МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное научное учреждение
ИНСТИТУТ УПРАВЛЕНИЯ ОБРАЗОВАНИЕМ РОССИЙСКОЙ АКАДЕМИИ ОБРАЗОВАНИЯ

ОБЪЕДИНЕННЫЙ ФОНД ЭЛЕКТРОННЫХ РЕСУРСОВ "НАУКА И ОБРАЗОВАНИЕ"
(основан в 1991 году)

СВИДЕТЕЛЬСТВО О РЕГИСТРАЦИИ ЭЛЕКТРОННОГО РЕСУРСА

ИУО РАО
ОФЭРНиО

№ 20960

Настоящее свидетельство выдано на электронный ресурс, отвечающий требованиям новизны и приоритетности:

Электронный образовательный ресурс « Алгебра и теория чисел. Часть 1»

Дата регистрации: **08 июня 2015 года**

Автор: **Султанов С.Р.**

Организация-разработчик: **Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Рязанский государственный университет имени С.А. Есенина»**

Директор ФГБНУ ИУО РАО,
д.экон.н., профессор _____ С.С. Неустроев

Руководитель ОФЭРНиО, почетный
работник науки и техники России _____ А.И. Галкина

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ИМЕНИ С.А. ЕСЕНИНА»

СУЛТАНОВ С.Р.

АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

ЧАСТЬ 1

Электронное учебное пособие

Рязань 2015

Данный курс основан на лекциях, которые читались автором студентам факультета вычислительной техники РГРТУ в 2002 – 2005 г.г. Автор выражает свою признательность студентам ФВТ, взявших на себя труд по набору текста лекций, и благодарит доцента кафедры высшей математики РГРТУ Тарасова Вячеслава Владимировича и доцента кафедры математики и методики преподавания математических дисциплин РГУ имени С.А. Есенина Крючкова Николая Ивановича за ряд ценных замечаний и советов.

ГЛАВА 1

ВВЕДЕНИЕ В АЛГЕБРУ

§1. Элементы математической логики

Логика является наукой о законах, формах и приемах мышления. Владение приемами правильного мышления, знание логических законов совершенно необходимо в науке. Математическая логика изучает логику, используя при этом математические методы исследования: формализацию предмета, определение основных понятий, строгое доказательство результатов. Рассмотрим некоторые основные понятия математической логики.

Под *высказываниями* мы будем понимать такие повествовательные предложения, которым мы можем однозначно приписать логические значения: истина или ложь.

Например, фразы «где находится цирк?», «бесконечное множество точек», «исключительное явление» не являются высказываниями. Также не является высказыванием утверждение «идёт дождь», для того чтобы превратить эту фразу в высказывание необходимо, очевидно, уточнить, когда и где он идет. «Дважды два равно пяти », «в Сибири бывают морозы зимой, и жара летом» – примеры ложного и, соответственно, истинного высказываний. Высказывания можно подразделить на *простые* и *составные*. Последние два примера являются иллюстрацией. Из простых высказываний (а также и из составных) с помощью логических операций можно составлять новые, более сложные высказывания, логические значения которых будут определяться значениями входящих в них составных частей. Например, «солдат спит, а служба идет» – составное высказывание, которое будет истинным только в случае правдивости обеих его частей.

Договоримся обозначать простые высказывания буквами: A,B,C,D.… Простые высказывания называют *логическими переменными*. Составные высказывания называют *логическими функциями*. Каждое составное высказывание можно задать с помощью *формулы*, состоящей из букв, обозначающих некоторые простые высказывания (логические переменные), знаков логических операций и скобок, определяющих порядок выполнения операций. Приведем определения основных логических операций над высказываниями.

1. *Конъюнкцией* высказываний A и B (варианты обозначений: A&B, A/\B – читается “A и B”) называется новое высказывание, которое истинно тогда и только тогда, когда A и B являются истинными.

2. *Дизъюнкцией* высказываний A и B (обозначается: A\/B – читается “A или B”) называется новое высказывание, которое ложно тогда и только тогда, когда и A и B являются ложными.

3. *Отрицанием* A (варианты обозначений: $\bar{A}$, ¬A – читается “не A”) называется высказывание, которое истинно тогда и только тогда, когда исходное высказывание ложно.

4. *Импликацией* высказываний A и B (обозначается: A → B – читается «из A следует B», “если A, то B”) называется высказывание, которое ложно тогда и только тогда, когда A истинно, а B ложно.

При этом A будем называть посылкой, а B – следствием, заключением.

5. *Эквивалентностью (эквиваленцией)* высказываний A и B (варианты обозначений: A~B, A↔B – читается “A эквивалентно B”, “A тогда и только тогда, когда B”) называется высказывание, которое истинно тогда и только тогда, когда A и B имеют одинаковые логические значения.

Все вышесказанное мы можем отразить в так называемой «таблице истинности»

A	B	$A \wedge B$	$A \vee B$	$A \to B$	$A \sim B$	$\bar{A} \vee B$	$\bar{A}$
И	И	И	И	И	И	И	Л
И	Л	Л	И	Л	Л	Л	Л
Л	И	Л	И	И	Л	И	И
Л	Л	Л	Л	И	И	И	И

Данные логические операции формализуют те способы построения логических рассуждений, которыми мы пользуемся и в математических выкладках, и в повседневной жизни. В наших рассуждениях, например, на практике мы используем правило вывода «modus ponens»: $(A, A \to B) \Rightarrow B$, когда из истинности высказывания A и истинности импликации $A \to B$ мы делаем вывод об истинности утверждения B.

Заметим, что данные логические операции над высказываниями могут быть точно также определены и в том случае, когда высказывания являются составными.

Таким образом, каждое составное высказывание мы можем записать в виде формулы, и в дальнейшем мы будем абстрагироваться от повествовательного содержания высказывания, описываемого формулой. Для нас будет представлять интерес только логическое значение формулы. Две формулы P и Q будем называть *равносильными,* если они принимают одинаковые значения истинности при любых одинаковых наборах значений истинности логических переменных, входящих в данные формулы. Условие равносильности будем обозначать: $P \Leftrightarrow Q$. Таким образом, например, из приведённой таблицы истинности следует, что $(A \to B) \Leftrightarrow (\bar{A} \vee B)$. Очевидно, $P \Leftrightarrow Q$ тогда и только тогда, когда эквиваленция $P \sim Q$ является истинной. Заметим также, что если в произвольной формуле мы заменим любую из входящих в неё подформул на равносильную, то получим формулу, равносильную исходной. Пусть P – некоторая формула. Если при любых значениях входящих в неё логических переменных значение P является истинным, то формула P называется *тождественно истинной*, или *тавтологией.* Соответственно, если формула P принимает ложное значение при любых значениях входящих в нее логических переменных, то она называется *тождественно ложной*.

Рассмотрим теперь предложения, которые содержат переменные, определенные на некоторых множествах значений. Если при подстановке в такое предложение вместо переменных конкретных их значений мы будем получать всякий раз высказывание, то такое предложение мы будем называть *предикатом*. Например, предложение «$x > 2$», при x, определенном на множестве целых чисел, является предикатом. Если предложение содержит n переменных (которые могут пробегать различные множества), то говорят, что задан n-местный предикат. Например, предложение «$x + y = z$», где $x \in R$, $y \in Q$, $z \in N$ – трехместный предикат. Если на множестве X задан предикат $P(x)$, то выражение $(\forall x)\ P(x)$ означает высказывание «для всех x выполняется $P(x)$», а выражение $(\exists x)\ P(x)$ есть высказывание «существует x, для которого верно $P(x)$». Знак $\forall$ называется *квантором всеобщности*, а знак $\exists$ – *квантором существования*.

На множестве всех предикатов также определяются логические операции: конъюнкция, дизъюнкция, эквиваленция, отрицание, импликация – аналогичным образом, как и для высказываний. Например, дизъюнкцией предикатов $P(x)$ и $Q(x)$ будем называть предикат $P(x) \vee Q(x)$, который обращается в ложное высказывание для тех и только тех $x \in X$, для которых $P(x)$ и $Q(x)$ являются ложными. Таким образом, значение предиката $P(x) \vee Q(x)$ при конкретном значении переменной будет вычисляться, исходя из значений исходных предикатов для данного значения переменной. Так же, как и для высказываний, аналогичным образом определяются и понятия *формулы логики предикатов* и *равносильности* формул; в этом случае мы должны в уже приведённом выше определении формулы заменить приведенный термин “высказывания” на слово “предикаты”.

Приведем некоторые формулы алгебры высказываний:

1) $(\neg(\neg A)) \Leftrightarrow A$ – закон двойного отрицания;
2) $(A \vee A) \Leftrightarrow A$,
   $(A \wedge A) \Leftrightarrow A$ – законы идемпотентности;

3) $(A \vee B) \Leftrightarrow (B \vee A)$,
$(A \wedge B) \Leftrightarrow (B \wedge A)$ – законы коммутативности;

4) $((A \vee B) \vee C) \Leftrightarrow (A \vee (B \vee C))$,
$((A \wedge B) \wedge C) \Leftrightarrow (A \wedge (B \wedge C))$ – законы ассоциативности;

5) $\overline{(A \vee B)} \Leftrightarrow (\bar{A} \wedge \bar{B})$,

$\overline{(A \wedge B)} \Leftrightarrow (\bar{A} \vee \bar{B})$ – законы обращения (Де Моргана);

6) $((A \vee B) \wedge C) \Leftrightarrow ((A \wedge C) \vee (B \wedge C))$,
$((A \wedge B) \vee C) \Leftrightarrow ((A \vee C) \wedge (B \vee C))$ – законы дистрибутивности;

7) $((A \vee B) \wedge A) \Leftrightarrow A$,
$((A \wedge B) \vee A) \Leftrightarrow A$ – законы поглощения;

8) $(\overline{(\exists x)P(x)}) \Leftrightarrow ((\forall x)\,\bar{P}(x))$,

$\overline{(\forall x)P(x)} \Leftrightarrow ((\exists x)\bar{P}(x))$ – законы обращения кванторов.

Для доказательства формул (1 – 7) достаточно составить таблицы истинности левой и правой частей и убедится в их совпадении. Также можно доказывать равносильность показывая, что из истинности (ложности) правой части следует и истинность (ложность) левой и наоборот. На практике применение этих законов позволяет значительно упрощать, сокращать логические формулы.

§2. Элементы теории множеств

Множество обычно определяется как произвольная совокупность различимых между собой объектов, называемых его *элементами*, мыслимая как единое целое. Однако подобные определения чреваты неприятными последствиями типа парадокса Рассела, который мы приведем. Будем принадлежность элемента a множеству A обозначать: $a \in A$.

Пусть R – множество, элементами которого являются все множества, не являющиеся своими элементами, то есть $R = \{A \mid A \notin A\}$. Очевидно R не пусто, назовем его множеством Рассела. Тогда, если $R \in R$, то $R \notin R$, поскольку все составляющие R элементы удовлетворяют этому условию, и, следовательно, данное предположение неверно. Но, если $R \notin R$, то $R \in R$, следовательно, и это предположение неверно.

Чтобы избежать данного противоречия, мы договоримся иметь дело только с теми множествами, которые сами являются элементами некоторых *классов,* которые и будут являться произвольными совокупностями объектов. Таким образом, определим *множество* как класс, который является элементом некоторого класса. Тогда парадокс Рассела превращается в утверждение, что определенный выше класс Рассела R не является множеством.

Рассмотрим теперь некоторые основные понятия теории множеств.

Будем говорить, что множество A является *подмножеством* множества B (или *включается* в множество B), и обозначать $A \subset B$, если каждый элемент множества A является элементом множества B.

Множества A и B называют *равными*, если они состоят из одних и тех же элементов, то есть если одновременно $A \subset B$ и $B \subset A$. Договоримся обозначать $A = \{x \mid P(x)\}$ – множество всех таких элементов x, для которых предикат $P(x)$ представляет собой истинное высказывание.

Договоримся также считать в дальнейшем, что все рассматриваемые нами множества будут являться подмножествами некоторого множества U, которое мы будем называть *универсальным множеством*.

Объединением множеств A и B называется множество $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$, то есть множество $A \cup B$ состоит из всех тех элементов, которые принадлежат хотя бы одному из этих множеств.

Пересечением множеств A и B называется множество $A \cap B = \{\, x \mid (x \in A) \wedge (x \in B) \,\}$, то есть множество $A \cap B$ состоит из всех тех элементов, которые принадлежат каждому из этих множеств.

Разностью множеств A и B называется множество $A \setminus B = \{\, x \mid (x \in A) \wedge (x \notin B) \,\}$, то есть множество $A \setminus B$ состоит из всех тех элементов множества A, которые не являются элементами множества B. Разность $A \setminus A$ очевидно не содержит ни одного элемента, договоримся считать ее так называемым *пустым множеством* и обозначать $\varnothing$. Очевидно, для любого множества A $\varnothing \subset A$.

Дополнением множества A будем называть множество $\overline{A} = U \setminus A$, состоящее из всех тех элементов универсального множества, которые не являются элементами множества A.

Приведем некоторые формулы алгебры множеств.

1) $\overline{\overline{A}} = A$ – закон двойного дополнения;
2) $\begin{matrix}(A \cup A) = A,\\ (A \cap A) = A\end{matrix}$ – законы идемпотентности;
3) $\begin{matrix}A \cup B = B \cup A,\\ A \cap B = B \cap A\end{matrix}$ – законы коммутативности;
4) $\begin{matrix}A \cup (B \cup C) = (A \cup B) \cup C,\\ A \cap (B \cap C) = (A \cap B) \cap C\end{matrix}$ – законы ассоциативности;
5) $\begin{matrix}\overline{A \cup B} = \overline{A} \cap \overline{B},\\ \overline{A \cap B} = \overline{A} \cup \overline{B}\end{matrix}$ – законы обращения (Де Моргана);
6) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
   $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
7) $\begin{matrix}(A \cup B) \cap C = (A \cap C) \cup (B \cap C),\\ (A \cap B) \cup C = (A \cup C) \cap (B \cup C)\end{matrix}$ – законы дистрибутивности;
8) $\begin{matrix}(A \cup B) \cap A = A,\\ (A \cap B) \cup A = A\end{matrix}$ – законы поглощения.

Доказательство данных формул не представляет трудностей, и основано на непосредственном определении данных операций. На практике данные законы позволяют значительно упрощать формулы алгебры множеств.

§3. Декартово произведение множеств и отношения в множествах.

Определение. Пусть X, Y – непустые множества. *Декартовым произведением* множеств X и Y называется множество $X \times Y$ всех упорядоченных пар (x, y), таких, что $x \in X, y \in Y$, то есть $X \times Y = \{(x, y) \mid x \in X,\ y \in Y\}$. Упорядоченные пары (x, y) и (x', y') полагают *равными* тогда и только тогда, когда $x = x'$ и $y = y'$.

Аналогично определяется и декартово произведение любого конечного числа непустых множеств.

Определение. Пусть $X_1, X_2, \ldots, X_n$ – некоторые непустые множества. *Декартовым произведением* множеств $X_1, X_2, \ldots, X_n$ называется множество $X_1 \times X_2 \times X_3 \times \ldots \times X_n$ всех *упорядоченных n-ок* вида $(x_1, x_2, \ldots, x_n)$, составленных так, что для всех $k = 1,2,\ldots,n$ элементы $x_k \in X_k$, то есть $X_1 \times X_2 \times X_3 \times \ldots \times X_n = \{(x_1, x_2, \ldots, x_n) \mid x_k \in X_k,\ k = 1,2,\ldots,n\}$. При этом полагаем, что две упорядоченные *n-ки* $(x_1, x_2, \ldots, x_n) = (x_1', x_2', \ldots, x_n')$ тогда и только тогда, когда $x_k = x_k'$ для всех $k = 1,2,\ldots,n$.

Если в произведении $X_1 \times X_2 \times X_3 \times \ldots \times X_n$ для всех $k = 1,2,\ldots,n$ множества $X_k = X$, то говорят о n-ой *декартовой степени множества* X.

Пример 1. $R \times R \times R = \{ (x, y, z) \,|\, x, y, z \in R \}$ – вещественный декартов куб. Элементами его являются всевозможные упорядоченные тройки действительных чисел. Тройки (1,2,3) и (3,2,1), например, не равны.

В дальнейшем мы будем полагать, что под R понимается множество действительных, Q означает множество рациональных, Z – целых и N – натуральных чисел, если не будет сделано особых оговорок.

Определение. Пусть $X_1 \times X_2 \times X_3 \times \ldots \times X_n$ – декартово произведение множеств $X_1, X_2, \ldots, X_n$. Любое непустое подмножество данного произведения мы будем называть *n-арным отношением между элементами множеств* $X_1, X_2, \ldots, X_n$. В случае $n = 1$ говорят об *унарном* отношении, при $n = 2$ – о *бинарном* отношении, и так далее….

Пример 2. Пусть $X=\{1,2,\ldots,10\}$, $Y=\{А,Б,В,Г\}$. Тогда $S=\{(1,А),(1,Б),(2,Б)\}$ – бинарное отношение между элементами множеств X и Y, а множество $\{(2,Г),(В,4)\}$ – не является таковым.

Заметим, что упорядоченную тройку элементов (x_1, x_2, x_3) можно рассматривать также как упорядоченную пару $((x_1, x_2), x_3)$, упорядоченную четверку (x_1, x_2, x_3, x_n) как упорядоченную пару $((x_1, x_2, x_3), x_n)$ и так далее… . В силу этого мы видим, что бинарные отношения занимают особое место, мы изучим некоторые из них.

Пусть X и Y – непустые множества. Будем обозначать ρ – бинарное отношение между элементами множеств X и Y, тогда $\rho \subset X \times Y$ – некоторое множество упорядоченных пар из $X \times Y$. Очевидно, можно задать ρ следующим образом: $\rho=\{(x,y) |\ x \in X,\ y \in Y,\ P(x,y)\}$, где $P(x,y)$ – некоторый предикат, определенный на множестве $X \times Y$.

Пример 3. Определим $\rho_1 = \{ (x, y) \,|\, x, y \in N,\ 2x = y \}$ – множество всех упорядоченных пар натуральных чисел вида $(n, 2n)$.

Если $\rho \subset X \times Y$ и $X = Y$, то бинарное отношение ρ будем называть *бинарным отношением в (на) множестве* X. Так, например, определяется *тождественное* бинарное отношение Δ_X на множестве X: $\Delta_X = \{ (x, x) \,|\, x \in X \}$.

Пусть ρ – бинарное отношение между элементами множеств X и Y, x – произвольный элемент множества X. Будем говорить, что $\rho(x)$ – *проекция* элемента x, если $\rho(x)$ определяется следующим образом: $\rho(x)=\{y \in Y \,|\, (x,y) \in \rho\}$.

Так, например, для определенного в примере 3 отношения ρ_1, проекция $\rho_1(n)=\{2n\}$ для каждого натурального числа n.

Пусть A – подмножество X. *Проекцией* $\rho(A)$ *множества* A будем называть множество $\rho(A) = \bigcup_{x \in A} \rho(x)$.

Например, для определенного в примере 2 отношения S, проекция $S(\{1,2\}) = \{А, Б\}$, а проекция $S(\{3,4,5\}) = \varnothing$.

Определение. Пусть ρ – бинарное отношение между элементами множеств X и Y. Будем называть ρ *однозначным* бинарным отношением, если для произвольного элемента x из множества X, проекция $\rho(x)$ содержит не более одного элемента.

Например, рассматривая определенные в примере 2 множества X и Y, заметим, что $\{(1,А),(2,А),(3,Б)\}$ – является однозначным, а $\{(1,А),(1,Б),(3,В)\}$ – не является однозначным бинарными отношениями между элементами данных множеств.

Заметим, что условие однозначности бинарного отношения ρ можно представить следующим образом: для любых элементов x, y, z, если $(x, y) \in \rho$ и $(x, z) \in \rho$, то $y = z$.

Определение. Пусть ρ – бинарное отношение между элементами множеств X и Y. Тогда, если выполняются следующие два условия:

1) $\rho(x) \neq \varnothing$ для каждого $x \in X$;

2) ρ – однозначное бинарное отношение,

то бинарное отношение ρ будем называть *отображением* множества X в множество Y, или *функцией,* отображающей множество X в множество Y. Будем говорить также, что отображение ρ является отображением *«на»* Y, если проекция $\rho(X) = Y$.

Определение. Пусть ρ – бинарное отношение между элементами множеств X и Y. Будем называть бинарное отношение ρ^{-1} *обратным* бинарным отношением для ρ, если ρ^{-1} определяется следующим образом: $\rho^{-1} = \{(y,x) | (x,y) \in \rho\}$. Очевидно, ρ^{-1} является при этом бинарным отношением между элементами множеств Y и X. Если отношения ρ и ρ^{-1} одновременно являются однозначными, то бинарное отношение ρ называется *взаимно однозначным*. Если бинарное отношение ρ является отображением множества X в множество Y, и при этом ρ^{-1} является однозначным бинарным отношением, то отображение ρ называют *инъективным* или *инъекцией*. При этом, если инъекция ρ является отображением «*на*», то данное отображение называется взаимно однозначным.

Пример 4. $\{(x, y) \mid y = x^3, x \in R\}$ – это взаимнооднозначное отображение R на R.

Определение. Пусть $\rho_1 \subset X \times Y$, $\rho_2 \subset Y \times Z$ – бинарные отношения между элементами множеств X и Y, и Y и Z, соответственно. *Произведением* $\rho_2 \circ \rho_1$ данных бинарных отношений называется бинарное отношение между элементами множеств X и Z, которое определяется следующим образом: $\rho_2 \circ \rho_1 \subset X \times Y$, $\rho_2 \circ \rho_1 = \{(x,z) | (\exists y \in Y): ((x,y) \in \rho_1 \wedge (y,z) \in \rho_2)\}$.

Если отношения являются функциями, то их произведение называется *суперпозицией,* или *композицией*. Заметим, что для любых бинарных отношений проекция их произведения $(\rho_2 \circ \rho_1)(A) = \rho_2(\rho_1(A))$, тогда нетрудно проверить, что *суперпозиция двух функций также является функцией*, то есть если f_1 отображает множество X в множество Y, а f_2 отображает множество Y в множество Z, то произведение $f_2 \circ f_1$ является отображением множества X в множество Z.

Теперь мы можем привести определения таких важнейших понятий, как индексированное семейство элементов, и индексированное семейство множеств. Пусть $x_1, x_2, ..., x_n, \ldots$ – это бесконечная последовательность, состоящая из элементов некоторого множества X. Тогда мы можем данной последовательности поставить в соответствие отображение $f : N \to X$ такое, что при данном отображении каждый элемент $n \in N$ имеет проекцию $f(n) = x_n$. Таким образом, мы можем определить последовательность как некоторое *индексированное множество* $\{x_n\}_{n \in N}$, где N *– множество индексов*. Аналогично определяется произвольное *индексированное множество* или *индексированное семейство элементов.*

Определение. Если для множества I и множества X определено отображение множества I на множество X, то говорят, что задано *индексированное семейство* элементов (или – *индексированное множество*) X : при этом данный факт обозначается следующим образом: $X = \{x_i\}_{i \in I}$. Множество I при этом называется *множеством индексов.*

Пусть A – некоторое семейство множеств, I – некоторое множество. Тогда, если определено отображение f множества I на множество A, то говорят, что задано *индексированное семейство множеств* $A = \{X_i\}_{i \in I}$, где $X_i = f(i)$. Очевидно, любое семейство множеств можно сделать индексированным, например $A = \{X_X\}_{X \in A}$, то есть за множество индексов можно взять само множество A, а отображение – тождественное: $f(X) = X$.

Исключительная роль среди всех бинарных отношений принадлежит отношениям эквивалентности и отношениям порядка.

Определение. Пусть ε – бинарное отношение на множестве X, будем говорить, что ε – *отношение эквивалентности*, если выполнены следующие условия:

1. $\Delta_X \subset \varepsilon$ – условие *рефлективности*
$((\forall x \in X): (x,x) \in \varepsilon)$;

2. $\varepsilon = \varepsilon^{-1}$ – условие *симметричности*
$((\forall x,y \in X): ((x,y) \in \varepsilon \leftrightarrow (y,x) \in \varepsilon))$;

3. $\varepsilon \circ \varepsilon \subset \varepsilon$ – условие *транзитивности*
$((\forall x,y,z \in X): ((x,y) \in \varepsilon \wedge (y,z) \in \varepsilon) \to (x,z) \in \varepsilon))$.

Рассмотрим некоторые примеры отношений эквивалентности.

Пример 1. Обычное отношение равенства на множестве действительных чисел.

Пример 2. Отношение подобия на множестве всех треугольников.

Пример 3. Можно определить отношение эквивалентности ε_7 на множестве натуральных чисел N следующим образом: $(x,y)\in\varepsilon_7$, если числа x и y дают одинаковые остатки при делении на число 7.

Договоримся, что принадлежность пары (x,y) отношению эквивалентности ε: $(x,y)\in\varepsilon$ будем обозначать также: $x\,\varepsilon\,y$ или $x\sim y$, и говорить в таком случае, что элементы x и y *эквивалентны*.

Теорема. *Каждое отношение эквивалентности ε на множестве X задает разбиение данного множества на попарно непересекающиеся подмножества эквивалентных между собой элементов (называемых* ***фактор-классами****). Обратно, каждое разбиение множества X на непересекающиеся между собой подмножества определяет отношение эквивалентности на данном множестве X.*

Доказательство. Пусть ε – отношение эквивалентности на множестве X, тогда для каждого $x\in X$ определим $\varepsilon(x)=\{y|y\in X,(x,y)\in\varepsilon\}$ – проекцию элемента x. Заметим, что в силу рефлексивности ε, для каждого $x\in X$ $x\in\varepsilon(x)$, и таким образом объединение указанных проекций дает все множество X.

Докажем, что данные проекции образуют попарно непересекающиеся подмножества, состоящие из эквивалентных между собой элементов. Действительно, если $y,z\in\varepsilon(x)$, то $(x,y)\in\varepsilon$ и $(x,z)\in\varepsilon$, следовательно $(y,z)\in\varepsilon$ (в силу симметричности и транзитивности ε), таким образом, все элементы, лежащие в одном таком классе, эквивалентны между собой. Докажем, что эти классы не пересекаются или совпадают. Пусть x и y – произвольные элементы множества X, и $\varepsilon(x)\cap\varepsilon(y)\neq\varnothing$, тогда найдется элемент $z\in X$ такой, что $(x,z)\in\varepsilon$ и $(y,z)\in\varepsilon$, а тогда $(x,y)\in\varepsilon$, следовательно $y\in\varepsilon(x)$, и $\varepsilon(y)\subset\varepsilon(x)$ в силу транзитивности ε. Аналогично, $\varepsilon(x)\subset\varepsilon(y)$, следовательно, $\varepsilon(x)=\varepsilon(y)$, и первое утверждение теоремы доказано.

Обратно, пусть задано некоторое разбиение множества X на непересекающиеся подмножества, то есть $X=\bigcup_{\alpha\in A}X_\alpha$, где $X_\alpha\cap X_\beta=\varnothing$ при $\alpha\neq\beta$, и A – некоторое множество индексов. Тогда определим отношение ε на множестве X, соответствующее данному разбиению, следующим образом: положим $(x,y)\in\varepsilon$ тогда и только тогда, когда найдется индекс $\alpha\in A$ такой, что $x\in X_\alpha$ и $y\in X_\alpha$. Покажем, что определенное таким образом отношение ε является отношением эквивалентности.

Действительно, для любого $x\in X$ найдется индекс $\alpha\in A$ такой, что X_α э x, следовательно, ε рефлексивно. Далее, если $(x,y\in X_\alpha)$ и $(y,z\in X_\beta)$ то, очевидно, $X_\alpha=X_\beta$, следовательно, $x,z\in X_\alpha$, и отношение ε транзитивно. Симметричность определенного нами отношения ε достаточно очевидна, таким образом, ε является отношением эквивалентности, а подмножества $X_\alpha,\alpha\in A$, являются фактор-классами для данного отношения ε. Теорема доказана.

Пусть ε – отношение эквивалентности на множестве X. Будем называть множество $X/_\varepsilon=\{\varepsilon(x),x\in X\}$ *фактор-множеством*, соответствующим данному отношению ε.

Пример 4. Например, если ε_4 – отношение эквивалентности на множестве целых чисел Z, связывающее между собой числа, дающие одинаковый остаток при делении на 4, то ε_4 задает разбиение Z на фактор-классы: $Z_1=\{4z|z\in Z\}$, $Z_2=\{4z+1|z\in Z\}$, $Z_3=\{4z+2|z\in Z\}$, $Z_4=\{4z+3|z\in Z\}$. При этом $Z/_{\varepsilon_4}=\{Z_1,Z_2,Z_3,Z_4\}$.

Для каждого непустого множества можно задать некоторую его количественную характеристику.

Определение. Если множество X состоит из конечного числа элементов, то *мощностью* множества X называется число составляющих его элементов.

Определение. Если между элементами множеств A и B можно установить взаимнооднозначное соответствие (т.е. существует взаимно однозначное отображение множества A на множество B), то говорят, что множества A и B *имеют одинаковую мощность*, или *равномощны*, и обозначают $m(A)=m(B)$.

Говорят, что *мощность множества* A *не превосходит мощности множества* B, если существует подмножество B' множества B такое, что между элементами множеств A и B' можно задать взаимно однозначное соответствие; другими словами, если множество A равномощно некоторому подмножеству B' множества B. Будем обозначать это следующим образом: $m(A)\le m(B)$. Если одновременно $m(A)\le m(B)$ и $m(B)\le m(A)$, то можно показать, что $m(A)=m(B)$.

Каждое множество A, равномощное множеству натуральных чисел N, называют *счетным*, обозначают в этом случае $m(A)=\chi_0$.

Теорема. *Объединение счетного семейства счетных множеств является счетным множеством*.

Доказательство. Пусть $A=\{X_\alpha\}_{\alpha\in N}$ – счетное семейство счетных множеств. Тогда, для каждого $\alpha\in N$, X_α можно представить в следующем виде: $X_\alpha=\{x_i^\alpha\}_{i\in N}$. Составим бесконечную таблицу

$$
\begin{aligned}
X_1&=\{x_1^1,x_2^1,x_3^1,\dots x_n^1,\dots\},\\
X_2&=\{x_1^2,x_2^2,x_3^2,\dots x_n^2,\dots\},\\
X_3&=\{x_1^3,x_2^3,x_3^3,\dots x_n^3,\dots\},\\
&\dots\dots\dots\dots\dots\dots\\
X_m&=\{x_1^m,x_2^m,x_3^m,\dots x_n^m,\dots\},\\
&\dots\dots\dots\dots\dots\dots\\
&\dots\dots\dots\dots\dots\dots
\end{aligned}
$$

состоящую из элементов множеств $X_1, X_2,\dots, X_m,\dots$.

Для простоты доказательства будем считать, что все множества X_α семейства A являются попарно непересекающимися.

Тогда объединение семейства A : $X=\bigcup_{\alpha\in N}X_\alpha$ можно представить в виде последовательности $\{x_1^1,x_2^1,x_1^2,x_1^3,x_2^2,x_3^1,x_4^1,\dots\dots\}$, т.е. мы составляем последовательность, пробегая элементы нашей таблицы по диагоналям, при этом сдвигаясь в конце каждой на один элемент вправо (или вниз). Установленное таким образом взаимнооднозначное соответствие между элементами $\bigcup_{\alpha\in N}X_\alpha$ и N доказывает справедливость нашего утверждения.

Будем говорить, что множество A имеет *мощность континуума*, и обозначать $m(A)=\chi_1$, если A равномощно множеству действительных чисел R. Легко увидеть, например, что интервал (0,1) и множество R равномощны, действительно, функция $y=tg(\pi x-\pi/2)$ является взаимнооднозначным отображением интервала (0,1) на R, и таким образом, $m((0,1))=m(R)$. Заметим, что если множество A является подмножеством X, то $m(A)\le m(X)$, следовательно $m(N)\le m(R)$, причём можно доказать, что $m(N)\ne m(R)$.

В завершении данного раздела рассмотрим ещё одно понятие – отношение порядка, играющее важную роль в теории множеств, и в математике в целом.

Определение. Пусть ρ – бинарное отношение в множестве X. Будем говорить что ρ – *отношение (частичного) порядка в множестве* X, если выполняются следующие три условия:

1. ρ – *рефлексивно*, т.е. $\Delta_X\subset\rho$;
2. ρ – *транзитивно*, т.е. $\rho^2\subset\rho$;
3. ρ – *антисимметрично*, т.е. $\rho\cap\rho^{-1}\subset\Delta_X$.

Если ρ – отношение порядка в X, то принято обозначать $x \le y$, если $(x,y)\in\rho$. *Упорядоченным множеством* (X,ρ) (или $(X, \le)$) будем называть множество X с определенным в нем отношением (частичного) порядка ρ.

Приведём некоторые примеры упорядоченных множеств.

Пример 1. Обычное отношение «меньше, или равно» на множестве всех действительных чисел определяет «естественный порядок», таким образом $(R, \le)$ – упорядоченное множество.

Пример 2. В множестве N натуральных чисел можно определить отношение ρ (частичного) порядка следующим образом: $(x,y)\in\rho <=> y|x$ (y является делителем числа x), и тогда (N, ρ) – упорядоченное множество.

Пример 3. Отношение включения множеств, заданное в множестве всех подмножеств произвольного непустого множества является (частичным) порядком.

Определение. Отношение (частичного) порядка ρ на множестве X называется *линейным порядком*, если для него выполняется дополнительное условие:

4. $\rho \cup \rho^{-1} = X \times X$.

Последнее означает, что для любых двух элементов $x,y\in X$ выполняется условие: $(x,y)\in\rho$ или $(y,x)\in\rho$ (любые два элемента сравнимы).

Если в множестве X задано отношение линейного порядка, то множество X называется *линейно упорядоченным*.

Пример 1 – пример линейно упорядоченного множества, примеры 2 и 3 – (частично) упорядоченного.

Определение. Пусть X упорядоченное множество, A – подмножество X. Элемент $a\in A$ называется *наименьшим (наибольшим)* в множестве A, если для каждого элемента $x\in A$ $a \le x$ ($a \ge x$, соответственно). Если каждое непустое подмножество A множества X обладает наименьшим элементом, то множество X называется *вполне упорядоченным*.

Заметим, что если a – наименьший элемент множества A, то он должен быть сравним с любым элементом данного множества A.

Нетрудно видеть, что $(R,\le)$ из примера 1 не является вполне упорядоченным, например интервал (0,1) не содержит наименьшего элемента, а множество натуральных чисел N с естественным порядком – вполне упорядоченно.

Существуют два равносильных утверждения в теории множеств: первое – теорема Цермело и второе – аксиома выбора, здесь мы приводим данные утверждения.

Теорема Цермело. *Всякое непустое множество X можно вполне упорядочить*.

Аксиома выбора. *Пусть $\{X_s\}_{s\in S}$ – произвольное семейство непустых множеств. Тогда найдётся функция f, отображающая множество S в $X=\bigcup_{s\in S} X_s$, такая, что $f(s)\in X_s$ для каждого $s\in S$.*

§4. Алгебраические структуры.

Определение. Пусть X – непустое множество, X^n – его n-я декартова степень. Отображение f множества X^n в множество X называется n - *арной операцией в множестве X.*

Например, при $n = 1$, $f(x) = x$ – тождественное отображение X в себя – *унарная* операция, при $n = 2$, $f((x,y)) = y$ – *бинарная* операция в множестве X, и т.д. ….

К бинарным операциям относятся операции: конъюнкция, дизъюнкция, импликация, заданные на множестве всех высказываний, а также операции пересечения, объединения, разности множеств в алгебре множеств.

Множество X с введёнными в нём операциями называется *алгеброй*, или *алгебраической структурой*. Особенное место среди алгебр занимают бинарные алгебраические структуры, т.е. структуры с бинарными операциями.

Пусть f – бинарная операция в множестве X, тогда $f \subset X^2 \times X$ – однозначное бинарное отношение между элементами множеств X^2 и X. Проекцию (или образ) $f(x,y)$ пары $(x,y)\in X^2$ будем называть *результатом операции*, и обозначать при помощи некоего знака операции: $f(x,y) = x\cdot y$ или $x\times y$, или $x+y$, или $x \bullet y$ и т.д.….. Иногда, для упрощения обозначения, знак операции опускается, и результат операции записывается в виде xy .

Самые распространённые способы обозначения знака бинарной операции – *мультипликативный* ($\cdot$, $\bullet$, $\times$, …) и *аддитивный* ($+$, $\oplus$, $+'$, …). Если на множестве X заданы две бинарные операции, то обычно для них применяют аддитивный и мультипликативный способы обозначения "+" и "$\cdot$", но не надо их путать с обычными операциями сложения и умножения в множестве R действительных чисел.

С учётом вышесказанного, будем обозначать (X , $\cdot$, $+$, $\times$, …) – бинарную алгебру с операциями $\cdot$, $+$, $\times$,… на множестве X.

Определение. Пусть (X, $\cdot$) и (X', $\times$) – две бинарные алгебры. Если существует взаимно однозначное отображение φ: $X \xrightarrow{на} X'$ такое, что для любых $x, y \in X$ $\varphi(x\cdot y) = \varphi(x)\times\varphi(y)$, то говорят что алгебры (X, $\cdot$) и (X' ,$\times$) – *изоморфны*, а отображение φ – *изоморфизм* (X, $\cdot$) *на* (X' , $\times$).

Заметим, что с алгебраической точки зрения изоморфные алгебраические структуры можно отождествлять, поскольку соответствие между элементами изоморфных алгебр сохраняется при выполнении операций над ними.

Пример 1. Рассмотрим две алгебры (R, $+$) и (R_+, $\cdot$) – действительных и действительных положительных чисел с операциями обычного сложения и умножения действительных чисел. Определим отображение φ: $R \xrightarrow{на} R_+$, полагая $\varphi(x) = 2^x$. Тогда $\varphi(x+y) = 2^{x+y} = 2^x \cdot 2^y = \varphi(x) \cdot \varphi(y)$. Взаимнооднозначность отображения φ очевидна, следовательно, данные алгебры изоморфны.

Определение. Пусть (X, $\cdot$) – бинарная алгебра. Операция "$\cdot$" называется *ассоциативной*, если для любых $x,y,z \in X$ выполняется равенство $(x\cdot y)\cdot z = x\cdot(y\cdot z)$.

Бинарная алгебра (X, $\cdot$) с ассоциативной операцией называется *полугруппой.*

Элемент $e \in X$ полугруппы называется *нейтральным*, если для всех $x \in X$, $e\cdot x = x\cdot e = x$. Если операция имеет мультипликативное обозначение, то нейтральный элемент называют *единичным,* и могут обозначать "*1*", в случае аддитивной операции – *нулевым*, и могут обозначать символом "*0*".

Заметим, что *если нейтральный элемент существует, то он единственен.*

Рассмотрим важный пример полугруппы функций на множестве X. Пусть X – произвольное непустое множество. Обозначим F_X – множество всех функций, отображающих данное множество X в X. Тогда (F_X , $\circ$) – полугруппа, где $\circ$ – операция произведения (композиции) функций. Действительно, если $\varphi_1, \varphi_2, \varphi_3 \in F_X$, то для любого элемента $x \in X$ ($(\varphi_3 \circ \varphi_2) \circ \varphi_1)(x) = (\varphi_3 \circ \varphi_2)\,(\varphi_1(x)) = \varphi_3(\varphi_2\,(\varphi_1(x)))$, и $(\varphi_3 \circ (\varphi_2 \circ \varphi_1))(x) = \varphi_3((\varphi_2 \circ \varphi_1)(x)) = \varphi_3(\varphi_2(\varphi_1(x)))$, следовательно $(\varphi_3 \circ \varphi_2) \circ \varphi_1 = \varphi_3 \circ (\varphi_2 \circ \varphi_1)$, и операция "$\circ$" ассоциативна.

Для произвольной полугруппы справедлива следующая теорема.

Теорема. *В произведении* $x_1 \cdot x_2 \cdot \ldots \cdot x_n$ *элементов полугруппы* (X, $\cdot$) *скобки можно расставлять в произвольном порядке.*

Доказательство. Докажем, что для любого произведения элементов полугруппы (X, $\cdot$) справедливо равенство $x_1 \cdot x_2 \cdot \ldots \cdot x_n = x_1 \cdot (x_2 \cdot (\ldots (x_{n-1} \cdot x_n))\ldots)$. Доказательство будем проводить индукцией по числу n элементов произведения. Для $n = 3$ это утверждение верно в силу ассоциативности операции в полугруппе.

Пусть равенство верно для всех $n \le k$, докажем его справедливость для $n = k+1$. В этом случае в произведении $x_1 \cdot x_2 \cdot \ldots \cdot x_{k+1}$ операция умножения производится k раз, тогда обозначим при помощи скобок последнее, k^{-oe} применение операции, и запишем $x_1 \cdot x_2 \cdot \ldots \cdot x_{k+1} = (x_1 \cdot \ldots \cdot x_i)(x_{i+1} \cdot \ldots \cdot x_{k+1})$, причем i может быть любым от 1 до k. Каждая из этих скобок содержит произведение элементов, состоящее не более чем из k множителей, а поэтому $x_1 \cdot x_2 \cdot \ldots \cdot x_{k+1} = (x_1 \cdot (x_2 \cdot (\ldots x_i))\ldots) \cdot (x_{i+1} \cdot \ldots \cdot x_{k+1}) = x_1 \cdot ((x_2 \cdot \ldots \cdot x_i) \cdot (x_{i+1} \cdot \ldots \cdot x_{k+1})) =$

$= x_1 \cdot (x_2 \cdot (\ldots \cdot (x_k \cdot x_{k+1}))\ldots)$. Теорема доказана.

Если мы обозначим для каждого натурального $n \in N$ $x^n = x \cdot x \cdot \ldots \cdot x$ (n - раз) , то на основании доказанной теоремы легко увидеть справедливость следующих свойств полугруппы: для любых натуральных n и m, $x^{m+n} = x^m \cdot x^n$, и $(x^m)^n = x^{m\cdot n}$.

Определение. Пусть (X, $\cdot$) – полугруппа с единичным элементом e и $x \in X$. Элемент x' полугруппы называется *обратным* для элемента x , если $x \cdot x' = x' \cdot x = e$.

Если (X, $\cdot$) – полугруппа с единичным элементом, и каждый элемент из X имеет обратный, то алгебра (X, $\cdot$) называется *группой*.

Заметим, что если элемент x полугруппы имеет обратный, то он единственен. Действительно, если x' и x'' – два обратных для x элемента, то $x' \cdot x \cdot x'' = x' \cdot (x \cdot x'') = x' \cdot e = x'$, и $x' \cdot x \cdot x'' = (x' \cdot x) \cdot x'' = e \cdot x'' = x''$.

В силу этого замечания, обратный элемент для элемента x в случае мультипликативного обозначения операции обозначим x^{-1}, и $-x$ в случае аддитивного обозначения операции.

Понятие группы имеет тесную связь с вопросом о разрешимости уравнения $a \cdot x = в$ в произвольной полугруппе. Следующее утверждение раскрывает эту связь.

Теорема. *Полугруппа* $(X, \cdot)$ *является группой тогда и только тогда, когда для любых элементов* $a, в \in X$ *найдутся элементы* $x, y \in X$ *такие, что* $a \cdot x = в$ *и* $y \cdot a = в$.

Доказательство. Пусть $(X, \cdot)$ – группа. Тогда для любых $a, в \in X$ существуют в множестве X элементы $a^{-1}, в^{-1}$, а следовательно X содержит и $a^{-1} \cdot в$, и $в \cdot a^{-1}$. Положим $x = a^{-1} \cdot в$, $y = в \cdot a^{-1}$. Тогда $a \cdot x = a \cdot \left(a^{-1} \cdot в\right) = (a \cdot a^{-1}) \cdot в = e \cdot в = в$, аналогично $y \cdot a = в$, и необходимость доказана.

Докажем обратное, пусть для любых $a, в \in X$ найдутся $x, y \in X$ такие, что $a \cdot x = в$ и $y \cdot a = в$. Тогда найдутся x_a и y_a такие, что $a \cdot x_a = a$ и $y_a \cdot a = a$. Покажем, что x_a – правый единичный элемент для $(X, \cdot)$, а y_a – левый. Действительно, если $в$ – произвольный элемент полугруппы X, то существуют $x, y \in X$ такие, что $a \cdot x = в$ и $y \cdot a = в$, но тогда $в \cdot x_a = (y \cdot a) \cdot x_a = y \cdot (a \cdot x_a) = y \cdot a = в$, аналогично и $y_a \cdot в = в$. В силу произвольности $в \in X$ отсюда следует, что x_a – правый, а y_a – левый единичный элементы для всех элементов $(X, \cdot)$, а поскольку $y_a \cdot x_a = x_a$, и одновременно $y_a \cdot x_a = y_a$, то $x_a = y_a = e$ – единичный элемент. Таким образом, $(X, \cdot)$ – полугруппа с единицей. Покажем, что каждый элемент в ней имеет обратный. Пусть $x \in X$, тогда для пары $x, e \in X$ найдутся x', $x'' \in X$ такие, что $x'' \cdot x = e$ и $x \cdot x' = e$, но тогда $x'' \cdot x \cdot x' = x'' \cdot (x \cdot x') = x'' \cdot e = x''$, и $x'' \cdot x \cdot x' = (x'' \cdot x) \cdot x' = e \cdot x' = x'$, следовательно элемент $x'' = x'$ является обратным для x. Теорема доказана.

Замечание 1. Отметим, что для любых элементов $a, в$ группы $(X, \cdot)$ уравнения $ax = в$ и $ya = в$ имеют единственное решение (или однозначно разрешимы). Действительно, если $ax = в$, то $a^{-1} \cdot (a \cdot x) = a^{-1} \cdot в$, следовательно $x = a^{-1} \cdot в$, аналогично $y = в \cdot a^{-1}$.

Замечание 2. Элемент, обратный для обратного элемента, совпадает с исходным, т.е. $(x^{-1})^{-1} = x$. Это следует из единственности обратного для данного элемента в произвольной полугруппе.

Замечание 3. Отметим, что для любого элемента x группы $(X, \cdot)$ справедливо равенство $(x^{-1})^n = (x^n)^{-1}$ для каждого натурального числа n, а тогда, если мы определим $x^{-n} = (x^n)^{-1}$, и положим $x^0 = e$, то для любых целых чисел n и m выполняются равенства: $x^{nm} = (x^n)^m$ и $x^{m+n} = x^m \cdot x^n$.

Пример 2. Пусть $X = \{a\}$. Определим в X операцию "$\cdot$" следующим образом: положим $a \cdot a = a$. Тогда $(\{a\}, \cdot)$ – группа, в которой $a = e$ и $a = a^{-1}$.

Пример 3. Множество $(Z, +)$ всех целых чисел с операцией обычного сложения является группой. Здесь $e = 0$, а $(-x)$ является обратным элементом для x.

Пример 4. $(R\backslash\{0\}, \cdot)$ – множество всех действительных чисел, отличных от нуля, с операцией обычного умножения является группой. Здесь $e = 1$, а x^{-1} совпадает с $\frac{1}{x}$.

Пример 5. $(\Phi_X, \circ)$ – множество всех взаимно однозначных функций, отображающих $X \xrightarrow{на} X$ с операцией произведения (композиции) функций является группой. Здесь роль единицы играет тождественное отображение Δ_X $(y = x)$, а обратным элементом для функции φ является обратная функция φ^{-1}.

Группа $(\Phi_X, \circ)$ называется *группой преобразований множества X.*

Определение. Бинарная операция "$\cdot$", заданная в множестве X называется *коммутативной*, если для всех $x, y \in X$ выполняется равенство $x \cdot y = y \cdot x$

Определение. Пусть $(X, \cdot)$ – группа, Y – непустое подмножество множества X. Тогда, если множество Y относительно заданной в X операции "$\cdot$" само образует группу, то говорят, что $(Y, \cdot)$ – *подгруппа* группы $(X, \cdot)$.

Нетрудно видеть, что $(Y, \cdot)$, где $Y \subset X$ (и не пустое), является подгруппой группы $(X, \cdot)$ тогда и только тогда, когда выполняются следующие два условия:

1) *для любых* $x, y \in Y$, $x \cdot y \in Y$ *(т.е. Y вместе с любыми двумя своими элементами содержит их произведение*);

2) *для каждого* $x \in Y$, $x^{-1} \in Y$ *(т.е. Y вместе с каждым элементом содержит и обратный для него)*.

Рассмотрим некоторые бинарные алгебры с двумя заданными операциями.

Определение. Алгебра $(X, \cdot, +)$ с двумя бинарными операциями называется *кольцом*, если $(X,+)$ образует коммутативную группу, $(X, \cdot)$ образует полугруппу, и операция «умножения»("$\cdot$") является *дистрибутивной* относительно операции «сложения»("+"), т.е. выполняются условия:
для любых $x, y, z \in X$, $(x+y)\cdot z = x\cdot z + y\cdot z$, и $x\cdot(y+z) = x\cdot y + x\cdot z$.

Замечание. Порядок выполнения операций в алгебре $(X, \cdot, +)$ определяется с помощью скобок, однако принято считать, что при отсутствии таковых операция "$\cdot$" имеет приоритетное значение по сравнению с операцией "+".

Пример 6. Рассмотрим группу $(\{a\}, \cdot)$ из примера 2, тогда, если мы определим операцию *"+"* в множестве $\{a\}$, полагая $a + a = a \cdot a$, то получим алгебру $(\{a\},+, \cdot)$ – одноэлементное кольцо.

Пример 7. Множество целых чисел, с обычными операциями сложения и умножения $(Z, +, \cdot)$ является кольцом.

Пример 8. Положим K_f – множество всех числовых функций, отображающих множество X в множество действительных чисел R. Определим «сумму» функций $f + g = \gamma \in K_f$ следующим образом: $\gamma(x) = (f+g)(x) = f(x)+g(x)$ для каждого $x \in X$, и «произведение» функций $f \cdot g = \lambda \in K_f$, полагая $\lambda(x) = (f \cdot g)(x) = f(x) \cdot g(x)$ для каждого $x \in X$. Тогда алгебра $(K_f, +, \cdot)$ является кольцом.

Действительно, определим нулевую функцию $0(x) = 0$ для всех $x \in X$, тогда она является нейтральным элементом в множестве K_f относительно операции "+" ; для любой функции $f \in K_f$ функция $(-f)$, такая, что для каждого $x \in X$ $(-f)(x) = -f(x)$, является обратной для данной относительно операции "+", следовательно $(K_f, +)$ – коммутативная группа. Ассоциативность операции "$\cdot$" и дистрибутивность её относительно "+" следуют из свойств операций сложения и умножения в множестве действительных чисел R.

Определение. Алгебру $(P, +, \cdot)$ называют *полем*, если выполняются следующие условия:

1) $(P, +, \cdot)$ – кольцо;

2) $(P\backslash\{0\}, \cdot)$ является коммутативной группой, где 0 – это нейтральный элемент относительно операции "+".

Нейтральный элемент в поле (или кольце) относительно операции "$\cdot$" обозначают 1 и называют *единицей поля (кольца*), а 0 *– нулём поля (кольца)*.

Примерами полей могут служить: поле действительных чисел, а также поле $(Q, +, \cdot)$ рациональных чисел. Заметим, что кольцо $(Z, +, \cdot)$ не является полем.

Приведём некоторые свойства колец и полей.

Пусть $(K,+, \cdot)$ – произвольное кольцо, тогда справедливы следующие равенства:

1) $\boldsymbol{a \cdot 0 = 0 \cdot a = 0}$ для каждого $a \in K$

Доказательство. $a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$. Прибавим к обеим частям равенства элемент $-(a\cdot 0)$ – обратный для $(a\cdot 0)$ по отношению к операции "+", тогда, используя ассоциативность, получим: $0 = a\cdot 0 + 0 = a\cdot 0$, аналогично $0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a$, и прибавляя к обеим частям $-(0\cdot a)$, получим $0 = 0\cdot a + 0$, следовательно $0 = 0\cdot a$.

2) $\boldsymbol{-(ab) = (-a)b = a(-b)}$ для любых $a, b \in K$.

Доказательство. Докажем, что $-(a\cdot b) = (-a)b$. Действительно, в силу свойства дистрибутивности $(-a)\cdot b + a\cdot b = ((-a)+a)\cdot b = 0\cdot b = 0$ по свойству 1, следовательно $(-a)\cdot b = -(a\cdot b)$ в силу единственности обратного элемента для $a\cdot b$. Аналогично доказывается, что $-(a\cdot b) = a\cdot(-b)$.

3) Определим разность элементов a - $в$ следующим образом: a - $в$ = a+(-$в$). Тогда, для любых $a,в,c \in K$ будет справедливо равенство: (***a*** - ***в***)***c***=***ac*** - ***вc***.

Действительно, (a - $в$)·c = (a+(-$в$)) ·c = a·c+(-$в$)·c = a·c+(-($в$·c)) = a·c - $в$·c.

Исключительно важная роль в современной математике принадлежит булевым алгебрам.

Определение. Бинарная алгебра (B, + , ·) называется *булевой алгеброй*, если выполняются следующие условия:

1) Операции "+", "·" – коммутативны: для любых $a,в \in B$, $a+в = в+a$ и $a \cdot в = в \cdot a$.
2) Операции дистрибутивны относительно друг друга: для любых $a,в,c \in B$,
   ($a+в$)·c = a·c+$в$·c;
   (a ·$в$)+c = (a+c)·($в$+c).

3) ($\exists!$ $0 \in B$) (существует единственный элемент из B) такой, что $a+0 = a$ для каждого $a \in B$;
($\exists!$ $1 \in B$) (существует единственный элемент из B) такой, что $a \cdot 1 = a$ для каждого $a \in B$ – условия существования и единственности нулевого и единичного элементов.

4) Для каждого $a \in B$ ($\exists! a' \in B$) (существует единственный элемент из B) такой, что $a \cdot a' = 0$, $a + a' = 1$ (закон исключённого третьего).

Пример 8. Пусть X – непустое множество. Обозначим 2^X – множество всех подмножеств множества X. Тогда алгебра $(2^X, \cup, \cap)$ является булевой. Здесь в роли операции "+" рассматривается операция объединения, а в роли операции "·" – операция пересечения двух множеств. Нулём в данной алгебре служит пустое множество, единицей – само множество X, и для каждого $Y \in 2^X$, $Y' = X \setminus Y$.

Пример 9. Пусть B – множество всевозможных формул алгебры высказываний. Тогда, отождествляя равносильные формулы, мы получим булеву алгебру $(B, V, \&)$, здесь дизъюнкция служит операцией сложения "+", а конъюнкция – операцией умножения "·", роль нуля играет тождественно ложная, а роль единицы – тождественно истинная формулы, для формулы A формула A' совпадает с $\neg A$.

Более наглядно данную алгебру представляет следующий пример.

Пример 10. Положим B={a,b}. Определим операции "+" и "·" в множестве {a,b} следующим образом:

$a+a = a$, $a \cdot в = a$,
$a + в = в$, $a \cdot a = a$,
$в + a = в$, $в \cdot a = a$,
$в + в = в$, $в \cdot в = в$.

Тогда ({a,b}, + , ·) – булева алгебра, где $0 = a$, $1 = в$, и $a' = в$ а $в' = a$.

Определение. Пусть задана булева алгебра

(B, + , ·) (1)

Для данной булевой алгебры мы рассмотрим алгебраическую структуру

(B', $\oplus$, (·)), (2)

где $B = B'$, и для любых элементов $a,в \in B'$, $a \oplus в = a \cdot в$, $a(\cdot)в = a + в$. Заметим, что алгебра (2) также является булевой алгеброй, она называется *двойственной* к исходной алгебре (1). Нетрудно видеть, что $0' = 1$, $1' = 0$ (где $0'$ и $1'$ – ноль и единица алгебры (2)). Заметим также, что алгебра (1) является двойственной для алгебры (2), т.е. двойственная для двойственной алгебры совпадает с исходной.

Отметим некоторые свойства булевых алгебр.

1. *Двойственность.* Если справедлива некоторая формула для произвольной булевой алгебры, то будет справедлива и двойственная ей формула, т.е. формула, которая получается из исходной заменой операции "+" на "·", операции "·" на "+" , 0 на 1, и 1 на 0. Данное свойство позволяет удваивать число формул.

2. ***a*·*a* = *a*** (***a* + *a* = *a*** – двойственная формула) – *идемпотентность*.

Доказательство. $a \cdot a = a \cdot a + 0 = a \cdot a + a \cdot a' = a \cdot (a + a') = a \cdot 1 = a$.

3. ***a*·0 = 0***, (***a* + 1 = 1**) – *подавление*.

Доказательство. $a \cdot 0 = a \cdot 0 + 0 = a \cdot 0 + a \cdot a' = a \cdot (0 + a') = a \cdot a' = 0$.

4. *Ассоциативность*: (***a*·*в*)·*c* = *a*·(*в*·*c*)**, **((*a* + *в*) + *c* = *a* + (*в* + *c*))**.

Доказательство. Положим $(a\cdot в)\cdot c = x$, $a\cdot(в\cdot c) = y$, тогда $a + x = a + (a\cdot в)\cdot c = (a + a\cdot в)\cdot(a + c) = (a\cdot 1 + a\cdot в)\cdot(a + c) = a\cdot 1\cdot(a + c) = a\cdot a + a\cdot c = a\cdot 1 + a\cdot c = a\cdot(1 + c) = a\cdot 1 = a$. Аналогично рассмотрим $a + y = a + a\cdot(в\cdot c) = a\cdot 1 + a\cdot(в\cdot c) = a\cdot(1 + в\cdot c) = a\cdot 1 = a$, следовательно, $a + x = a + y$.

Заметим далее, что

$a' + x = a' + (a\cdot в)\cdot c = (a' + a\cdot в)\cdot(a' + c) = (a' + a)\cdot(a' + в)\cdot(a' + c) = (a' + в)\cdot(a' + c) = a' + в\cdot c$, и

$a' + y = a' + a\cdot(в\cdot c) = (a' + a)\cdot(a' + в\cdot c) = a' + в\cdot c$, таким образом $a' + x = a' + y$.

Рассмотрим полученную систему:

$$\begin{cases} a + x = a + y \\ a' + x = a' + y \end{cases}$$

Перемножая соответственно левые и правые части данных равенств получим, что $(a + x)\cdot(a' + x) = (a + y)(a' + y)$, тогда $a\cdot a' + x = a\cdot a' + y$, откуда и следует, что $x = y$.

5. *Обращение:* $\mathbf{(a\cdot в)' = a' + в'}$, $\mathbf{((a + в)' = a'\cdot в')}$.

Доказательство. $(a' + в')\cdot(a\cdot в) = a'\cdot(a\cdot в) + в'\cdot(a\cdot в) = (a'\cdot a)\cdot в + (в'\cdot в)\cdot a = 0\cdot в + 0\cdot a = 0$. Заметим далее, что $(a' + в') + (a\cdot в) = a' + (в' + a\cdot в) = a' + (в' + a)\cdot(в' + в) = a' + в' + a = (a' + a) + в' = в' + 1 = 1$, тогда, в силу закона исключения третьего, $a' + в' = (a\cdot в)'$.

6. *Законы поглощения*: $\mathbf{a\cdot(a + в) = a}$, $\mathbf{(a + (a\cdot в) = a)}$.

Доказательство. $a\cdot(a + в) = a\cdot a + a\cdot в = a\cdot 1 + a\cdot в = a\,(1 + в) = a$

7. *Склейка*: $\mathbf{(a + в)\cdot(a + в')} = \mathbf{a}$,

$\mathbf{((a\cdot в) + (a\cdot в')} = \mathbf{a)}$.

8. $\mathbf{(a')' = a}$ *– закон двойного дополнения.*

9. $0' = 1$,

$1' = 0$.

10. $a + a'\cdot в = a + в$ и $a\cdot(a' + в) = a\cdot в$ *– законы частичного поглощения.*

§5. Комплексные числа

5.1. Поле комплексных чисел

Рассмотрим $R^2 = R\times R = \{(x,y) \mid x,y\in R\}$ – декартов квадрат множества действительных чисел R. Напомним, что упорядоченные пары считаются равными: $(x_1,y_1)=(x_2,y_2)$ тогда и только тогда, когда $[(x_1=x_2) \wedge (y_1=y_2)]$. Определим в R^2 операцию сложения "+" упорядоченных пар следующим образом: положим $\mathbf{(x_1,y_1)+(x_2,y_2)=(x_1+x_2,y_1+y_2)}$.

Определенная таким образом операция сложения является ассоциативной и коммутативной в силу ассоциативности и коммутативности операции сложения в множестве действительных чисел. Здесь существует нейтральный элемент, им является пара $(0,0) = 0$. Обозначим $R^2 = C$. Отметим, что для каждого элемента $z\in C$ существует обратный (относительно операции сложения "+"): если $z = (x,y)$, то $-(x,y) = (-x,-y)$

Действительно, $(x,y)+(-x,-y) = (0,0)=0$. Таким образом, алгебра $(C, +)$ является коммутативной группой.

Введём операцию умножения "$\cdot$" упорядоченных пар в множестве C, полагая для любых пар (x_1,y_1) и (x_2,y_2) из данного множества $\mathbf{(x_1,y_1)\cdot(x_2,y_2) = (x_1x_2 - y_1y_2, x_1y_2+y_1x_2)}$.

Заметим, что определённая таким образом операция умножения обладает следующими свойствами:

1) $\mathbf{(x_1,y_1)\cdot(x_2,y_2) = (x_2,y_2)\cdot(x_1,y_1)}$ – *коммутативность*, следует из свойств операций умножения и сложения в множестве действительных чисел;

2) $\mathbf{((x_1,y_1)\cdot(x_2,y_2))\cdot(x_3,y_3) = (x_1,y_1)\cdot((x_2,y_2)\cdot(x_3,y_3))}$ – *ассоциативность.* Действительно, $(z_1\cdot z_2)\cdot z_3 = (x_1x_2-y_1y_2,\ x_1y_2+y_1x_2)\cdot(x_3,y_3) = (x_1x_2x_3-y_1y_2x_3-x_1y_2y_3-y_1x_2y_3,\ x_1y_3x_2-y_1y_2y_3+x_1y_2x_3+\ y_1x_2x_3) = (x_1(x_2x_3-y_2y_3)-y_1(x_2y_3+y_2x_3) = x_1(y_3x_2+y_2x_3)+y_1(x_2x_3-y_2y_3)) = (x_1y_1)(x_2x_3-y_2y_3,\ x_2y_3+y_2x_3) = (x_1,y_1)((x_2,y_2)(x_3,y_3)) = z_1\cdot(z_2\cdot z_3)$

3) (1,0) – *нейтральный элемент* относительно операции "$\cdot$", так как $(x,y)\cdot(1,0) = (x,y)$. Будем обозначать пару $(1, 0) = 1$

4) Пусть $(x,y)\neq(0,0)$ – отличный от нуля элемент C. Тогда существует элемент $\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right)\in C$, и произведение $\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right)(x,y)=\left(\frac{x^2+y^2}{x^2+y^2},0\right)=(1,0)=1$, следовательно $\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right)=(x,y)^{-1}$, и таким образом, алгебра $(C/\{0\},\ \cdot\ )$ является коммутативной группой.

5) Отметим, что операция умножения в алгебре $(C, +, \cdot)$ *дистрибутивна* относительно операции сложения, т.е. для любых элементов (x_1,y_1), (x_2,y_2), (x_3,y_3) множества C выполняется равенство: $\mathbf{((x_1,y_1)+(x_2,y_2))(x_3,y_3) = (x_1,y_1)(x_3,y_3)+(x_2,y_2)(x_3,y_3)}$.
Действительно, $(x_1+x_2,\ y_1+y_2)(x_3,y_3) = (x_1x_3+x_2x_3-y_1y_3-y_2y_3,\ x_1y_3+x_2y_3+y_1x_3+y_2x_3) = ((x_1x_3-y_1y_3)+(x_2x_3-y_2y_3),\ (x_1y_3+y_1x_3)+\ (x_2y_3+y_2x_3)) = (x_1,y_1)(x_3,y_3)+(x_2,y_2)(x_3,y_3)$.
Таким образом алгебра $(C, +, \cdot)$ является полем, назовем данную алгебраическую структуру *полем комплексных чисел*. Покажем, что в этом поле уравнение $z^2 = -1$ имеет решение. Действительно, если положим $z = (0,1)$, то $z^2 = (-1,0) = -(1,0) = -1$. Договоримся данную пару $(0,1)$ обозначать символом i, т.е. $i = (0,1)$.

Выделим в множестве C подмножество R', состоящее из всех пар с нулевой второй компонентой, т.е. $R' = \{(x,0) \mid x\in R\}$. Операции "+" и "$\cdot$" будут определены в R', т.е. для любых $z, z'\in R'$ $\quad z\cdot z',\ z+z'\in R'$. Действительно $(x,0)+(y,0)=(x+y,0)\in R'$, и $(x,0)\cdot(y,0) = (x\cdot y,0)$. Отметим, что $0\in R'$, и $1\in R'$, следовательно $(R', +, \cdot)$ является полем, и таким образом – подполем поля комплексных чисел $(C, +, \cdot)$.

Рассмотрим множество действительных чисел R и отображение f множества R на R', заданное следующим образом: для каждого $x\in R$ $\quad f(x)=(x,0)$. Нетрудно видеть, что f является взаимнооднозначным отображением множества R на R', причём это отображение задаёт соответствие элементов, сохраняющееся при операциях "+" и "$\cdot$", т.е. для любых элементов $x,y\in R$ $\quad f(x+y) = f(x)+f(y)$ и $f(x\cdot y) = f(x)\cdot f(y)$.

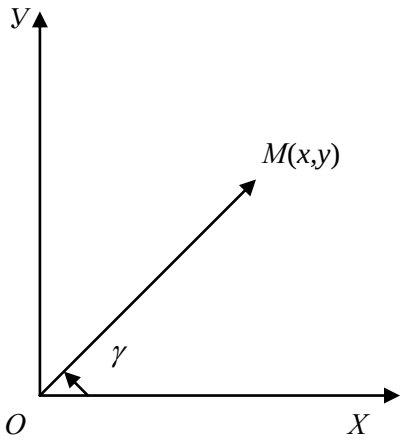
Такие соответствия называются *изоморфизмами алгебр*, и изоморфные алгебраические структуры отождествляются. Следовательно, мы можем считать, что R – подполе C, поскольку R и R' – изоморфны. При данном изоморфизме, паре $(a,0)\in R'$ соответствует число $a\in R$, в частности паре $(0,0) = 0$ соответствует число 0.

Любое комплексное число $z=(a,b)$ можно представить следующим образом: $z=(a,0)+(в,0)\cdot(0,1)$. Тогда, отождествляя в силу вышесказанного пару $(a,0)$ с действительным числом a и пару $(в,0)$ с действительным числом $в$, получим *алгебраическую форму* записи комплексного числа: $z = a + в\cdot i$. Отметим при этом, что операции сложения и умножения в данном выражении понимаются в смысле операций, определенных выше для комплексных чисел. Слагаемое $в\cdot i$ называется *мнимой частью*, а действительное число a *– действительной частью* данного комплексного числа z. Также заметим, что в силу отождествления $(0,0) = 0$ получим, что $a + 0\cdot i = a$, $\ 0 + в\cdot i = в\cdot i$, $\ 0\cdot z = 0$.

Запись комплексного числа в алгебраической форме позволяет нам пользоваться всеми свойствами операций + и $\cdot$ (коммутативностью, ассоциативностью, дистрибутивностью и т.д.) привычным для нас образом. Так, например, при сложении комплексных чисел в алгебраической форме мы будем просто складывать их действительные и мнимые части, при умножении комплексных чисел $z_1 = a + в\cdot i$ и $z_2 = c + d\cdot i$, отождествляя $i^2 = -1 + 0\cdot i = -1$, получаем $z_1z_2 = (a + в\cdot i)\,(c + d\cdot i) = ac + ad\cdot i + bc\cdot i + bd\cdot i^2 = ac - bd + (ad + bc)\cdot i$. При делении комплексных чисел в алгебраической форме поступают следующим образом:

$$\frac{z_1}{z_2} = \frac{a + b\cdot i}{c + d\cdot i} = \frac{(a + b\cdot i)(c - d\cdot i)}{(c + d\cdot i)(c - d\cdot i)} = \frac{ac + bd + (bc - ad)\cdot i}{c^2 + d^2} = \frac{ac + bd}{c^2 + d^2} + \frac{(bc - ad)}{c^2 + d^2}\cdot i \quad .$$

5.2. Геометрическая интерпретация поля комплексных чисел.



Рассмотрим прямоугольную декартову систему координат на плоскости *XOY*. Тогда каждому комплексному числу $z = x + y \cdot i$ мы можем поставить в соответствие единственную точку плоскости $M(x,y)$ с данными координатами. Заметим, что установленное таким образом соответствие между комплексными числами и точками плоскости является взаимнооднозначным. Существует взаимнооднозначное соответствие между точками плоскости и радиус-векторами данных точек (точке *M* соответствует вектор $\overline{OM}$), и таким образом устанавливается взаимнооднозначное соответствие между комплексными числами и радиус-векторами точек плоскости, соответствующих данным числам. При данном соответствии множеству R действительных чисел соответствует множество точек на оси OX.

Каждый вектор $\overline{OM}$ характеризуется длиной и направлением. Полагая r – длина вектора $\overline{OM}$, а γ – угол, образуемый данным вектором $\overline{OM}$ с положительным направлением оси OX, (отсчитываемый против часовой стрелки), мы получим *полярную систему координат* на плоскости. В ней каждой точке плоскости *M* (и, соответственно, радиус-вектору $\overline{OM}$ данной точки) соответствует упорядоченная пара действительных чисел (r, γ), причем декартовы координаты точки *M* связаны с полярными координатами следующим образом: $x = r \cdot \cos\gamma$, $y = r \cdot \sin\gamma$. Таким образом, используя полярную систему координат, каждое комплексное число $z = x + y \cdot i$, представленное в алгебраической форме, мы можем представить следующим образом: $z = x + y \cdot i = r \cdot \cos\gamma + (r \cdot \sin\gamma) \cdot i = r(\cos\gamma + i \cdot \sin\gamma)$. Данное представление называется *тригонометрической формой* комплексного числа. При этом длина вектора $\overline{OM}$, соответствующего числу z, называется *модулем комплексного числа* z и обозначается $|z|$, а угол γ - *аргументом числа* z, и обозначается $Argz$. Отметим, что модуль комплексного числа определен однозначно, $|z| = \sqrt{x^2 + y^2}$. Аргументы же комплексного числа этим свойством не обладают, но они отличаются друг от друга на $2\pi k$, где k – любое целое число, т.е. если $\gamma = Argz$, то угол $\gamma + 2\pi k$ также будет являться аргументом z. Если $-\pi < Argz \le \pi$, то он обозначается $\arg z$ и называется *главным значением аргумента* комплексного числа *z*. Отметим также, что представление комплексного числа в тригонометрической форме является единственным (с точностью до $2\pi k$).

5.3. Действия над комплексными числами в тригонометрической форме

Пусть $z_1 = x_1 + i \cdot y_1 = r_1 \cdot (\cos\gamma_1 + i \cdot \sin\gamma_1)$; $z_2 = x_2 + i \cdot y_2 = r_2 \cdot (\cos\gamma_2 + i \cdot \sin\gamma_2)$. Тогда $z_1 \cdot z_2 = r_1 \cdot r_2 (\cos\gamma_1 \cdot \cos\gamma_2 + i \cdot (\sin\gamma_2 \cdot \cos\gamma_1 + \cos\gamma_2 \cdot \sin\gamma_1) + i \cdot i \cdot \sin\gamma_1 \sin\gamma_2 = \mathbf{r_1 \cdot r_2 (\cos(\gamma_1 + \gamma_2) + i \cdot \sin(\gamma_1 + \gamma_2))}$. Таким образом, *при умножении двух комплексных чисел в тригонометрической форме их модули перемножаются, а аргументы складываются*. Данное свойство распространяется на произведение любого конечного числа комплексных чисел, и позволяет легко находить степень комплексного числа z^n при $n \in N$.

Если $z = r \cdot (\cos\gamma + i \cdot \sin\gamma)$, то из вышесказанного следует, что

$$\mathbf{z^n = r^n \cdot (\cos n\gamma + i \cdot \sin n\gamma)}$$

Это равенство называется *формулой Муавра*. Определим в C операцию деления на ненулевые элементы, полагая (при $z_2 \neq 0$) $\frac{z_1}{z_2} = z_1 \cdot z_2^{-1}$, тогда, поскольку *1* = 1·(cos 0 + *i*·sin 0) и $z_2 = r_2 \cdot (\cos \gamma_2 + i \cdot \sin \gamma_2)$, то $z_2^{-1} = \frac{1}{r_1} \cdot (\cos(-\gamma_2) + i \cdot \sin(-\gamma_2))$ в силу единственности обратного элемента для данного в группе, и $\frac{z_1}{z_2} = \frac{r_1}{r_2} \cdot (\cos(\gamma_1 - \gamma_2) + i \cdot \sin(\gamma_1 - \gamma_2))$, таким образом, *при делении комплексных чисел в тригонометрической форме модуль первого делится на модуль второго, а аргумент второго вычитается из аргумента первого.*

Далее мы рассмотрим вопрос извлечения корня *n*-й степени из комплексного числа z при любом $n \in N$. Будем полагать $z' = \sqrt[n]{z}$ если справедливо равенство $(z')^n = z$. Если число z в тригонометрической форме имеет вид $z = r \cdot (\cos\gamma + i \cdot \sin\gamma)$, а $z' = r' \cdot (\cos\gamma' + i \cdot \sin\gamma')$, то по формуле Муавра $(r')^n \cdot (\cos n \cdot \gamma' + i \cdot \sin n \cdot \gamma') = r \cdot (\cos\gamma + i \cdot \sin\gamma)$. Тогда, в силу единственности представления числа в тригонометрической форме, $(r')^n = r$, $\cos n \cdot \gamma' = \cos\gamma$, $\sin n \cdot \gamma' = \sin\gamma$, следовательно, $r' = \sqrt[n]{r}$, и $n \cdot \gamma' = \gamma + 2\pi k$, $k \in Z$, отсюда $\gamma' = \frac{\gamma + 2\pi k}{n}$, и таким образом, все корни из z имеют вид:

$(\sqrt[n]{z})_k = \sqrt[n]{r} \cdot (\cos \frac{\gamma + 2\pi k}{n} + i \cdot \sin \frac{\gamma + 2\pi k}{n})$, где *k = 0, 1, ... , (n – 1).*

Действительно, заметим, что $(\sqrt[n]{z})_{k=n} = (\sqrt[n]{z})_{k=0}$, $(\sqrt[n]{z})_{k=n+1} = (\sqrt[n]{z})_{k=1}, \ldots, (\sqrt[n]{z})_{k=2 \cdot n-1} = (\sqrt[n]{z})_{k=n-1}$, и т.д.

Таким образом, придавая k значения от 0 до (*n – 1*), мы получим n различных корней, которые геометрически будут лежать на окружности радиуса $r' = \sqrt[n]{r}$, и отстоять каждый от соседнего на угол $\frac{2\pi}{n}$ (они будут таким образом делить данную окружность на n равных частей). При всех остальных целых k мы будем попадать в эти уже построенные точки.

5.4. Комплексно - сопряженные числа.

Определение. Если комплексное число $z = x + y \cdot i$, то число $\bar{z} = x - y \cdot i$ называют *сопряжённым* для z.

Отметим некоторые свойства сопряжённых чисел:

1) $|z| = |\bar{z}|$;

2) комплексные числа z и $\bar{z}$ расположены симметрично относительно оси OX;

3) $\arg z = -\arg \bar{z}$;

4) $z\bar{z} = |z|^2$;

5) $\overline{z_1 \pm z_2} = \bar{z_1} \pm \bar{z_2}$;

6) $\overline{z_1 \cdot z_2} = \bar{z_1} \cdot \bar{z_2}$;

7) $\frac{\bar{z_1}}{z_2} = \overline{\left(\frac{z_1}{z_2}\right)}$.

Доказательство данных свойств не представляет затруднений и носит технический характер.

5.5. Корни из единицы

Пусть $\varepsilon_0, \varepsilon_1, ..., \varepsilon_{n-1}$ – все корни n-й степени из единицы, т.е. $\varepsilon_k = \left(\sqrt[n]{1}\right)_k$, $k = 0,1,2,..., n-1$. Поскольку $1 = 1\cdot(\cos 0 + i\cdot\sin 0)$, то $(\sqrt[n]{1})_k = \sqrt[n]{1}\cdot(\cos\frac{2\pi k}{n} + i\cdot\sin\frac{2\pi k}{n})$.

Заметим, что данные корни лежат на окружности единичного радиуса и делят её на n равных частей. Отсюда следует (поскольку 1 является одним из корней), что все недействительные корни из единицы можно разбить на пары сопряжённых чисел.

Отметим также, *что для любого комплексного числа z все его корни n-ой степени могут быть получены при умножении любого одного из его корней $z' = \sqrt[n]{z}$ на все корни n-й степени из единицы $\varepsilon_0, \varepsilon_1, ..., \varepsilon_{n-1}$*. Действительно, корни из единицы $\varepsilon_0, \varepsilon_1, ..., \varepsilon_{n-1}$ лежат на окружности единичного радиуса и отстоят друг от друга на угол $\frac{2\pi}{n}$, следовательно, произведение выбранного корня z' на них также даст аналогичное относительно друг друга расположение полученных чисел на окружности радиуса $\sqrt[n]{r}$, где $r = |z|$. Таким образом, мы получаем n различных комплексных чисел. Заметим, что все эти произведения являются корнями n-й степени из числа z, поскольку $\left(z'\cdot\varepsilon_j\right)^n = \left(z'\right)^n\cdot\varepsilon_j^n = z\cdot 1 = z$ при каждом $j = 0,1,...,(n-1)$.

5.6. Показательная форма комплексного числа.

Рассмотрим комплексное число z в тригонометрической форме $z = r\cdot\left(\cos\gamma + i\cdot\sin\gamma\right)$, и обозначим $e^{i\gamma} = \left(\cos\gamma + i\cdot\sin\gamma\right)$. Тогда число z можно записать в виде $z = re^{i\gamma}$; данный вид называется *показательной формой* комплексного числа. Исходя из свойств операций умножения и деления комплексных чисел в тригонометрической форме, мы получим справедливость следующих равенств: $z^n = r^n e^{i(n\gamma)}$, а также, если $z_1 = r_1 e^{i\gamma_1}$ и $z_2 = r_2 e^{i\gamma_2}$, то $z_1\cdot z_2 = r_1 r_2 e^{i(\gamma_1+\gamma_2)}$, а $\frac{z_1}{z_2} = r_1 r_2 e^{i(\gamma_1-\gamma_2)}$. Отметим также, что корни из комплексного числа z в показательной форме имеют вид: $\sqrt[n]{z} = \sqrt[n]{r}\cdot e^{\frac{\gamma+2\pi\kappa}{n}}$, где k = 0,1,…,(n - 1). Таким образом, показательная форма комплексного числа позволяет производить действия над комплексными числами в компактной, удобной форме.

ГЛАВА 2

СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ.

§6. Определители и их свойства.

6.1. Определители второго и третьего порядков.

Рассмотрим систему двух линейных уравнений с двумя неизвестными

$$\begin{cases} a_1x + a_2y = c_1 \\ b_1x + b_2y = c_2 \end{cases},$$

где a_i, b_i, c_i – элементы некоторого поля (**P**, +, ·) , $i = 1,2.$ Договоримся элементы поля **P** называть в дальнейшем *числами.* Умножим обе части первого уравнения на b_1 и вычтем из него соответствующие части второго, умноженные на a_1, тогда получим равенство

$$(a_2b_1 - a_1b_2)y = b_1c_1 - a_1c_2 .$$

Аналогично, умножая первое уравнение на b_2 и вычитая из него второе, умноженное на a_2, получим равенство

$$(a_1b_2 - a_2b_1)x = c_1b_2 - c_2a_2 .$$

Положим $a_1b_2 - a_2b_1 = \Delta$, тогда, если $\Delta \neq 0$, то определяя операцию деления в (**P**, +, ·), естественным образом полагая, что $\frac{c}{d} = cd^{-1}$ (при $d \neq 0$), получим, что $x = \frac{b_2c_1 - a_2c_2}{\Delta}$, $y = \frac{a_1c_2 - b_1c_1}{\Delta}$, где $\Delta = a_1b_2 - a_2b_1$.

Обозначим $c_1b_2 - a_2c_2 = \Delta_1$ и $a_1c_2 - c_1b_1 = \Delta_2$, тогда $x = \frac{\Delta_1}{\Delta}$, $y = \frac{\Delta_2}{\Delta}$.

Последние равенства называются *формулами Крамера*.

Решение данной системы уравнений с двумя неизвестными естественным образом приводит нас к определению матрицы и определителя второго порядка.

Определение. Квадратную таблицу, состоящую из двух строк и столбцов элементов поля **P**

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

мы назовём *квадратной матрицей второго порядка* над полем **P**.

Определителем квадратной матрицы A второго порядка называют число, полученное следующим образом:

$$|A| = \begin{vmatrix} a_{11}a_{12} \\ a_{21}a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

С учётом данного определения отметим, что величины $\Delta, \Delta_1, \Delta_2$, участвующие в приведённых формулах Крамера, совпадают с определителями второго порядка:

$$\Delta = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}, \ \Delta_1 = \begin{vmatrix} c_1 & a_2 \\ c_2 & b_2 \end{vmatrix}, \ \Delta_2 = \begin{vmatrix} a_1 & c_1 \\ b_1 & c_2 \end{vmatrix},$$

где Δ_1 получается из определителя Δ заменой первого столбика на столбик из свободных членов c_1, c_2, а Δ_2 – заменой второго столбика в определителе Δ на указанный столбец.

Определение. Пусть

$$A=\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

– *квадратная матрица третьего порядка* над полем Р. *Определителем* квадратной матрицы A третьего порядка называют число, полученное следующим образом:

$$|A|=\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}=a_{11}\cdot a_{22}\cdot a_{33}+a_{12}\cdot a_{23}\cdot a_{31}+a_{13}\cdot a_{21}\cdot a_{32}-a_{13}\cdot a_{22}\cdot a_{31}-a_{11}\cdot a_{23}\cdot a_{32}-a_{12}\cdot a_{21}\cdot a_{33}$$

Формулы Крамера справедливы также и для системы трёх линейных уравнений с тремя неизвестными

$$\begin{cases} a_{11}x+a_{12}y+a_{13}z=c_1 \\ a_{21}x+a_{21}y+a_{23}z=c_2 \\ a_{31}x+a_{32}y+a_{33}z=c_3 \end{cases}$$

Пусть $\Delta=|A|\neq 0$, тогда данная система имеет единственное решение, которое находится по формулам:

$$x=\frac{\Delta_1}{\Delta},\ y=\frac{\Delta_2}{\Delta},\ z=\frac{\Delta_3}{\Delta},$$

где Δ_i получается из определителя Δ путём замены *i*-го столбика на столбик из свободных членов c_1, c_2, c_3, $i=\overline{1,3}$. Данное утверждение будет нами доказано в дальнейшем.

6.2. Определитель *n*-го порядка.

Рассмотрим множество *P* первых n натуральных чисел: $P=\{1,2,...,n\}$. Если все эти числа записать в определенном порядке так, чтобы они не повторялись, то получим упорядоченную *n*-ку, являющейся элементом *n*-ой декартовой степени множества *P*, например $(1,2,..,n)$ – упорядоченная *n*-ка, причём напомним, что, например, $(2,1,...,n)\neq(1,2,...,n)$.

Любая такая упорядоченная *n*-ка называется *перестановкой.*

Выясним сколько всего перестановок из элементов *P* существует: на первом месте может быть любое из n чисел, на втором (при выбранном первом) – любое из оставшихся (n – 1) чисел, и т.д… Таким образом, число всех различных вариантов выбора элементов составляет произведение 1·2 ….. $(n-1)\cdot n = n!$ (n факториал), следовательно, число всех возможных перестановок первых n чисел равно $n!$

Рассмотрим произвольную перестановку ($\alpha_1, \alpha_2, \dots, \alpha_n$). Будем говорить, что пара (α_i, α_j) образует *инверсию*, если $i < j$, но $\alpha_i > \alpha_j$. Будем говорить, что перестановка *четная*, если в ней содержится четное число инверсий, и *нечетная* в противном случае.

Транспозицией будем называть перемену местами двух элементов перестановки.

Теорема. *Одна транспозиция меняет чётность перестановки.*

Доказательство. Рассмотрим перестановку ($\alpha_1, \dots, \alpha_i, \dots, \alpha_j, \dots, \alpha_n$). Совершим транспозицию двух элементов: поменяем местами элементы α_i и α_j. Если эти элементы соседние, то справедливость утверждения следует из того, что инверсии выбранных элементов с остальными элементами остаются такими же, а расположение их относительно друг друга меняется.

Пусть $j = i+\kappa$ и $\kappa\neq 1$. Тогда, после транспозиции элементов α_i и α_j мы получим перестановку ($\alpha_1, \dots, \alpha_j, \dots, \alpha_i, \dots, \alpha_n$). Данную перестановку можно также получить следующим образом: в исходной перестановке меняем местами α_i с α_{i+1}, затем α_i с α_{i+2}, и т.д., …, и, наконец, α_i с α_j. Всего при этом мы совершим κ транспозиций, и получим перестановку $(\alpha_1,\dots,\alpha_{i+1},\ \alpha_{i+2},\ \cdots\ \alpha_{i+k},\alpha_i,\dots,\alpha_n)$. Сделав затем ($\kappa$ – 1) транспозиций элемента α_{i+k}

поочередно с предыдущими, мы получим требуемую перестановку, где элементы α_i и α_j меняются местами (относительно исходной).

Таким образом, требуемую перестановку можно получить, совершив $(2k-1)$ транспозиций соседних элементов. Полученная перестановка, следовательно, имеет другую четность, нежели исходная, и теорема доказана.

Определение. Пусть $P=\{1,2,\ldots,n\}$. Взаимно-однозначное отображение φ множества P на себя называется подстановкой n - ой степени. Всякую подстановку можно записать в виде:

$$\begin{pmatrix} \alpha_1 & \cdots & \alpha_n \\ \varphi(\alpha_1) & \cdots & \varphi(\alpha_n) \end{pmatrix} \qquad (*)$$

или, в каноническом виде:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \beta_1 & \beta_2 & \cdots & \beta_n \end{pmatrix} \qquad (1)$$

где $(\alpha_1, \ldots, \alpha_n)$ – любая перестановка элементов из множества P, а $(\varphi(\alpha_1),\ldots,\varphi(\alpha_n))$ – тоже перестановка, состоящая из образов элементов верхней перестановки при данном отображении φ, причем $\beta_i=\varphi(i)$ при всех $i=1,2,\ldots,n$.

Подстановка называется *четной*, если четности верхней и нижней перестановок, образующих ее, совпадают, и *нечетной* в противном случае. Подстановку вида (*) очевидно можно привести за конечное число транспозиций (одновременно верхних и нижних соответствующих друг другу элементов) к каноническому виду (1). Четности подстановок (*) и (1) совпадают, поскольку каждая такая транспозиция меняет одновременно четность верхней и нижней перестановок, составляющих подстановку, поэтому данное определение четности и нечетности подстановки является корректным (не зависит от вида, в котором данная подстановка будет представлена).

Заметим, что множество всех подстановок n-ой степени образует *группу преобразований* множества P, а все четные подстановки в ней образуют подгруппу. Отметим также, что число подстановок n-ой степени совпадает с числом перестановок и равно $n!$.

Определение. Прямоугольную таблицу, состоящую из n строк и m столбцов, элементами которой являются элементы некоторого поля $\mathbf{P}$, мы будем называть *матрицей размерности* $n\times m$ над полем $\mathbf{P}$:

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{pmatrix}$$

Каждый элемент a_{ij} матрицы A имеет два индекса: первый индекс указывает номер строки, а второй – номер столбца, в котором находится данный элемент. Будем данную матрицу A обозначать также: $A=(a_{ij})_{n\times m}$, или $A=[a_{ij}]_{n\times m}$.

Замечание. В дальнейшем мы рассматриваем матрицы и определители над полем действительных чисел, но все рассуждения и результаты без ограниченной общности переносятся на случай *любого другого поля.*

Если число строк и столбцов матрицы A совпадает и равно n, то матрица A называется *квадратной матрицей n-ого порядка.*

Определение. Пусть матрица A – это квадратная матрица n-ого порядка. *Определителем* матрицы A называется сумма всевозможных произведений элементов матрицы A, стоящих в различных строках и столбцах, взятых со знаком "+" или " – " в зависимости от четности подстановки, образуемой индексами элементов произведения; "+" в случае четной, и " – " в случае нечетной.

Данное определение справедливо и для определителя 1-го порядка, в этом случае определитель одноэлементной матрицы равен данному элементу. Таким образом, обозначая определитель матрицы A как $|A|$, получим, что

$$|A|=\sum(-1)^{\delta}a_{1\alpha_1}\cdot a_{2\alpha_2}\cdot\ldots\cdot a_{n\alpha_n},$$

где $\delta=1$, если перестановка $(\alpha_1,\ldots,\alpha_n)$ – нечетная, и $\delta=0$, если перестановка $(\alpha_1,\ldots,\alpha_n)$ – четная. Каждое слагаемое указанной суммы мы будем называть *членом определителя* $|A|$. Заметим, что число всех членов определителя равно $n!$.

6.3. Свойства определителей.

Свойство 1. *Если в определителе существует строчка (столбец) состоящая из одних нулей, то данный определитель равен нулю.*

Определение. Матрица $A'=\left(a'_{ij}\right)_{m\times n}$ называется *транспонированной* матрицей для матрицы $A = (a_{ij})_{n\times m}$ и обозначается A^{T}, если для любых индексов $i = \overline{1,m}$ и $j = \overline{1,n}$ выполняется условие: $a'_{ij} = a_{ji}$.

Столбцами матрицы A^{T} являются соответствующие строки матрицы A, а строчками матрицы A^{T} – соответствующие столбцы матрицы A.

Например, если $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$, то $A^{\mathrm{T}} = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$.

Заметим, что $(A^{\mathrm{T}})^{\mathrm{T}} = A$ (транспонирование транспонированной приводит к исходной матрице).

Свойство 2. *При транспонировании матрицы её определитель не меняется.*

Доказательство. Пусть $A = (a_{ij})_{n\times n}$. Тогда каждый член определителя $|A|$ имеет вид $(-1)^{\delta}\cdot a_{1\alpha_1}\cdot a_{2\alpha_2}\cdot\ldots\cdot a_{n\alpha_n}$, где δ определяется четностью подстановки

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}.$$

Заметим, что данный член является также членом определителя $|A^{\mathrm{T}}|$ в силу того, что он представляется в виде $(-1)^{\delta}a'_{\alpha_1 1}\cdot a'_{\alpha_2 2}\cdot\ldots\cdot a'_{\alpha_n n}$, где a'_{ij} - элементы матрицы A^{T} . Поскольку подстановка

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

имеет ту же четность, что и приведенная выше, то и знак вхождения данного члена в определитель $|A^{\mathrm{T}}|$ тот же самый, что и знак вхождения в определитель $|A|$. Таким образом, перебирая все члены определителя $|A|$, мы получим все члены определителя $|A^{\mathrm{T}}|$, и данное свойство доказано.

Замечание. Полученное свойство позволяет нам все доказанные утверждения относительно строк определителя переносить на столбцы (и наоборот).

Свойство 3. *При перемене местами двух строк (столбцов) определитель меняет свой знак на противоположный.*

Доказательство. Пусть $A = (a_{ij})_{n\times n}$, и матрица A' получена из матрицы A переменой местами i-ой и j-ой строчек. Тогда каждый член исходного определителя $|A|$ имеет вид $(-1)^{\delta}a_{1\alpha_1}\cdot a_{2\alpha_2}\cdot\ldots\cdot a_{n\alpha_n}$. Отметим, что данное произведение является также и членом определителя $|A'|$, однако знак его вхождения в $|A'|$ определяется четностью подстановки

$$\begin{pmatrix} 1 & 2 & \ldots & i & \ldots & j & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_j & \ldots & \alpha_i & \ldots & \alpha_n \end{pmatrix},$$

четность которой не совпадает с четностью подстановки

$$\begin{pmatrix} 1 & 2 & \ldots & i & \ldots & j & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_i & \ldots & \alpha_j & \ldots & \alpha_n \end{pmatrix},$$

определяющей δ, и следовательно знак вхождения данного произведения в $|A'|$ является противоположным относительно знака вхождения его в определитель $|A|$. Перебирая таким образом все члены определителя $|A|$, мы получим все члены определителя $|A'|$, взятые с обратным знаком, и свойство (3) доказано.

Свойство 4. *Если в определителе существуют две одинаковые строчки (столбца), то данный определитель равен нулю.*

Доказательство. Если в определителе $|A|$ существует две одинаковые строки, то, поменяв их местами, получим, что $|A| = -|A|$, следовательно $|A| = 0$.

Определение. Пусть $\overline{e_i} = (a_{i1} \quad a_{i2} \quad \ldots \quad a_{in})$ – строка матрицы, α – любое число. *Произведением строки* $\overline{e_i}$ *на число* α называется строка $\alpha \cdot \overline{e_i} = (\alpha \cdot a_{i1} \quad \alpha \cdot a_{i2} \quad \ldots \quad \alpha \cdot a_{in})$.

Аналогично определяется *произведение столбца на число.*

Свойство 5. *Если в определителе строчку (столбец) умножить на некоторое число, то сам исходный определитель умножится на это число.*

Доказательство. Пусть в определителе $|A|$ каждый элемент *i*-ой строки умножается на число *k*, тогда получим определитель

$$|A'| = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ k \cdot a_{i1} & k \cdot a_{i2} & \ldots & k \cdot a_{in} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix},$$

причём $|A'| = \sum (-1)^n a_{1\alpha_1} \cdots k a_{i\alpha_i} \cdots a_{n\alpha_n} = k \cdot |A|$, и всё доказано.

Определение. Пусть $\overline{e_i} = (a_{i1} \quad a_{i2} \quad \ldots \quad a_{in})$ и $\overline{e_j} = (a_{j1} \quad a_{j2} \quad \ldots \quad a_{jn})$ – две строки одинаковой размерности. *Суммой этих строк называется* строка $\overline{e_i} + \overline{e_j} = (a_{i1} + a_{j1} \quad a_{i2} + a_{j2} \quad \ldots \quad a_{in} + a_{jn})$.

Аналогичным образом определяется *сумма столбцов одинаковой размерности*.

Свойство 6. *Если каждый элемент строчки (столбца) исходной матрицы можно представить в виде суммы двух слагаемых, то исходный определитель равен сумме двух определителей, определяемых первыми и вторыми слагаемыми, т.е.*

$$|A'| = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{i1} + b_{i1} & a_{i2} + b_{i2} & \ldots & a_{in} + b_{in} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots & \ldots \\ b_{i1} & b_{i2} & \ldots & b_{in} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}$$

Доказательство.

$|A'| = \sum (-1)^{\delta} a_{1\alpha_1} \cdots (a_{i\alpha_i} + b_{i\alpha_i}) \cdots a_{n\alpha_n} = \sum (-1)^{\delta} a_{1\alpha_1} \cdots a_{i\alpha_i} \cdots a_{n\alpha_n} \cdots + \sum (-1)^{\delta} a_{1\alpha_1} \cdots b_{1\alpha_1} \cdots a_{n\alpha_n}$, откуда и следует требуемое равенство.

Свойство 7. *Если в определителе существуют две пропорциональные строки (столбца), то данный определитель равен нулю.*

Доказательство. Если в определителе $|A|$ элементы $a_{jk} = c \cdot a_{ik}$ для всех $k = \overline{1,n}$, то $|A| = c|A'| = 0$, поскольку в определителе $|A'|$ *i*-я и *j*-я строки одинаковые.

Свойство 8. *Если к строке (столбцу) определителя прибавить другую строчку (столбец), умноженную на некоторое число, то определитель не изменится.*

Данное свойство непосредственно следует из свойств 6 и 7.

Определение. Пусть $\overline{e_1}$, ..., $\overline{e_k}$ – это некоторые строки матрицы *A*. *Линейной комбинацией данных строк* с коэффициентами $\beta_1, \ldots, \beta_k$ мы назовем строку, получающуюся следующим образом:

$\overline{e} = \beta_1 \overline{e}_1 + \beta_2 \overline{e}_2 + \cdots + \beta_k \overline{e}_k = (\beta_1 a_{11} + \beta_2 a_{21} + \cdots + \beta_k a_{k1} \quad \beta_1 a_{12} + \beta_2 a_{22} + \cdots + \beta_k a_{k2} \quad \cdots$

$\cdots \quad \beta_1 a_{1n} + \beta_2 a_{2n} + \cdots + \beta_k a_{kn})$.

Аналогичным образом определяется понятие *линейной комбинации столбцов матрицы A*.

Свойство 9. *Если одна из строк (столбцов) определителя* $|A|$ *является линейной комбинацией всех его остальных строк (столбцов), то данный определитель равен нулю*.

Действительно, если одна из строк является линейной комбинацией остальных, то разложим определитель в сумму (n – 1) определителей, каждый из которых будет содержать две пропорциональные строки, и, следовательно, равен нулю.

Определение. Строчки $\overline{e_1}, \overline{e_2}, \ldots, \overline{e_k}$ называют *линейно зависимыми,* если найдется такой набор чисел $\alpha_1, \ldots, \alpha_n$, среди которых хотя бы одно отлично от нуля, что линейная комбинация данных строк с указанными коэффициентами дает нулевую строку, т.е.

$$\sum_{i=1}^{k} \alpha_i \overline{e}_i = \overline{0} = (0 \quad 0 \quad 0 \quad \cdots \quad 0).$$

Линейную комбинацию строк (столбцов) хотя бы с одним ненулевым коэффициентом называют *нетривиальной.*

Теорема. *Система строк* $\overline{e_1}, \ldots, \overline{e_n}$ *одинаковой размерности линейно зависима тогда и только тогда, когда одна из этих строк является линейной комбинацией остальных.*

Доказательство. Допустим, что система строк $\overline{e_1}, \ldots, \overline{e_n}$ линейно зависима, тогда найдется такой нетривиальный набор чисел $\alpha_1, \ldots, \alpha_n$, что $\alpha_1 \cdot \overline{e_1} + \ldots + \alpha_n \cdot \overline{e_n} = \overline{0}$.

Поскольку найдется $\alpha_i \neq 0$, то, прибавляя к обеим частям равенства $(-\alpha_i) \cdot \overline{e_i}$, получим $\alpha_1 \cdot \overline{e_1} + \ldots + \alpha_n \cdot \overline{e_n} = -\alpha_i \cdot \overline{e_i}$ (в данном равенстве слагаемое в левой части с индексом i отсутствует). Умножив обе части равенства на число $\left(-\frac{1}{\alpha_i}\right)$, получим, что

$$\overline{e_i} = \sum_{\substack{j=1 \\ j \neq i}}^{n} a_j^* \cdot \overline{e_j}, \quad \text{где} \quad a_j^* = -\frac{\alpha_j}{\alpha_i}.$$

Обратно, если одна из данных строчек является линейной комбинацией всех остальных, то найдется i такое, что $\overline{e_i} = \sum_{\substack{j=1 \\ j \neq i}}^{n} a_j \cdot \overline{e_j}$, тогда, прибавив к обеим частям данного равенства ($-\overline{e_i}$), получим: $-\overline{e_i} + \sum_{\substack{j=1 \\ j \neq i}}^{n} a_j \cdot \overline{e_j} = \overline{0}$, и, таким образом, система строк $\overline{e_1}, \ldots, \overline{e_n}$ – линейно зависима, так как в данной нулевой линейной комбинации коэффициент $\alpha_i = -1$. Теорема доказана.

Свойство 10. *Если между строками (столбцами) определителя существует линейная зависимость, то данный определитель равен нулю*.

Действительно, если между строками определителя существует линейная зависимость, то одна из них является линейной комбинацией остальных, и, следовательно, определитель равен нулю.

6.4. Вычисление определителей.

Определение. Пусть A – квадратная матрица n-го порядка. Если мы вычеркнем из матрицы A i-ю строку и j-й столбец, то определитель полученной матрицы (n – 1) - го порядка называют *минором* элемента a_{ij} и обозначают M_{ij}. *Алгебраическим дополнением* элемента a_{ij} называют число $A_{ij} = (-1)^{i+j} \cdot M_{ij}$.

Пример.

$$A = \begin{vmatrix} 1 & 2 & 3 \\ 4 & 1 & 2 \\ 6 & 7 & 9 \end{vmatrix}, \quad M_{33} = \begin{vmatrix} 1 & 2 \\ 4 & 1 \end{vmatrix}, \quad A_{33} = (-1)^{3+3} \cdot \begin{vmatrix} 1 & 2 \\ 4 & 1 \end{vmatrix}, \quad A_{23} = (-1)^{2+3} \cdot \begin{vmatrix} 1 & 2 \\ 6 & 7 \end{vmatrix}.$$

Теорема. *Если в квадратной матрице A n-го порядка существует строка, все элементы которой, за исключением одного, равны нулю, то определитель матрицы A равен произведению данного элемента на его алгебраическое дополнение.*

Доказательство.

1. Пусть данный ненулевой элемент находится в первой строчке и в первом столбике матрицы A, т.е., для всех $j \neq 1$, $a_{1j} = 0$. Тогда, поскольку по определению $|A| = \sum (-1)^{\delta} a_{1\alpha_1} \cdot a_{2\alpha_2} \cdot \ldots \cdot a_{n\alpha_n}$, то так как $a_{1\alpha_1} = 0$ при всех $\alpha_1 \neq 1$, то $|A| = \sum (-1)^{\delta} a_{11} \cdot a_{2\alpha_2} \cdot \ldots \cdot a_{n\alpha_n} = a_{11} \sum (-1)^{\delta} a_{2\alpha_2} \cdot \ldots \cdot a_{n\alpha_n}$, где δ определяется чётностью подстановки

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & \alpha_2 & \cdots & \cdots & \alpha_n \end{pmatrix}.$$

Заметим, что каждое произведение $(-1)^{\delta} a_{2\alpha_2} \cdot \ldots \cdot a_{n\alpha_n}$ – это не что иное, как член минора M_{11}, причём знак вхождения данного произведения в M_{11} будет то же самый, поскольку определяется чётностью подстановки $\begin{pmatrix} 1 & 2 & \ldots & n-1 \\ \alpha_2 - 1 & \alpha_3 - 1 & \ldots & \alpha_n - 1 \end{pmatrix}$, составленной из индексов, с которыми сомножители произведения входят в определитель M_{11}. Таким образом, в этом случае $|A| = a_{11} \cdot M_{11} = a_{11} \cdot (-1)^{1+1} \cdot M_{11} = a_{11} \cdot A_{11}$.

2. Пусть все элементы i-й строки, за исключением a_{ij}, равны нулю.

Меняем j-й столбик поочередно местами с предыдущими столбцами до тех пор, пока он не окажется на первом месте. После этого, аналогичным образом, i-ю строчку поднимаем вверх. В результате мы получаем определитель $|A'|$ с единственным ненулевым первым элементом в первой строке. Заметим, что в результате этих преобразований определитель $|A|$ поменяет знак $(i + j - 2)$ раза. Полученный определитель $|A'| = a_{ij} A'_{11}$ по доказанному первому пункту.

При указанной перемене местами строк и столбцов, элементы остальных строк и столбцов (кроме i-й строки и j-го столбца) остались в том же положении относительно друг друга. Поэтому, вычеркивание i-й строки и j-го столбца в исходной матрице A и вычеркивание первой строки и первого столбца в получившейся матрице A' приводят к одному и тому же минору. Тогда $|A'| = a_{ij} A'_{11} = a_{ij} (-1)^{1+1} M'_{11} = a_{ij} M_{ij}$. С другой стороны $|A'| = (-1)^{i+j-2} |A|$, следовательно, и определитель $|A| = (-1)^{i+j} |A'|$, а тогда $|A| = (-1)^{i+j} a_{ij} M_{ij} = a_{ij} A_{ij}$. Теорема доказана.

Теорема. *Определитель матрицы A равен сумме произведений элементов любого его столбца (строки) на их соответствующие алгебраические дополнения*, т.е. если $A = (a_{ij})_{n \times n}$, то $|A| = \sum_{k=1}^{n} a_{ki} A_{ki}$, и $|A| = \sum_{k=1}^{n} a_{ik} A_{ik}$ для каждого $i = 1, 2, \ldots, n$.

Доказательство. Пусть

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

Тогда, поскольку i-ю строку мы можем представить в виде суммы: $(a_{i1} \quad a_{i2} \quad \cdots \quad a_{in}) = (a_{i1} \quad 0 \quad 0 \quad \cdots \quad 0) + (0 \quad a_{i2} \quad 0 \quad \cdots \quad 0) + \ldots + (0 \quad 0 \quad 0 \quad \cdots \quad a_{in})$ строк с единственным ненулевым элементом, то $|A|$ можно представить в виде суммы n определителей

$|A| = |A^{(1)}| + |A^{(2)}| + ... |A^{(n)}|$, где все определители $|A^{(j)}|$ при $j = 1,2,...,n$ отличаются друг от друга и от определителя $|A|$ только одной i-ой строчкой:

$$|A| = \begin{vmatrix} a_{11} & \dots & \dots & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & \dots & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \dots & \dots & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & a_{i2} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & \dots & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \dots & \dots & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & a_{i3} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & \dots & \dots & a_{nn} \end{vmatrix} + ... +$$

$$+ \begin{vmatrix} a_{11} & \dots & \dots & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & \dots & \dots & a_{nn} \end{vmatrix} = a_{i1} \cdot A_{i1}^{(1)} + a_{i2} \cdot A_{i2}^{(2)} + a_{i3} \cdot A_{i3}^{(3)} + .. + A_{in}^{(n)} = a_{i1} \cdot A_{i1} + a_{i2} \cdot A_{i2} + a_{i3} \cdot A_{i3} + ... + a_{in} \cdot A_{in},$$

так как $A_{ij}^{(j)} = A_{ij}$ для всех $j = \overline{1,n}$. Теорема доказана.

Пример.

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 2 & 6 \\ 2 & 1 & 2 & 3 \\ 2 & 2 & 4 & 1 \end{vmatrix} = 1 \cdot A_{11} + 1 \cdot A_{21} + 2 \cdot A_{31} + 2 \cdot A_{41},$$

таким образом, вычисление данного определителя четвертого порядка сводится к вычислению четырёх определителей третьего порядка. На практике, чтобы упростить вычисления, получают вначале определитель с минимальным числом ненулевых элементов в некотором столбце (строке) при помощи прибавления к строкам (столбцам) других строк (столбцов), умноженных на некоторые коэффициенты, а уже затем вычисляют его по данной теореме. Таким образом, значительно проще будет вычислять приведенный в примере определитель, используя подобный способ:

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 2 & 6 \\ 2 & 1 & 2 & 3 \\ 2 & 2 & 4 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & -1 & 2 \\ 0 & -3 & -4 & -5 \\ 0 & -2 & -2 & -7 \end{vmatrix} = 1 \cdot (-1)^{1+1} \begin{vmatrix} 0 & -1 & 2 \\ -3 & -4 & -5 \\ -2 & -2 & -7 \end{vmatrix} = \begin{vmatrix} 0 & -1 & 0 \\ -3 & -4 & -13 \\ -2 & -2 & -11 \end{vmatrix} =$$

$$= (-1) \cdot (-1)^{1+2} \cdot \begin{vmatrix} -3 & -13 \\ -2 & -11 \end{vmatrix}.$$

В данных вычислениях, в исходном определителе мы из второй строки вычитали первую, из третьей – первую, умноженную на 2, из четвертой – первую, умноженную на 2, затем разложили полученный определитель по первому столбцу. В полученном определителе третьего порядка к третьему столбику прибавляем второй, умноженный на 2, и затем разложим его по первой строчке.

Теорема. *Сумма произведений элементов строки (столбца) определителя на алгебраические дополнения соответствующих элементов другой строки (столбца) равна нулю.*

Доказательство. Рассмотрим произвольную квадратную матрицу

$$A=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

Пусть $i \neq j$, тогда, заменив в матрице A j-ю строку на i-ю, мы получим матрицу A', определитель которой $|A'|=0$, поскольку в нём присутствуют две одинаковые строки. С другой стороны $|A'|=a'_{j1}\cdot A'_{j1}+\ldots+a'_{jn}\cdot A'_{jn}=\sum_{k=1}^{n} a_{ik}\cdot A_{jk}$, поскольку $a'_{jk}=a_{ik}$, а $A'_{jk}=A_{jk}$ для всех $k=\overline{1,n}$. Теорема доказана.

§7. Формулы Крамера.

Рассмотрим систему n линейных уравнений с n неизвестными $x_1, x_2, \ldots, x_n$:

$$\begin{cases} a_{11}x_1+a_{12}x_2+\ldots+a_{1n}x_n=b_1 \\ a_{21}x_1+a_{22}x_2+\ldots+a_{2n}x_n=b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n`1}x_1+a_{n2}x_2+\ldots+a_{nn}x_n=b_n \end{cases} \qquad (1)$$

Обозначим

$$A=\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} \qquad (2)$$

– матрицу данной системы (1), и

$$B=\begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_n \end{pmatrix} \qquad (3)$$

– столбец, состоящий из свободных членов данной системы (1). Положим $|A|=\Delta$. Далее, для каждого $i=\overline{1,n}$ определим определитель Δ_i следующим образом:

$$\Delta_i=\begin{vmatrix} a_{11} & \ldots & \overset{(i)}{b_1} & \ldots & a_{1n} \\ a_{21} & \ldots & b_2 & \ldots & a_{2n} \\ \ldots & \ldots & b_3 & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & \ldots & b_n & \ldots & a_{nn} \end{vmatrix},$$

т.е. определитель Δ_i получается из определителя Δ заменой i-го столбца на столбец B свободных членов системы (1).

Теорема. *Если система линейных уравнений (1) имеет матрицу с ненулевым определителем, то система имеет единственное решение, которое находится по формулам Крамера:*

$$x_1 = \frac{\Delta_1}{\Delta},\ \ x_2 = \frac{\Delta_2}{\Delta},\ \ \ldots\ldots,\ \ x_n = \frac{\Delta_n}{\Delta}.$$

Доказательство. Пусть определитель матрицы A данной системы уравнений отличен от нуля, и система (1) имеет решение $x_1, x_2, \ldots, x_n$. Умножив первое уравнение на A_{11}, второе на A_{21}, … , n-е на A_{n1}, и сложив затем их все, получим следующее равенство:

$$x_1(a_{11}\cdot A_{11} + a_{21}\cdot A_{21} + \ldots + a_{n1}\cdot A_{n1}) + x_2(a_{12}\cdot A_{11} + a_{22}\cdot A_{21} + \ldots + a_{n2}\cdot A_{n1}) + \ldots +$$
$$+ x_n(a_{1n}\cdot A_{11} + a_{2n}\cdot A_{21} + \ldots + a_{nn}\cdot A_{n1}) = b_1\cdot A_{11} + b_2\cdot A_{21} + \ldots + b_n\cdot A_{n1}$$

Заметим, что каждое из выражений, стоящих в скобках в левой части, кроме первого, равно нулю в силу последней теоремы, а выражение, стоящее в первой скобке равно Δ, правая же часть данного равенства совпадает с Δ_1, следовательно, $x_1\Delta = \Delta_1$, откуда $x_1 = \frac{\Delta_1}{\Delta}$.

Если бы мы первое уравнение умножили на A_{12}, второе на A_{22}, … , n-е на A_{n2} и просуммировали, мы аналогично получили бы равенство $x_2 = \frac{\Delta_2}{\Delta}$.

Продолжая этот процесс, мы получим таким образом, что для каждого $j = \overline{1,n}$ будет выполняться равенство $x_j = \frac{\Delta_j}{\Delta}$.

Докажем, что найденные значения $x_1,\ x_2, \ldots,\ x_n$ действительно образуют решение системы уравнений (1). Действительно, для каждого $i = \overline{1,n}$

$$a_{i1}x_1 + \ldots + a_{in}x_n = \sum_{k=1}^{n} a_{ik}\cdot x_k = \sum_{k=1}^{n} a_{ik}\cdot\frac{\Delta_k}{\Delta} = \frac{1}{\Delta}\sum_{k=1}^{n} a_{ik}\cdot\Delta_k = \frac{1}{\Delta}\sum_{k=1}^{n} a_{ik}\left(\sum_{j=1}^{n} b_j\cdot A_{jk}\right) =$$
$$= \frac{1}{\Delta}\sum_{k=1}^{n}\sum_{j=1}^{n}\left(a_{ik}\cdot b_j\cdot A_{jk}\right) = \frac{1}{\Delta}\sum_{j=1}^{n}\sum_{k=1}^{n}\left(b_j\cdot a_{ik}\cdot A_{jk}\right) = \frac{1}{\Delta}\sum_{j=1}^{n}\left(b_j\cdot\sum_{k=1}^{n} a_{ik}\cdot A_{jk}\right) = \frac{1}{\Delta}b_i\cdot\Delta = b_i\ .$$

Теорема доказана.

§8. Матрицы и действия над ними.

Определение. Пусть даны две матрицы $A = (a_{ij})_{m\times n}$ и $B = (b_{ij})_{m\times n}$ одинаковой размерности над полем **P**. *Суммой* данных матриц называют матрицу C той же размерности, каждый элемент которой равен сумме соответствующих элементов первой и второй матрицы: т.е. $A_{m\times n} + B_{m\times n} = C_{m\times n}$, где $C = (c_{ij})_{m\times n}$ и $c_{ij} = a_{ij} + b_{ij}$ для всех $i = \overline{1,m}$ и $j = \overline{1,n}$.

Приведём некоторые свойства определённой нами операции сложения матриц.

1. $A + B = B + A$;
2. $(A + B) + C = A + (B + C)$;

3. $0 = (0)_{m\times n}$ – нулевая матрица, является нейтральным элементом в данной алгебре матриц, т.е. $A + 0 = A$;

4. $-A = (-a_{ij})_{m\times n}$ – обратный элемент для матрицы A относительно операции сложения.

Таким образом, *множество матриц одинаковой размерности образует коммутативную группу по сложению.*

Определение. Пусть $A = (a_{ij})_{m\times n}$, где $a_{ij}\in\mathbf{P}$ и $\alpha\in\mathbf{P}$, **P** – некоторое поле.

Произведением матрицы A на число α мы будем называть матрицу $D = \alpha\cdot A$, такую, что все её элементы получены в результате произведения элементов матрицы A на α, т.е. $D = (d_{ij})_{m\times n}$, где элементы $d_{ij} = \alpha\cdot a_{ij}$ для всех $i = \overline{1,m}$ и $j = \overline{1,n}$.

Определённая таким образом операция умножения матрицы на число обладает следующими достаточно очевидными свойствами, вытекающими из свойств операций поля **P**:

1. $(\alpha \cdot \beta) \cdot A = \alpha \cdot (\beta \cdot A) = \beta \cdot (\alpha \cdot A)$**;**

2. $0 \cdot A = \boldsymbol{0}$**;**

3. $1 \cdot A = A$**;**

4. $(\alpha + \beta) \cdot A = \alpha \cdot A + \beta \cdot A$**;**

5. $\alpha \cdot (A + B) = \alpha \cdot A + \alpha \cdot B$**;**

где α, β – любые элементы поля **P.**

Заметим, что любую матрицу A размерности $m \times n$ можно рассматривать в виде строки размерности $m \cdot n$, или столбца той же размерности.

Определение. Пусть A и B – матрицы размерности $m \times n$ и $n \times k$ соответственно, т.е. $A = (a_{ij})_{m \times n}$ и $B = (b_{ij})_{n \times k}$. *Произведением матрицы A на матрицу B* мы будем называть матрицу $C = A \cdot B$ размерности $m \times k$ такую, что $C = (c_{ij})_{m \times k}$, где $c_{ij} = \sum_{s=1}^{n} a_{is} \cdot b_{sj}$ для всех $i = \overline{1, m}$ и $j = \overline{1, k}$.

Другими словами, каждый элемент c_{ij} матрицы C равен сумме произведений соответствующих элементов i*-й* строки матрицы A и j*-го* столбца матрицы B.

Заметим, что *умножение матриц определено в том и только в том случае, когда число столбцов первой матрицы совпадает с числом строк второй*, поэтому произведение матриц, очевидно, не является коммутативной операцией. Отметим следующие свойства операции произведения матриц:

1. *Ассоциативность*, т.е. $A \cdot (B \cdot C) = (A \cdot B) \cdot C$.

Данное равенство справедливо для любых матриц *A, B, C*, для которых определена хотя бы одна из частей равенства (т.е. из определённости левой части следует определённость правой и их равенство и наоборот).

2. *Дистрибутивность относительно сложения*, т.е. $(A + B) \cdot C = A \cdot C + B \cdot C$, $A \cdot (B + C) = A \cdot B + A \cdot C$.

3. $\alpha \cdot (A \cdot B) = (\alpha \cdot A) \cdot B = A \cdot (\alpha \cdot B)$ для любого $\alpha \in \mathbf{P}$.

4. Если A – квадратная матрица n-го порядка, то $A \cdot E = E \cdot A = A$, где E – *единичная* матрица n-го порядка, определяемая следующим образом:

$$E = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

т.е. E – квадратная матрица, у которой по главной диагонали расположены единицы, а остальные элементы равны нулю.

5. *Если A и B – квадратные матрицы n-го порядка, то* $|A \cdot B| = |A| \cdot |B|$.

6. $(A \cdot B)^T = B^T \cdot A^T$. Здесь также из определённости левой части следует определённость правой и их равенство, и наоборот.

Доказательство всех данных свойств, за исключением пятого, носит технический характер и не представляет сложностей, поэтому предлагается проделать самостоятельно.

Определение. Пусть A – квадратная матрица n-го порядка. Матрица A' n-го порядка, являющаяся обратным элементом для матрицы A относительно операции произведения матриц, называется *обратной* для матрицы A (т.е. A' обратная, если $A \cdot A' = A' \cdot A = E$), и обозначается A^{-1} в силу её единственности (при условии существования). Отметим, что не каждая квадратная матрица имеет обратную, например нулевая матрица, очевидно, не обладает обратной. Условие существования обратной матрицы для данной описывает следующая теорема.

Теорема. *Квадратная матрица A n-го порядка имеет обратную матрицу тогда и только тогда, когда определитель $|A|$ отличен от нуля.*

Доказательство.

Достаточность. Пусть определитель квадратной матрицы A *n*-го порядка отличен от нуля, т.е.

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

и $|A|\neq 0$. Рассмотрим матрицу $\tilde{A}$, определённую следующим образом:

$$\tilde{A}=\begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix},$$

где A_{ij} – алгебраические дополнения элементов a_{ij} матрицы A. Назовём $\tilde{A}$ присоединенной матрицей для матрицы A. Положим $\frac{1}{|A|}\cdot\tilde{A}=A'$ и покажем, что матрица A' является обратной для матрицы A. Действительно, $\left(\frac{1}{|A|}\cdot\tilde{A}\right)\cdot A=\frac{1}{|A|}\left(\tilde{A}\cdot A\right)=E$, так как если c_{ij} – элементы матрицы $\left(\tilde{A}\cdot A\right)$, то $c_{ij}=\sum_{s=1}^{n}A_{si}\cdot a_{sj}=\begin{cases}0, & i\neq j\\ |A|, & i=j\end{cases}$. Совершенно аналогично доказывается, что $A\cdot\left(\frac{1}{|A|}\cdot\tilde{A}\right)=\frac{1}{|A|}\cdot\left(A\cdot\tilde{A}\right)=E$, и таким образом матрица A' является обратной матрицей для A.

Необходимость. Пусть обратная матрица для матрицы A существует, докажем, что определитель $|A|$ отличен от нуля. Допустим, что $|A|=0$. Тогда $\left|A\cdot A^{-1}\right|=|E|=1$, но с другой стороны $|A|\cdot\left|A^{-1}\right|=0$. Полученное противоречие доказывает неверность нашего предположения.

Теорема доказана.

Замечание. Отметим, что данное доказательство теоремы содержит конкретный способ нахождения обратной матрицы для любой невырожденной матрицы.

Отметим ещё несколько достаточно очевидных свойств произведения матриц.

7. $\left(A^{-1}\right)^{-1}=A$.

8. $(AB)^{-1}=B^{-1}A^{-1}$.

9. *Множество квадратных матриц n-го порядка с операциями сложения и умножения матриц образует кольцо.*

10. *Множество квадратных невырожденных (т.е. с ненулевым определителем) матриц n-го порядка образует группу по умножению матриц.*

§9. Ранг матрицы.

Определение. Пусть дана матрица $A_{m\times n}$. Выберем в этой матрице произвольным образом некоторые *к* строк и *к* столбцов. Рассмотрим элементы матрицы *A*, стоящие на пересечении выбранных строк и столбцов. Определитель, состоящий из данных элементов, стоящих в том же порядке, называется *минором к - го порядка матрицы A*.

Например, для матрицы

$$A=\begin{pmatrix}2 & 3 & 4 & 5\\ 6 & 1 & 2 & 3\\ 2 & 1 & 3 & 0\end{pmatrix},$$

выбирая первую и третью строчки и второй и четвертый столбцы, мы получим определитель

$$\begin{vmatrix}3 & 5\\ 1 & 0\end{vmatrix}$$

– минор второго порядка матрицы A.

Определение. *Рангом матрицы* A называется наивысший порядок отличного от нуля минора матрицы A.

Ранг матрицы A будем обозначать $r(A)$, или $rg(A)$. Очевидно, если $A=(a_{ij})_{m\times n}$, то $rg(A)\le m$ и $rg(A)\le n$.

Определение. *Элементарными преобразованиями* матрицы $A=(a_{ij})_{m\times n}$ называются следующие преобразования:

- *перемена местами строк (столбцов)*;
- *умножение всех элементов строки (столбца) на ненулевое число*;
- *прибавление к строке (столбцу) другой строки (столбца), умноженной на любое число*;
- *транспонирование матрицы.*

Теорема. *Элементарные преобразования не меняют ранга матрицы*.

Доказательство.

1). Рассмотрим произвольную матрицу A и поменяем в ней местами i-ю и j-ю строчки, получим матрицу A'. Тогда любой минор матрицы A' является либо минором матрицы A, либо может быть получен из минора матрицы A при помощи перемены местами строк. Поэтому ранг матрицы A' будет не больше ранга матрицы A, т.е. $rg(A')\le rg(A)$.

Заметим, что матрица A получается из матрицы A' обратной перестановкой указанных строк, следовательно и $rg(A)\le rg(A')$. Значит, $rg(A')=rg(A)$.

2). Если в матрице A умножить j-й столбик на любое ненулевое число α, то получим матрицу A'. Тогда каждый минор матрицы A' – либо минор матрицы A, либо минор, полученный умножением соответствующего минора матрицы A на число α, и поэтому $rg(A')\le rg(A)$.

Поскольку A получается из A' при умножении j-го столбца на $1/\alpha$, то аналогично и $rg(A)\le rg(A')$, следовательно $rg(A')=rg(A)$.

3). Пусть к i-й строчке матрицы A прибавлена j-*ая* строчка, умноженная на α. Получим матрицу A' следующего вида:

$$A'=\begin{pmatrix}a_{11} & a_{12} & \dots & a_{1n}\\ \dots & \dots & \dots & \dots\\ a_{i1}+\alpha\cdot a_{j1} & a_{i2}+\alpha\cdot a_{j2} & \dots & a_{in}+\alpha\cdot a_{jn}\\ \dots & \dots & \dots & \dots\\ a_{j1} & a_{j2} & \dots & a_{jn}\\ \dots & \dots & \dots & \dots\\ a_{m1} & a_{m2} & \dots & a_{mn}\end{pmatrix}$$

Данная матрица A' отличается от матрицы A только одной i-й строчкой.

Рассмотрим любой минор матрицы A'. Если он не содержит i-ю и j-ю строчки, то он является минором исходной матрицы. Если он содержит i-ю и j-ю строчки, то его можно рассматривать как сумму двух миноров, где первый будет являться минором исходной матрицы, а второй будет равен 0, в силу того, что он содержит две пропорциональные строки.

Если же в выбранном миноре есть j-я строчка, а i-й строки нет, то данный минор также является минором исходной матрицы.

Наконец, если минор не содержит *j*-ю строчку, но содержит *i*-ю, то он разлагается на сумму двух миноров, где первый является минором исходной матрицы, а второй – минор, полученный путем перестановки строк из минора исходной матрицы, и умножения строки на число.

Таким образом мы видим, что данное преобразование не увеличивает ранга матрицы. Но матрица A также может быть получена из матрицы A' путем прибавления к *i*-й строке *j*-й строки, умноженной на число $(-\alpha)$, следовательно $rg(A') = rg(A)$.

4). Если $A' = A^T$, то любой минор матрицы A' получается транспонированием минора матрицы A, и следовательно $rg(A^T) \le rg(A)$, но поскольку $(A^T)^T = A$, то $rg(A) = rg(A^T)$

Определение. Если ранг матрицы *A* равен r, то любой ее отличный от нуля минор порядка r называется *базисным*.

Теорема (о базисном миноре). *Пусть ранг матрицы A равен числу r. Тогда строки (столбцы) данной матрицы, в которых расположен ее базисный минор, являются линейно независимыми, и каждая строка (столбец) матрицы A может быть представлена в виде линейной комбинации данных r строк (столбцов).*

Доказательство. Пусть дана матрица

$$A = \begin{pmatrix} a_{11} & a_{12} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2n} \\ \dots\dots\dots\dots\dots \\ a_{m1} & a_{m2} \dots a_{mn} \end{pmatrix},$$

и пусть $rg(A) = r$. Рассмотрим произвольный базисный минор M матрицы A. Пусть он получен пересечением строк $i_1, \dots, i_r$ и столбиков $j_1, \dots, j_r$ данной матрицы, т.е.

$$M = \begin{vmatrix} a_{i_1 j_1} & a_{i_1 j_2} \dots a_{i_1 j_r} \\ a_{i_2 j_1} & a_{i_2 j_2} \dots a_{i_2 j_r} \\ \dots\dots\dots\dots\dots\dots \\ a_{i_r j_1} & a_{i_r j_2} \dots a_{i_r j_r} \end{vmatrix}.$$

1). Докажем, что строки $\overline{e}_{i_1}, \dots, \overline{e_{i_r}}$ матрицы A являются линейно независимыми.

Допустим, это не так. Тогда существует набор чисел $\alpha_1, \alpha_2, \dots, \alpha_r$ (и найдется индекс i, для которого $\alpha_i \neq 0$) такой, что линейная комбинация $\alpha_1 \overline{e_{i_1}} + \dots + \alpha_r \overline{e_{i_r}} = \overline{0}$.

Данное равенство говорит о том, что линейная покомпонентная комбинация элементов данных строк с указанными коэффициентами $\alpha_1, \alpha_2, \dots, \alpha_r$ равна нулю для каждой компоненты.

Тогда, если мы возьмем строчки $\overline{e'_{i_1}}, \dots, \overline{e'_{i_r}}$ определителя M, то заметим, что каждая из них является частью строки основной матрицы, следовательно, получим, что и для них справедливо равенство: $\alpha_1 \overline{e'_{i_1}} + \dots + \alpha_r \overline{e'_{i_r}} = \overline{0}$. Значит, между строчками минора M существует линейная зависимость, следовательно, $M = 0$, что противоречит нашему условию выбора минора M, и таким образом система строк $\overline{e}_{i_1}, \dots, \overline{e_{i_r}}$ матрицы A является линейно независимой.

2). Докажем, что любая из строк матрицы A может быть представлена в виде линейной комбинации данных линейно независимых строк $\overline{e}_{i_1}, \dots, \overline{e_{i_r}}$.

Пусть натуральные числа j и k таковы, что $1 \le j \le n$, причем $k \neq i_1, i_2 \dots i_r$, и $1 \le k \le m$. Тогда для каждого такого индекса k и каждого такого j рассмотрим строчку $\overline{e_k} = (a_{k1} a_{k2} \dots a_{kn})$ и столбец $\begin{pmatrix} a_{1j} \\ a_{2j} \\ \dots \\ a_{mj} \end{pmatrix}$ матрицы A. Добавляя к минору M элементы данных столбца и строчки, стоящие на пересечении с ними строчек $i_1, \dots, i_r, k$ и столбцов $j_1, \dots, j_r, j$, получим определитель $(r+1)$-го порядка

$$M' = \begin{vmatrix} a_{i_1 j_1} & a_{i_1 j_2} \dots a_{i_1 j_r} & a_{i_1 j} \\ a_{i_2 j_1} & a_{i_2 j_2} \dots a_{i_2 j_r} & a_{i_2 j} \\ \dots\dots\dots & \dots\dots\dots & \dots\dots \\ a_{i_r j_1} & a_{i_r j_2} \dots a_{i_r j_r} & a_{i_r j} \\ a_{k j_1} & a_{k j_2} \dots a_{k j_r} & a_{k j} \end{vmatrix}.$$

Отметим, что $M' = 0$, так как если $j \neq j_1, j_2, ..., j_r$, то M' является минором $(r+1)$-го порядка матрицы A, в случае же, если индекс j принимает одно из значений $j_1, j_2, j_3, ..., j_r$, то M' не будет являться минором матрицы A, но он все равно будет равен нулю, поскольку содержит тогда два одинаковых столбца.

Рассмотрим разложение, определителя M' по последнему столбику: $M' = a_{i_1 j} A'_{i_1 j} + a_{i_2 j} A'_{i_2 j} + ... + a_{i_r j} A'_{i_r j} + a_{i_k j} A'_{i_k j}$, где $A'_{i_s j}$ – алгебраические дополнения элементов $(r+1)$-го столбца в определителе M'.

Заметим, что числа $A'_{i_s j}$ не зависят от индекса j, и, следовательно, являются постоянными одновременно для всех $j = \overline{1,n}$. Заметим также, что $A'_{kj} = (-1)^{2(r+1)} M \neq 0$.

Отсюда следует, что $a_{kj} = \alpha'_1 a_{i_1 j} + \alpha'_2 a_{i_2 j} + ... + \alpha'_r a_{i_r j}$, где коэффициенты $\alpha'_s = -\dfrac{A'_{i_s j}}{A'_{kj}}$, $(s = \overline{1,2})$ не зависят от j, поэтому, придавая j все значения от 1 до n, мы пробегаем все элементы k-ой строчки матрицы A, что означает, что строчка $\bar{e}_k$ является линейной комбинацией указанных строк $\bar{e}_1, \bar{e}_2, \dots\dots, \bar{e}_r$ с коэффициентами $\alpha'_1, \alpha'_2, \ , \alpha'_r$. Теорема доказана.

Следствие. *Определитель квадратной матрицы A n-ого порядка равен нулю тогда и только тогда, когда между ее строчками (столбцами) существует линейная зависимость.*

Доказательство. Если строки матрицы A линейно зависимы, то ее определитель будет равен нулю по свойству 10.

Обратно, если определитель $|A|$ равен нулю, то отсюда следует, что $rg(A) < n$ (n – порядок матрицы). Пусть $rg(A) = r$, тогда в определителе $|A|$ существуют r линейно независимых строк, и по теореме о базисном миноре найдется строчка $\bar{e}$ матрицы A, не входящая в указанную систему строк, которая может быть представлена в виде линейной комбинации данных r линейно независимых строк. Отсюда следует, что данная строчка $\bar{e}$ может быть представлена в виде линейной комбинации всех остальных строк матрицы A, а тогда все строчки матрицы A являются линейно зависимыми. Следствие доказано.

§10. Решение систем линейных уравнений.

10.1. Совместность системы линейных уравнений.

Рассмотрим систему m линейных уравнений с n неизвестными

$$\begin{cases} a_{11} x_1 + a_{12} x_2 + \dots + a_{1n} x_n = b_1, \\ a_{21} x_1 + a_{22} x_2 + \dots + a_{2n} x_n = b_2, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1} x_1 + a_{m2} x_2 + \dots + a_{mn} x_n = b_m. \end{cases} \qquad (1)$$

Как и ранее, матрицу A, составленную из коэффициентов при неизвестных $x_1, x_2, ..., x_n$:

$$A = \begin{pmatrix} a_{11} & a_{12} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2n} \\ \dots\dots\dots\dots\dots \\ a_{m1} & a_{m2} \dots a_{mn} \end{pmatrix},$$

будем называть матрицей системы (1), матрицу A_p, полученную добавлением к матрице A столбика свободных членов:

$$A_p = \begin{pmatrix} a_{11} & a_{12} \dots a_{1n} & b_1 \\ a_{21} & a_{22} \dots a_{2n} & b_2 \\ \dots\dots\dots\dots\dots\dots\dots \\ a_{m1} & a_{m2} \dots a_{mn} & b_m \end{pmatrix},$$

назовём *расширенной матрицей* системы (1).

Положим $X = \begin{pmatrix} x_1 \\ x_2 \\ .. \\ x_n \end{pmatrix}$, $B = \begin{pmatrix} b_1 \\ b_2 \\ .. \\ b_m \end{pmatrix}$, тогда система (1) может быть представлена в виде

$$AX = B. \qquad (1)'$$

Данное равенство называется *матричной формой записи* системы (1).

Теорема (Кронекера – Капелли). *Система (1) совместна тогда и только тогда, когда ранги матрицы системы и расширенной матрицы системы совпадают.*

Доказательство.

Необходимость. Пусть система (1) совместна, тогда существует набор значений переменных x^0_1, x^0_2 ... x^0_n , который удовлетворяет всем уравнениям системы (1). Используя операции умножения столбцов на числа и сложения столбцов, получим тогда, что будет справедливо равенство

$$\begin{pmatrix} a_{11} \\ a_{21} \\ .. \\ a_{m1} \end{pmatrix} x^0_1 + \begin{pmatrix} a_{12} \\ a_{22} \\ .. \\ a_{m2} \end{pmatrix} x^0_2 + \dots + \begin{pmatrix} a_{1n} \\ a_{2n} \\ .. \\ a_{mn} \end{pmatrix} x^0_n = \begin{pmatrix} b_1 \\ b_2 \\ .. \\ b_m \end{pmatrix},$$

и таким образом последний столбик матрицы A_p является линейной комбинацией всех остальных столбиков. Тогда, если мы к последнему столбику матрицы A_p прибавим первый, умноженный на $(-x^0_1)$, второй умноженный на $(-x^0_2)$, и т.д.,…, и, наконец, n-й, умноженный на $(-x^0_n)$, то в полученной матрице A'_p последним столбцом станет нулевой столбик, т.е. A'_p имеет вид:

$$A'_p = \begin{pmatrix} a_{11} & a_{12} \dots a_{1n} & 0 \\ a_{21} & a_{22} \dots a_{2n} & 0 \\ \dots\dots\dots\dots\dots\dots \\ a_{m1} & a_{m2} \dots a_{mn} & 0 \end{pmatrix}.$$

Поскольку добавление к матрице нулевого столбика не увеличит её ранг, то, следовательно, $rg(A'_p)$ и $rg(A)$ совпадают. С другой стороны, по теореме об элементарных преобразованиях, $rg(A'_p) = rg(A_p)$, и следовательно $rg(A) = rg(A_p)$.

Достаточность. Пусть ранги основной матрицы A и расширенной матрицы A_p системы (1) совпадают. Покажем, что она совместна (двумя способами).

1. Пусть ранги данных матриц совпадают и равны r, тогда для матрицы A существует базисный минор порядка r, который расположен в строках и столбцах матрицы A; этот минор является базисным и для A_p, тогда, по замечанию к теореме о базисном миноре, последний столбик матрицы A_p представляется в виде линейной комбинации столбиков матрицы A, входящих в этот минор.

Пусть это будут столбики с номерами j_1, j_2 ...j_r, тогда, как сказано выше, найдутся коэффициенты $\alpha_1\ \alpha_2,\ldots,\ \alpha_r$ такие, что

$$\begin{pmatrix} a_{1j_1} \\ a_{2j_1} \\ .. \\ a_{mj_1} \end{pmatrix}\alpha_1+\begin{pmatrix} a_{1j_2} \\ a_{2j_2} \\ .. \\ a_{mj_2} \end{pmatrix}\alpha_2+\ldots+\begin{pmatrix} a_{1j_r} \\ a_{2j_r} \\ .. \\ a_{mj_r} \end{pmatrix}\alpha_r=\begin{pmatrix} b_1 \\ b_2 \\ .. \\ b_m \end{pmatrix}\ .$$

Добавим в левую сторону данного равенства все остальные столбики матрицы A, умножив их на 0. Тогда получим, что набор коэффициентов $\alpha_1\ ,\ldots,\ \alpha_n$ из левой части полученного равенства будет являться решением системы (1), следовательно, система (1) является совместной.

2. Пусть $rg(A)$ совпадает с $rg(A_p)$, тогда у данных матриц существует общий базисный минор. Рассмотрим этот общий базисный минор порядка r, без ограничения общности мы можем считать, что он находится в верхнем левом углу матрицы.

Если это не так, то мы можем этого добиться перестановкой строк и столбцов расширенной матрицы, что соответствует тому, что в исходной системе уравнений будут переставлены местами уравнения (при перестановке строк) и будут переименовываться (или переставляться) неизвестные при перестановке столбцов. В результате, полученная при этом матрица A'_p с требуемым верхним базисным минором, будет определять систему, равносильную исходной:

$$A'_p=\left(\begin{array}{cccc|ccc} a'_{11} & a'_{12}\ldots a'_{1r} & . & a'_{1r+1}\ldots a'_{1n} & b'_1 \\ a'_{21} & a'_{22}\ldots a'_{2r} & . & a'_{2r+1}\ldots a'_{2n} & b'_2 \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots & \ldots\ldots \\ a'_{r1} & a'_{r2}\ldots a'_{rr} & . & a'_{rr+1}\ldots a'_{rn} & b'_r \\ \hline \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots & \ldots\ldots \\ a'_{m1} & a'_{m2}\ldots a'_{mr} & & a'_{mr+1}\ldots a'_{mn} & b'_m \end{array}\right)\ .$$

При этом последний столбик $\begin{pmatrix} b'_1 \\ \ldots \\ b'_m \end{pmatrix}$ остается на своем (n + 1)-м месте, но могут поменяться местами его элементы. В матрице A'_p все строчки, начиная с (r+1)-й, являются линейной комбинацией первых r строчек по теореме о базисном миноре, следовательно, для системы уравнений, определяемой матрицей A'_p, каждое уравнение, начиная с (r+1)-го, является линейной комбинацией первых r уравнений. Это значит, что все оставшиеся уравнения, начиная с (r+1)-го, являются следствиями первых r уравнений, т.е. каждое решение первых r уравнений является и решением для остальных. Тогда решение полученной системы сводится к решению системы, состоящей из первых r уравнений. Возьмем первые r уравнений, и в левой их части оставим только члены, содержащие первые r неизвестных (возможно переименованных), назовём их *базисными*. Оставшиеся члены уравнений переносим в правую часть. Будем придавать всем оставшимся переменным (назовём их *свободными*) произвольные значения. Тогда, при каждом таком наборе значений свободных переменных, получаем столбик из свободных членов в правой части системы уравнений, но тогда, полученная при этом система уравнений имеет решение, причем единственное, которое находится по формулам Крамера, в силу того, что определитель матрицы полученной системы отличается от нуля.

Придавая свободным переменным другие значения, мы будем получать другие решения, при этом возможны следующие варианты:

$r = n$ (т.е. ранг равен числу неизвестных) или $(n - r) = 0$, тогда система имеет единственное решение;

$r < n$, число свободных неизвестных $(n-r) \neq 0$. В этом случае, придавая свободным неизвестным всевозможные значения, мы получаем бесконечное множество решений.

Теорема доказана.

10.2. Метод Гаусса.

Рассмотрим систему (1). Тогда, если мы к некоторой строчке расширенной матрицы A_p данной системы прибавим некоторую другую строчку, умноженную на число, или поменяем местами строчки или столбики (кроме последнего), то это будет равносильно тому, что в системе уравнений мы проделываем такие же операции с самими уравнениями. Следовательно, указанные преобразования приводят к тому, что полученная при этом матрица будет определять систему уравнений, равносильную исходной. Поэтому мы будем производить преобразования расширенной матрицы A_p.

Проводя указанные выше элементарные преобразования, мы приводим матрицу A_p к трапецеидальному или треугольному виду, т.е. к такому виду, когда все элементы, стоящие ниже главной диагонали – нулевые, а стоящие на главной диагонали – ненулевые (до появления оставшихся нулевых строк). Для этого мы зафиксируем первую строку таким образом, чтобы элемент a_{11} был отличен от нуля, и к каждой строке с номером $j = \overline{2,m}$ прибавим первую, умноженную на $\left(-\frac{a_{j1}}{a_{11}}\right)$. Тогда мы получим матрицу, у которой в первом столбике ниже элемента a_{11} будут расположены нули. Затем, сделав если нужно перестановку столбиков так, чтобы во второй строке второй элемент a'_{22} был отличен от нуля, мы, проводя аналогичные преобразования, приведём матрицу к такому виду, когда ниже элемента a'_{22} во втором столбике будут расположены нули, прибавляя к каждой j-ой строке ($j = \overline{3,m}$) вторую, умноженную на $\left(-\frac{a'_{j2}}{a'_{22}}\right)$, и т.д., … , до завершения этого процесса.

Вид полученной матрицы позволяет нам ответить на вопросы:

1) о совместности системы;
2) о количестве решений;
3) найти все решения.

Пусть ранг исходной матрицы A равен r. Тогда в результате преобразований мы получим матрицу A'_p:

$$A'_p = \begin{pmatrix} a'_{11} & a'_{12} & a'_{13} & \dots & a'_{r} & \dots & a'_{1n} & b'_1 \\ 0 & a'_{22} & a'_{23} & \dots & a'_{2r} & \dots & a'_{2n} & b'_2 \\ 0 & 0 & a'_{33} & \dots & a'_{3r} & \dots & a'_{3n} & b'_3 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & a'_{rr} & \dots & a'_{m} & b'_r \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & \dots & 0 & b'_m \end{pmatrix}.$$

В данной матрице A'_p все строки, находящиеся ниже строки с номером r, состоят из нулей (за исключением, быть может, последнего элемента b'_j). Это следует из того, что ранги матриц A и A' (получаемой из A'_p отбрасыванием последнего столбика) равны r, следовательно все строки матрицы A', начиная с $(r+1)$-й должны быть нулевыми.

Если (r+1)-я (или нижестоящая строчка) матрицы A'_p содержит ненулевой элемент b'_j, то система уравнений, соответствующая матрице A'_p (а значит и исходная) – будут несовместны по теореме Кронекера-Каппелли. Если же это не так, то оставляя базисные переменные в левой части уравнений, а свободные перенося в правую, мы выразим через них из последнего уравнения базисную переменную x'_r, затем из предпоследнего переменную x'_{r-1} и т.д., поднимаясь вверх до x'_1, выражая, таким образом, все базисные неизвестные через свободные. Придавая свободным переменным (в случае их существования) всевозможные значения, получаем множество решений системы (1).

Пример. Рассмотрим систему уравнений

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 4 \\ x_1 - x_2 + x_3 - x_4 = 0 \\ 3x_1 - x_2 + 3x_3 - x_4 = 4 \end{cases}$$

Тогда, производя указанные выше преобразования, получим

$$A_p = \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 1 & -1 & 1 & -1 & 0 \\ 3 & -1 & 3 & -1 & 4 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 0 & -2 & 0 & -2 & -4 \\ 0 & -4 & 0 & -4 & -8 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 0 & 2 & 0 & 2 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) = A'_p ,$$

следовательно, $rg(A)=rg(A_p)=2$. Полученная матрица A'_p соответствует системе уравнений

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 4 \\ x_2 + x_4 = 2 \end{cases},$$

которую, оставляя базисные неизвестные в правой части, перепишем в виде

$$\begin{cases} x_1 + x_2 = 4 - x_3 - x_4 \\ x_2 = 2 - x_4 \end{cases}$$

Тогда, подставляя найденное из второго уравнения выражение для переменной x_2 в первое уравнение, получим уравнение $x_1 + x_3 + 2 = 4$, таким образом, мы получаем систему

$$\begin{cases} x_1 = 2 - x_3 \\ x_2 = 2 - x_4 \end{cases},$$

где x_3 и x_4 – свободные переменные, которым мы можем придавать любые значения.

Следовательно столбцы вида $\begin{pmatrix} 2 - c_1 \\ 2 - c_2 \\ c_1 \\ c_2 \end{pmatrix}$, где произвольные постоянные $c_1, c_2 \in R$, образуют множество всех решений данной системы.

Пример. Рассмотрим систему уравнений

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 4 \\ x_1 - x_2 + x_3 - x_4 = 0 \\ 3x_1 - x_2 + 3x_3 - x_4 = 6 \end{cases}$$

Аналогичным образом, преобразуя расширенную матрицу данной системы, получим

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 1 & -1 & 1 & -1 & 0 \\ 3 & -1 & 3 & -1 & 6 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 0 & -2 & 0 & -2 & -4 \\ 0 & -4 & 0 & -4 & -6 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 4 \\ 0 & -2 & 0 & -2 & -4 \\ 0 & 0 & 0 & 0 & 2 \end{array}\right),$$

следовательно, ранг расширенной матрицы равен трем, а ранг матрицы системы равен двум. Таким образом, данная система является несовместной.

Рассмотрим уравнение $AX=B$, где A – квадратная невырожденная матрица, и умножение матрицы A на матрицу X определено, B – некоторая заданная матрица такая, что данное уравнение имеет смысл. Умножая обе части уравнения на матрицу A^{-1}, получим (в силу ассоциативности произведения) $\left(A^{-1}\cdot A\right)\cdot X = A^{-1}\cdot B$, следовательно, $E\cdot X = A^{-1}\cdot B$, и $X = A^{-1}\cdot B$. Аналогично для уравнения $X\cdot A = B$, $X\cdot\left(A\cdot A^{-1}\right) = B\cdot A^{-1}$, следовательно $X\cdot E = B\cdot A^{-1}$, и $X = B\cdot A^{-1}$.

Замечание. Отметим, что равенства $E\cdot X = X$, и $Y\cdot E = Y$ справедливы всегда, когда эти произведения определены, при этом матрицы X и Y не обязаны являться квадратными.

§11. Системы линейных однородных уравнений.

Рассмотрим систему (1) с правой частью, состоящей из нулей, обозначим ее $(1')$:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0 \end{cases} \qquad (1')$$

Такая система называется *системой линейных однородных уравнений*.

В матричной форме система $(1')$ может быть записана следующим образом: $A\cdot X = \overline{O}$, где A – матрица системы $(1')$, а $\overline{O}$ – нулевой столбик свободных членов.

Очевидно, что система $(1')$ всегда совместна, у неё существует тривиальное решение

$$\overline{O} = \begin{pmatrix} 0 \\ 0 \\ \ldots \\ 0 \end{pmatrix}.$$

На вопрос о существовании нетривиальных решений данной системы отвечает следующая теорема.

Теорема. *Система* $(1')$ *имеет нетривиальные решения тогда и только тогда, когда ранг матрицы системы меньше числа неизвестных (т.е.* $r < n$*).*

Доказательство. Если $n = r$, то из доказательства теоремы Кронекера-Капелли следует, что система $(1')$ имеет единственное решение (следовательно, тривиальное), откуда и следует, что если существует нетривиальное решение, то ранг r должен быть меньше n.

Обратно, пусть $r < n$, тогда, применяя метод Гаусса, мы получим $(n - r)$ свободных неизвестных и, следовательно, система имеет бесконечное множество решений. Теорема доказана.

Следствие. *Система однородных линейных уравнений, в которой число уравнений равно числу неизвестных, имеет нетривиальное решение тогда и только тогда, когда определитель матрицы данной системы будет равен нулю.*

Напомним, что линейной комбинацией столбиков $X_1 = \begin{pmatrix} x_1^{(1)} \\ x_2^{(1)} \\ \ldots \\ x_n^{(1)} \end{pmatrix}$ и $X_2 = \begin{pmatrix} x_1^{(2)} \\ x_2^{(2)} \\ \ldots \\ x_n^{(2)} \end{pmatrix}$ с коэффициентами α и β мы называем столбик, состоящий из элементов, которые являются линейной комбинацией соответствующих компонент данных столбцов:

$$\alpha X_1 + \beta X_2 = \begin{pmatrix} \alpha \cdot x_1^{(1)} + \beta \cdot x_1^{(2)} \\ \alpha \cdot x_2^{(1)} + \beta \cdot x_2^{(2)} \\ \cdots \\ \alpha \cdot x_n^{(1)} + \beta \cdot x_n^{(2)} \\ \end{pmatrix}.$$

Аналогично определяется линейная комбинация любой конечной системы столбиков одинаковой размерности. Напомним также, что система столбиков $X_1, X_2, \ldots, X_к$ (размерности n) будет называться линейно зависимой, если существует их нетривиальная нулевая линейная комбинация, т.е. когда найдется набор чисел $\alpha_1, \alpha_2, \ldots, \alpha_k$, где хотя бы одно $\alpha_i \neq 0$, такой, что $\alpha_1 X_1 + \alpha_2 X_2 + \ldots + \alpha_k X_k = \overline{O}$, и линейно независимой в противном случае.

Определение. Линейно независимая система столбцов $X_1, X_2, \ldots, X_k$ размерности n, состоящая из решений системы уравнений $(1')$, называется *фундаментальной системой решений* данной системы, если каждое решение системы $(1')$ можно представить в виде линейных комбинаций данной системы столбцов.

Теорема. *Пусть ранг r матрицы системы линейных однородных уравнений $(1')$ меньше числа неизвестных n. Тогда система $(1')$ обладает фундаментальной системой решений, состоящей из $(n - r)$ членов.*

Доказательство. Рассмотрим систему $(1')$. Пусть матрица данной системы имеет ранг r, предположим, что базисный минор матрицы этой системы расположен в верхнем левом углу (если это не так, то, как отмечалось ранее, мы можем добиться данного расположения базисного минора перестановкой местами строк и столбцов).

Тогда, после переноса в каждом уравнении свободных неизвестных в правую часть, получим систему:

$$\begin{cases} a'_{11} x_1 + \ldots + a'_{1r} x_r = -a'_{1r+1} x_{r+1} - \ldots - a'_{1n} x_n \\ a'_{21} x_1 + \ldots + a'_{2r} x_r = -a'_{2r+1} x_{r+1} - \ldots - a'_{2n} x_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a'_{r1} x_1 + \ldots + a'_{rr} x_r = -a'_{rr+1} x_{r+1} - \ldots - a'_{rn} x_n \end{cases},$$

являющуюся равносильной для системы $(1')$. Придавая свободным неизвестным определенные значения, построим фундаментальную систему решений данной (а значит, и исходной) системы.

1) Положим $\begin{cases} x_{r+1} = 1 \\ x_{r+2} = 0 \\ \ldots\ldots\ldots \\ x_n = 0 \end{cases}$, тогда получим решение X_1 системы $(1')$, соответствующее данному набору свободных неизвестных: $X_1 = \begin{pmatrix} x_1^{(1)} \\ x_2^{(1)} \\ \ldots \\ x_r^{(1)} \\ 1 \\ 0 \\ \ldots \\ 0 \end{pmatrix}$. Далее, полагая $\begin{cases} x_{r+1} = 0 \\ x_{r+2} = 1 \\ \ldots\ldots\ldots \\ \ldots\ldots\ldots \\ x_n = 0 \end{cases}$, получим

решение $X_2 = \begin{pmatrix} x_1^{(2)} \\ x_2^{(2)} \\ \dots \\ x_r^{(2)} \\ 0 \\ 1 \\ \dots \\ 0 \end{pmatrix}$, и т.д.,…, продолжая этот процесс передвижения единицы вниз на одну позицию, мы получим ($n - r$) решений системы $(1')$, где последнее решение $X_{n-r} = \begin{pmatrix} x_1^{(n-r)} \\ x_2^{(n-r)} \\ \dots \\ x_r^{(n-r)} \\ 0 \\ 0 \\ \dots \\ 1 \end{pmatrix}$.

Нетрудно увидеть, что полученная система столбцов $X_1, X_2, \dots, X_{n-r}$ является линейно независимой. Действительно, если $\alpha_1 X_1 + \alpha_2 X_2 + \dots + \alpha_{n-r} X_{n-r} = \overline{O}$, то отсюда следует, что $\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \dots \\ \alpha_{n-r} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}$ в силу покомпонентного равенства столбцов (начиная с (r + 1)-ой позиции), т.е. для всех $i = \overline{1, n-r}$ коэффициенты $\alpha_i = 0$. Таким образом, мы показали, что система $(1')$ обладает системой, состоящей из $(n-r)$ линейно независимых решений.

2) Покажем, что каждое решение системы $(1')$ можно представить в виде линейной комбинации столбиков найденной системы. Сначала отметим, что если $X_1, X_2, \dots, X_k$ – решения однородной системы $(1')$, то любая их линейная комбинация $\alpha_1 X_1 + \alpha_2 X_2 + \dots + \alpha_k X_k$ также является решением данной системы в силу выполнимости в таком случае равенства

$$A(\alpha_1 X_1 + \alpha_2 X_2 + \dots + \alpha_k X_k) = \alpha_1 (AX_1) + \alpha_2 (AX_2) + \dots + \alpha_k (AX_k) = \overline{O}.$$

Пусть теперь $X = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}$ – решение системы $(1')$. Тогда положим $X' = x_{r+1} \cdot X_1 + x_{r+2} \cdot X_2 + \dots + x_n \cdot X_{n-r}$, где коэффициенты x_i – компоненты решения X для всех $i = \overline{r+1, n}$, а $X_1, X_2, \dots, X_{n-r}$ – найденная выше линейно независимая система решений системы $(1')$.

Тогда, как было отмечено выше, X' является решением системы $(1')$. Но решения X и X' обладают одним и тем же набором свободных переменных, а, следовательно, они равны.

Теорема доказана.

Определение. *Общим решением системы* $(1')$ мы будем называть совокупность решений данной системы вида: $\overline{X} = \sum_{i=1}^{n-r} \alpha_i X_i$, где $X_1, X_2, ..., X_{n-r}$ – фундаментальная система решений системы $(1')$, а $\alpha_1, \alpha_2, ..., \alpha_{n-r}$ – произвольные числа.

Из последней теоремы следует, что каждое решение X системы $(1')$ будет получаться из общего решения $\overline{X}$ данной системы при некотором конкретном наборе значений $\alpha_1, \alpha_2, ..., \alpha_{n-r}$.

В заключении докажем теорему, которая позволяет описать все решения совместной системы линейных неоднородных уравнений.

Теорема. *Все решения совместной системы линейных неоднородных уравнений* (1), *при условии, что ранг матрицы системы меньше числа неизвестных, можно представить в виде* $X = \tilde{X} + \overline{X}$, *где* $\tilde{X}$ *– это некоторое (произвольным образом выбранное) «частное» решение системы* (1), *а* $\overline{X}$ *– общее решение однородной системы* $(1')$, *соответствующей системе* (1).

Доказательство. Пусть X – произвольное решение системы (1). Если $\tilde{X}$ – некоторое «частное» решение данной системы, то $(X - \tilde{X})$ будет являться решением системы $(1')$. Действительно, поскольку $AX = A\tilde{X} = B$, то $A(X - \tilde{X}) = AX - A\tilde{X} = B - B = \overline{O}$. Следовательно, если $X_1, X_2, ..., X_{n-r}$ – фундаментальная система решений однородной системы $(1')$, соответствующей системе (1), то найдутся такие коэффициенты $\alpha_1, \alpha_2, ..., \alpha_{n-r}$, что $X - \tilde{X} = \alpha_1 X_1 + \alpha_2 X_2 + ... + \alpha_{n-r} X_{n-r}$, и значит $X = \tilde{X} + \alpha_1 X_1 + \alpha_2 X_2 + ... + \alpha_{n-r} X_{n-r}$ для некоторого набора $\alpha_1, \alpha_2, ..., \alpha_{n-r}$. Таким образом мы показали, что каждое решении системы (1) представляется в указанном виде: $X = \tilde{X} + \overline{X}$. Верно и обратное утверждение, т.е. столбцы вида $\tilde{X} + \overline{X}$ при любых наборах коэффициентов $\alpha_1, \alpha_2, ..., \alpha_{n-r}$ линейных комбинаций будут являться решениями системы (1) в силу равенства: $A(\tilde{X} + \overline{X}) = A\tilde{X} + A\overline{X} = B + \overline{O} = B$.

Теорема доказана.