))^{2n}=2^n(\cos\frac{n\pi}{2}+ i\sin\frac{n\pi}{2}) \qquad (2)$$

Заметим, что из (1) и (2) следует, что сумма

$$C_{2n}^0 - C_{2n}^2 + C_{2n}^4 -\ldots. (-1)^n C_{2n}^2 =\mathrm{Re}[(1 + i)^{2n}]= 2^n\cos\frac{n\pi}{2}. \quad (3)$$

Когда мы вычисляли сумму всех биномиальных коэффициентов (см. с.15) было показано, что

$$C_{2n}^0 + C_{2n}^2 + C_{2n}^4 +\ldots. + C_{2n}^2 =2^{2n-1} \qquad (4)$$

Прибавляя (3) и (4), получаем, что

$$2(C_{2n}^0+C_{2n}^4...+C_{2n}^{4n}) = 2^{2n+1}+2^n\cos\frac{n\pi}{2}.$$

Отсюда находим, что $C_{2n}^0+C_{2n}^4...+C_{2n}^{4n} = 2^{2n} + 2^{n-1}\cos\frac{n\pi}{2}$

2) *Указание*. Рассмотрите сумму

$\cos x+\cos 2x+\ldots+\cos nx + i(\sin x + \sin 2x + \sin 3x +\ldots+ \sin nx) = a+a^2+\ldots+a^n$,

где $a =\cos x + i\sin x$.

Получаем сумму членов геометрической прогрессии, мнимая часть которой и равна искомому выражению.

УПР. Найти формулу для подсчета сумм биномиальных коэффициентов

$$C_n^0+C_n^3+C_n^6\ldots+C_n^{3t}+\ldots$$

УКАЗАНИЕ. Для этого нужно рассмотреть формулы бинома Ньютона для чисел 1 и 1, 1 и ρ, 1 и ρ^2, где $1+\rho+\rho^2=0$.

ОПР. Число b называется **корнем степени n из комплексного числа z**, если $b^n=z$.

ТЕОРЕМА 2.3.4 (Формула извлечения степени) Пусть $\mathbf{z}=|\mathbf{z}|=(\cos\varphi+i\sin\varphi)$ - комплексное число, где |z|-модуль z, а φ - аргумент этого комплексного числа, Тогда множество всех корней n-ой степени из комплексного числа z можно вычислить по формуле

$$\{z^{1/n}\}=|\mathbf{z}|^{1/n}\left(\cos\left(\frac{\varphi+2\pi k}{n}\right)+i\sin\left(\frac{\varphi+2\pi k}{n}\right)\right),$$

где k пробегает множество от 0 до n-1.

Доказательство. Покажем, что любое число вида

$$|\mathbf{z}|^{1/n}\left(\cos\left(\frac{\varphi+2\pi k}{n}\right)+i\sin\left(\frac{\varphi+2\pi k}{n}\right)\right),$$

где k пробегает множество от 0 до n-1, является корнем n-ой степени из числа z. Это сразу следует из теоремы Муавра примененной к z.

Рассмотрим w: $w^n=z$. Тогда по определению

$$|w| = \sqrt[n]{|z|} \text{ и } n\cdot\arg w = \arg z + 2k\pi = \varphi + 2k\pi,$$

где k – произвольное целое число. Отсюда получаем, что $\arg w = \frac{\varphi+2\pi k}{n}$, для некоторого целого k.

На интервале от 0 до 2π есть только n различных значений argw, все остальные будут повторяться с точностью до $2k\pi$, а это означает, что есть только n различных комплексных чисел, которые могут быть корнями степени n из z.

Это и завершает доказательство теоремы.

ПРИМЕРЫ. Найти а) $\{\sqrt[3]{1}\}$; б) $\{\sqrt[3]{-i}\}$.

Решение. а) Запишем число 1 в тригонометрической форме (модуль 1 равен 1)

$$1 = \cos 0+i\sin 0 = \cos 2\pi k + i\sin 2\pi k.$$

Тогда по теореме 2.3.4 отсюда будет следовать, что все корни степени 3 из 1 будут находиться по формуле $\cos\frac{2\pi k}{3}+i\sin\frac{2\pi k}{3}$, k=0,1,2.

б) Запишем число i в тригонометрической форме (модуль i равен 1)

$$i = \cos(\frac{\pi}{2} + 2\pi k) + i\sin(\frac{\pi}{2} + 2\pi k)$$

Тогда по теореме 2.3.4 отсюда будет следовать, что все корни степени 3 из i будут находиться по формуле $\cos\frac{\pi + 4\pi k}{6} + i\sin\frac{\pi + 4\pi k}{6}$, k=0,1,2.

ОПР. Корнем n-ой степени из 1 называется комплексное число ε: $\varepsilon^n=1$.

Как несложно получить по формуле извлечения корней n степени из 1 элементы этого множества имеют вид

$$\{\sqrt[n]{1}\}=\{\varepsilon_k,\ k=0,1,..,n\} = \{\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, k=0,1,..,n-1\}.$$

Для множества корней степени n из 1 в поле комплексных чисел есть ряд интересных результатов, которые мы сформулируем и докажем.

ЛЕММА 2.3.5. Множество $\{\varepsilon_k,\ k=0,1,..,n\}$ образует множество из n элементов, геометрическая интерпретация которого - вершины правильного n-угольника, одна из вершин которого совпадает с точкой (1,0).

Доказательство следует непосредственно из определения корней степени n из 1. Во-первых, заметим, что модули всех корней степени n из 1 равны 1, то есть все эти числа лежат на единичной окружности, радиуса 1, с центром в начале координат. Во-вторых, в этом множестве всегда есть элемент $\varepsilon_o = 1$. Поэтому, одна из точек данного множества располагается в точке (1,0). И в-третьих, заметим, что угол между радиус-вектором $\overline{\varepsilon_k}$ и $\overline{\varepsilon_{k-1}}$, для любого k=1,2,…,n-1, равен $\frac{2\pi}{n}$. Следовательно, это правильный n- угольник, одна из вершин которого расположена в точке (1,0). А это и требовалось доказать.

ЛЕММА 2.3.6. Множество корней n-ой степени из 1 образует группу по умножению.

Доказательство. Чтобы показать, что данное множество является группой достаточно показать, что операция умножения ассоциативна, что есть единичный элемент и для любого ε_k, k=0,1,…,n-1 есть обратный элемент.

Заметим, что ассоциативность показывать не нужно, так как на всем множестве **C** операция умножения ассоциативна, значит и для рассматриваемого множества это также выполняется.

В качестве 1 можно взять ε_o**=1**, которой всегда лежит в множестве корней степени n из 1.

И для любого ε_k, k≠0, в качестве обратного к нему можно взять элемент ε_{n-k}. Для $\varepsilon_o = 1$ обратный элемент совпадает с ней самой, т.е. с ε_o. Несложно проверить, что при умножении аргумент полученного произведения будет кратен 2π.

УПР. Доказать, что подгруппы этой группы, не совпадающие с единичной и самой группой, будут существовать тогда и только тогда, когда n составное число.

ОПР. Комплексное число b — называется **первообразным корнем степени n из 1**, если $b^n=1$, и $b^m\neq 1$, для всех $0<m<n$.

Рассмотрим некоторые свойства первообразных корней.

ЛЕММА 2.3.7. Корень ε_k (k=0,1,…,n-1) степени n из 1 будет первообразным тогда и только тогда, когда, когда (k,n)=1.

Доказательство. Понятно, что для любого ε_k (k=0,1,…,n-1) выполняется свойство $\varepsilon_k^n=1$. Рассмотрим, когда выполняется свойство $\varepsilon_k^m=1$, m<n. Учитывая формулу Муавра, получаем, что тогда выполняется равенство

$$\varepsilon_k^m = \cos\frac{2\pi km}{n} + i\sin\frac{2\pi km}{n} = 1.$$

Отсюда получаем, что $\frac{2\pi km}{n} = 2\pi t$, где t - целое. Это будет только тогда, когда (k,n)>1, (иначе m не может разделиться нацело на n, так как меньше его).

Если же (k,n)=1, то $\frac{2\pi km}{n} = 2\pi t$, где t - целое, только тогда, когда m кратно n, т.е. наименьшее натуральное число, для которого это выполняется, равно n. Отсюда ε_k - является первообразным, что и требовалось доказать.

ЗАМЕЧАНИЕ. Отсюда несложно заметить, что число первообразных корней степени n из 1 равно .

Докажем еще одно несложное свойство первообразных корней.

ЛЕММА 2.3.8. Любой корень n-ой степени из 1 - ε_k (k=0,1,…,n-1) - является первообразным корнем какой-то степени d из 1, причем $d \mid n$.

Доказательство. Что нам нужно показать? Нужно показать, что для любого ε_k, где k натуральное от 1 до n-1 (k=0 не рассматриваем, для него условия леммы очевидно выполняется, так как $\varepsilon_o=1$) выполняется такое свойство, что если $(\varepsilon_k)^m=1$ и m наименьшее натуральное с таким условием, то m является делителем n.

Итак, если $\varepsilon_k{}^n=1$, и допустим, что он уже в некоторой меньшей степени m равен 1, т.е. $\varepsilon_k{}^m=1$, и допустим, что это наименьшая степень для рассматриваемого корня ε_k. Тогда разделим n на m. Получим n=mq+r, где $0\le r<m$. Поэтому получаем (при этом учитывая предполагаемые равенства), что

$$(\varepsilon_k)^n = \varepsilon_k{}^{mq+r}=(\varepsilon_k{}^m)^q\,\varepsilon_k{}^r=\varepsilon_k{}^r=1.$$

Получаем либо противоречие с выбором m либо r=0. Но в последнем случае это и означает, что n делится на m.

ОПР. **Круговым многочленом порядка n** (его также называют **многочлен деления круга**) называется приведенный многочлен наименьшей степени, корнями которого являются все первообразные корни степени n из 1. Он обозначается в разной литературе по-разному. Мы будем обозначать его так: $X_n(x)$.

Вопрос: как найти круговой многочлен данного порядка?

Помимо естественного способа найти все первообразные корни (все ε_k) степени n из 1 и перемножить скобки ($x-\varepsilon_k$), после чего перегруппировать скобки и перемножить их, иногда можно использовать и другой метод, который также позволяет находить этот круговой многочлен, основанный на свойствах, которые показаны в доказанных выше леммах.

ПРИМЕРЫ. Найти круговые многочлены а) $X_5(x)$; б) $X_{12}(x)$.

Ответ. а) $X_5(x) = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$,

Пояснение к решению. Во-первых, заметим, что все корни 5-ой степени из 1 являются корнями многочлена x^5-1. Во-вторых, только один корень, а именно 1, не является первообразным корнем степени 5 из 1. Поэтому и нужно x^5-1 разделить на многочлен x-1.

б) *Ответ*. $X_{12}(x)=\frac{(x^{12}-1)(x^2-1)}{(x^4-1)(x^6-1)}=\frac{(x^6-1)(x^6+1)(x^2-1)}{(x^6-1)(x^2-1)(x^2+1)}=\frac{(x^6+1)}{(x^2+1)}=\frac{(x^2+1)(x^4-x^2+1)}{(x^2+1)}=$

x^4-x^2+1.

Пояснения к решению этой задачи немного посложнее. Аналогично задаче выше, все корни степени 12 из 1 есть корни многочлена $x^{12}-1$. Заметим, что во-первых, любой корень степени 12 из 1 является первообразным корнем степени, которая является делителем 12, т.е. это числа 1, 2, 3, 4, 6 или 12; во-вторых, если число является корнем многочлена меньшей степени, например, многочлена x^6-1, то оно не будет первообразным корнем степени 12 из 1 (так как уже в 6-ой степени равно 1). Поэтому эти корни у многочлена $x^{12}-1$ нужно сократить. Это же нужно сказать и про корни многочлена x^4-1. Их также нужно сократить у многочлена $x^{12}-1$. Но отметим, что таким образом мы сократили дважды одни и те же корни, а именно корни многочлена x^2-1. Поэтому на этот многочлен нужно домножить числитель. Отсюда и получаем искомый результат. (Заметим, что по лемме 2.3.7 число корней у искомого многочлена (равно степени $X_{12}(x)$), т.е. число первообразных корней степени 12 из 1 ровно $4=\varphi(12)$).

ЗАМЕЧАНИЯ. Заметим, что в обоих случаях мы использовали несколько фактов, которые либо очевидны, либо были указаны или использованы в доказательстве лемм 2.3.7-2.3.8:

- что, если корень $(\varepsilon_k)^m=1$, то ε_k - является корнем многочлена порядка m - $f(x)=x^m-1$;
- что, если корень $(\varepsilon_k)^m=1$, то $((\varepsilon_k)^m)^t=1$, для любого натурального t;
- что, если корень $(\varepsilon_k)^m=1$, то m делитель n;
- что число корней кругового многочлена порядка n равно $\varphi(n)$.

СОДЕРЖАНИЕ

Учебное издание

Мерзляков Александр Сергеевич

Алгебра - 1

Учебно-методическое пособие

Авторская редакция

Издательство «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, 4Б, каб. 021
Тел. +7 (3412) 916-364 E-mail: editorial@udsu.ru