



Лекция 1

Внутренний закон композиции

Содержание лекции:

Предметом изучения в алгебре являются алгебраические структуры - множества наделенные законами композиции элементов. Начиная с понятия закона композиции и описания распространенных свойств некоторых элементов рассматриваемых множеств мы последовательно вводим основные (базовые) алгебраические структуры,

Ключевые слова:

Внутренний закон композиции, нейтральный элемент относительно закона композиции, регулярный элемент, обратимый элемент, поглощающий элемент, ассоциативность закона, коммутативность закона, теорема об ассоциативном коммутативном законе, основные структуры, магма, полугруппа, моноид, группа.

Авторы курса:

Трифанов А. И.

Москаленко М. А.

Ссылка на ресурсы:

mathdep.ifmo.ru/geolin

1.1 Внутренний закон композиции

Внутренним законом композиции на множестве M называется отображение $M \times M \rightarrow M$ декартова произведения $M \times M$ в M . Значение

$$(x, y) \mapsto z \in M$$

называется композицией элементов x и y относительно этого закона.

Пример 1.1. Пусть $\wp(M)$ - семейство всех подмножеств множества M . Тогда операции объединения и пересечения

$$(X, Y) \rightarrow X \cup Y, \quad (X, Y) \rightarrow X \cap Y,$$

являются законами композиции на $\wp(M)$.

Nota bene Для записи композиции элементов $x, y \in M$ чаще всего используют одно из следующих обозначений:

$$x + y, \quad x \cdot y, \quad x \circ y.$$

Также для удобства будем иногда использовать запись $x \top y$

Левым нейтральным элементом относительно закона композиции $x \circ y$ называется элемент e_L , такой что:

$$e_L \circ x = x, \quad \forall x \in M.$$

Правым нейтральным элементом называется элемент e_R со свойством:

$$x \circ e_R = x, \quad \forall x \in M.$$

Пример 1.2. Пустое множество и множество $\wp(M)$ являются примерами двусторонних нейтральных элементов относительно, соответственно, операций объединения и пересечения подмножеств:

$$X \cup \emptyset = X, \quad X \cap \wp(M) = X.$$

Лемма 1.1. Если относительно данного закона композиции существуют одновременно и левый e_L и правый e_R нейтральный элементы, то они совпадают и существует единственный нейтральный элемент e :

$$e_L = e_R \equiv e$$

ВНУТРЕННИЙ ЗАКОН КОМПОЗИЦИИ



По определению правого нейтрального элемента имеем:

$$e_L = e_L \circ e_R = e_R.$$



Элемент x называется **идемпотентом** относительно закона композиции, если

$$x \circ x = x$$

Nota bene Нейтральные элементы являются идемпотентами:

$$e_L = e_L \circ e_L.$$

Пример 1.3. Каждое подмножество $X \subset \wp(M)$ является идемпотентом относительно операций объединения и пересечения множеств:

$$X \cup X = X, \quad X \cap X = X.$$

Элемент y_L называется **левым регулярным** относительно закона композиции, определенном на множестве M , если для всех $x_1, x_2 \in M$ выполняется условие

$$y_L \circ x_1 = y_L \circ x_2 \Rightarrow x_1 = x_2.$$

Элемент y_R называется **правым регулярным**, если при аналогичных условиях

$$x_1 \circ y_R = x_2 \circ y_R \Rightarrow x_1 = x_2.$$

Nota bene Нейтральные элементы являются регулярными элементами:

$$x = e_L \circ x = e_L \circ y = y.$$

Пример 1.4. Пусть A - некоторый алфавит и S - множество строк, составленных из букв алфавита A . Множество S , наделенное операцией конкатенации строк является множеством, все элементы которого регулярные (слева и справа).

Элемент z_L называется **левым обратным** к элементу x относительно рассматриваемого закона композиции с нейтральным элементом e , если

$$z_L \circ x = e$$

Элемент z_R называется **правым обратным** к x если при тех же условиях

$$x \circ z_R = e$$

Пример 1.5. Во множестве $\wp(M)$ всех подмножеств множества M , наделенном операцией симметрической разности, каждый элемент является обратным к самому себе:

$$(X, Y) \rightarrow X \Delta Y = (X \setminus Y) \cup (Y \setminus X), \\ X \Delta X = \emptyset, \quad X \Delta \emptyset = X.$$

Элемент $\theta \in M$ называется **поглощающим элементом** относительно выбранного закона композиции, если

$$\forall x \in M \quad x \circ \theta = \theta \circ x = \theta.$$

1.2 Свойства законов композиции

Пусть $\{x_i\}_{i \in I}$ - конечное семейство элементов из M . **Композицией элементов** $\{x_i\}_{i \in I}$ относительно внутреннего закона \top называется элемент $x \in M$, определяемый индукцией по числу элементов следующим образом:

1. если $I = \{i_0\}$, тогда $\top_{i \in I} x_i = x_{i_0}$;
2. если $I = \{i_1, i_2, \dots\}$, тогда $\top_{i \in I} x_i = x_k \circ \left(\top_{i \in I'} x_i \right), \quad \forall i \in I' \quad i < k.$

Закон композиции элементов множества M называется **ассоциативным**, если для любых элементов $x, y, z \in M$ выполняется равенство:

$$(x \circ y) \circ z = x \circ (y \circ z)$$

Пример 1.6. Пример неассоциативного закона на $\mathbb{Z}[1/2]$:

$$x \oplus y = (x + y)/2.$$

Пример ассоциативного закона на \mathbb{Z} :

$$x \oplus y = \gcd(x, y).$$

Лемма 1.2. Если для данного элемента x существуют одновременно и левый z_L и правый z_R обратные элементы относительно ассоциативного закона композиции, то эти элементы совпадают и существует элемент $z = x^{-1}$, называемый обратным элементов к x :

$$z_L = z_R \equiv z = x^{-1}.$$



По определению нейтрального и правого обратного элементов имеем:

$$z_L = z_L \circ e = z_L \circ (x \circ z_R) = (z_L \circ x) \circ z_R = e \circ z_R = z_R.$$



Теорема 1.1. (об ассоциативном законе) Пусть $\{x_i\}_{i=1}^n$ - семейство элементов множества M с ассоциативным законом композиции \top , тогда для любого $p \in \mathbb{N}$, такого что $1 \leq p \leq n$ имеет место равенство

$$\top_{i=1}^n x_i = \left(\top_{i=1}^p x_i \right) \top \left(\top_{j=p+1}^n x_j \right).$$

Элементы $x, y \in M$ называются **перестановочными** относительно заданного закона композиции, если имеет место равенство:

$$x \circ y = y \circ x.$$

Если перестановочна любая пара элементов $x, y \in M$, тогда внутренний закон \circ называется **коммутативным**.

Теорема 1.2. (об ассоциативном коммутативном законе) Пусть $\{x_i\}_{i=1}^n$ - семейство элементов множества M с ассоциативным коммутативным законом композиции \top , тогда для любой перестановки σ имеет место равенство

$$\top_{i=1}^n x_i = \top_{i=1}^n x_{\sigma(i)}.$$

1.3 Определение основных структур

|| Множество, наделенное внутренним законом композиции, называется **магмой**.

Пример 1.7. Пусть множество M содержит только три элемента $\{-1, 0, 1\}$. Алгебраическую структуру магмы на S задает следующий закон композиции:

$$x \circ y = x \Leftrightarrow y = \begin{cases} 1, & x < y, \\ 0, & x = y, \\ -1, & x > y. \end{cases}$$

|| Множество M , наделенное **ассоциативным** всюду определенным законом композиции называется **полугруппой**.

Пример 1.8. Множество натуральных чисел \mathbb{N} с операцией $\circ = "+"$ является полугруппой $(\mathbb{N}, "+")$.

ВНУТРЕННИЙ ЗАКОН КОМПОЗИЦИИ

|| Полугруппа S , содержащая **нейтральный элемент**, называется **моноидом**.

Пример 1.9. Множество натуральных чисел \mathbb{N} с операцией $\circ = "$ \cdot $"$ является моноидом $(\mathbb{N}, 1, "$ \cdot $"$).

|| Говорят, что на множестве M определена структура **группы**, если закон композиции, заданный на M удовлетворяет следующим требованиям (аксиомам):

1. ассоциативность закона;
2. существование нейтрального элемента;
3. для каждого элемента существует обратный.

Пример 1.10. Множество целых чисел \mathbb{Z} , снабженное операцией сложения является коммутативной группой $(\mathbb{Z}, "+")$.



Лекция 2

Структура группы

Содержание лекции:

В настоящей лекции мы кратко рассмотрим основы теории групп, введем связанные объекты и понятия, которые будут необходимы в дальнейшем и в целом играют очень важную роль в приложениях. Лекция носит ознакомительный характер.

Ключевые слова:

Группа, коммутативная группа, гомоморфизм групп, изоморфизм, автоморфизм, ядро гомоморфизма, образ гомоморфизма, вложение, подгруппа, отношение эквивалентности, правый (левый) смежный класс, нормальная подгруппа, фактор-группа, канонический гомоморфизм, теорема об изоморфизме.

Авторы курса:

Трифанов А.И.

Ссылка на ресурсы:

mathdep.ifmo.ru/geolin

2.1 Определение. Примеры

Непустое множество G называется **группой**, если на нем задан закон композиции $G \times G \rightarrow G$, так что $(x, y) \mapsto xy$ и имеют место следующие три свойства:

G1. Ассоциативность закона:

$$\forall x, y, z \in G \quad (xy)z = x(yz).$$

G2. Существует нейтральный элемент:

$$\exists e \in G : \quad \forall x \in G \quad xe = x = ex.$$

G3. Существует обратный элемент:

$$\forall x \in G \quad \exists x^{-1} : \quad xx^{-1} = e = x^{-1}x.$$

Пример 2.1. На практике группы чаще всего встречаются в виде *групп преобразований* каких-то объектов:

- группа D_3 симметрий правильного треугольника;
- симметрическая группа S_n перестановок;
- группа Рубика - группа внутренних вращений кубика Рубика;

Коммутативной или **абелевой** называется такая группа, любые два элемента которой *коммутируют*:

$$\forall x, y \in G \quad xy = yx.$$

Пример 2.2. Примеры коммутативных групп:

1. Аддитивная группа целых чисел \mathbb{Z}^+ ;
2. Мультипликативная группа вещественных чисел $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$;
3. Группа углов (точек единичной окружности) - группа вещественных чисел \mathbb{R}^+ по модулю $2\pi\mathbb{Z}$. Групповая операция \oplus определяется следующим образом:

$$\begin{cases} x \oplus y = x + y, & x + y < 2\pi \\ x \oplus y = x + y - 2\pi, & x + y \geq 2\pi \end{cases}$$

4. Булева группа множества X - множество 2^X всех подмножеств множества X вместе с операцией симметрической разности Δ ;
5. Группа размерностей физических величин;

2.2 Гомоморфизмы групп

Гомоморфизмом групп G и G' называется отображение $\sigma : G \rightarrow G'$, обладающее следующими свойствами:

$$\forall x, y \in G \quad \sigma(xy) = \sigma(x)\sigma(y), \quad \sigma(e) = e'.$$

Nota bene Множество гомоморфизмов из группы G в группу G' принято обозначать $\text{Hom}(G, G')$. Гомоморфизмы из G в G называются эндоморфизмами и их множество обозначается $\text{End}(G) \triangleq \text{Hom}(G, G)$.

Лемма 2.1. Пусть $\sigma \in \text{Hom}(G, G')$, тогда

$$\forall x \in G \quad \sigma(x^{-1}) = \sigma(x)^{-1}.$$

Гомоморфизм σ называется **изоморфизмом**, если

$$\exists \chi \in \text{Hom}(G', G) : \quad \chi \circ \sigma = \text{id}_G, \quad \sigma \circ \chi = \text{id}_{G'}.$$

Nota bene Подмножество отображений в $\text{Hom}(G, G')$, являющихся изоморфизмами, принято обозначать $\text{Iso}(G, G')$. В случае $\text{Iso}(G, G)$ обычно пишут $\text{Aut}(G)$ и соответствующие отображения называют **автоморфизмами**.

Пример 2.3. Множество $\text{Aut}(G)$ вместе с операцией композиции и тождественным отображением id_G является группой (автоморфизмов группы G).

Ядром гомоморфизма $\sigma \in \text{Hom}(G, G')$ называется множество

$$\ker \sigma = \{g \in G : \sigma(g) = e'\}.$$

Лемма 2.2. Ядро $\ker \sigma$ является группой.

Лемма 2.3. Гомоморфизм $\sigma \in \text{Hom}(G, G')$ ядро которого тривиально инъективен.

Образом гомоморфизма $\sigma \in \text{Hom}(G, G')$ называется подмножество G' , такое что

$$\text{Im } \sigma = \{g' \in G' : \exists g \in G, \quad \sigma(g) = g'\}.$$

Лемма 2.4. Образ $\text{Im } \sigma$ является группой.

Вложением называется гомоморфизм $\sigma \in \text{Hom}(G, G')$, обладающий следующим свойством

$$G \simeq \text{Im } \sigma \subset G'.$$

2.3 Подгруппы

|| Подгруппой H группы G называется подмножество G , имеющее структуру группы, индуцированной групповым законом G .

Nota bene Подгруппа $\{e\}$ называется *тривиальной подгруппой*, G как подгруппа самой себя называется *несобственной*, остальные подгруппы G называются *собственными подгруппами*.

Пример 2.4. Пусть $\sigma \in \text{hom}(G, G')$, тогда $\ker \sigma \leq G$ и $\text{Im } \sigma \leq G'$.

Nota bene Напомним, что отношением эквивалентности на произвольном множестве называется отношение, удовлетворяющее свойствам:

- рефлексивность: $\forall x \in M \quad x \sim x$;
- симметричность: $\forall x, y \in M \quad x \sim y \Rightarrow y \sim x$;
- транзитивность: $\forall x, y, z \in M \quad x \sim y, \quad y \sim z \Rightarrow x \sim z$.

Отношение эквивалентности разбивает множество M на непересекающиеся подмножества (классы эквивалентности). Множество классов эквивалентности по заданному отношению, называется фактор-множеством множества M по отношению \sim и обозначается M/\sim .

Лемма 2.5. Пусть G - группа и $H \leq G$. Тогда отношением эквивалентности является

$$x \sim y \Rightarrow xy^{-1} \in H.$$

►

Проверим свойства:

- $x \sim x : \quad xx^{-1} = e \in H$;
- $x \sim y \Rightarrow xy^{-1} = (yx^{-1})^{-1} \in H \Rightarrow yx^{-1} \in H \Rightarrow y \sim x$.
- $x \sim y, \quad y \sim z \Rightarrow xy^{-1}, yz^{-1} \in H \Rightarrow xy^{-1}yz^{-1} = xz^{-1} \in H \Rightarrow x \sim z$.

◀

Nota bene Из того, что $xy^{-1} \in H$ получаем

$$x \in Hy = \{hy : h \in H\} \Rightarrow \exists h_x \in H : h_x y = x.$$

|| Множество Hy называется **правым смежным классом** G по подгруппе H .

Лемма 2.6. Смежные классы, Hx и Hu , имеющие хотя бы один общий элемент, совпадают.



Пусть $z \in Hx$ и $z \in Hu$, тогда существуют $u, v \in H$, такие что $z = ux = vy$ и мы имеем:

$$ux = vy \Rightarrow x = u^{-1} \cdot v \cdot y, \quad u^{-1}v \in H$$

и тогда

$$Hx = Hu^{-1}vy = Hy.$$



Nota bene Смежные классы, соответствующие различным элементам $x \in G$ не пересекаются.

Nota bene Так как существует только один правый смежный класс, которому принадлежит элемент $x \in G$ целесообразно выбрать данный элемент представителем этого класса и записывать $[x]_R$. В зависимости от ситуации мы будем использовать как мультипликативную, так и аддитивную (для абелевых групп) форму записи для правых смежных классов:

$$[x]_R = Hx, \quad [x]_R = H + x.$$

Nota bene Аналогично правым смежным классам, могут быть определены **левые смежные классы** группы G по подгруппе H :

$$[x]_L = xH, \quad [x]_L = x + H.$$

|| Подгруппа H группы G называется **нормальной**, если

$$\forall x \in G \quad xH = Hx.$$

Nota bene Если H - нормальная подгруппа в G , то обычно пишут $H \triangleleft G$.

Nota bene Нормальной является любая подгруппа абелевой группы.

Nota bene В случае нормальной подгруппы имеем

$$\forall x \in G \quad [x]_R = [x]_L = \bar{x}.$$

Лемма 2.7. Пусть $\sigma \in \text{hom}(G, G')$, тогда $\ker \sigma \triangleleft G$.



Пусть $H = \ker \sigma$, тогда

$$e' = \sigma(x \cdot x^{-1}) = \sigma(x)\sigma(H)\sigma(x^{-1}) = \sigma(x \cdot H \cdot x^{-1}) \Rightarrow x \cdot H \cdot x^{-1} \subset H.$$

Замена $x \leftrightarrow x^{-1}$ дает

$$H \subset x \cdot H \cdot x^{-1} \Rightarrow H = x \cdot H \cdot x^{-1}$$



Лемма 2.8. Пусть $H \triangleleft G$, тогда G/H имеет структуру группы.



Для доказательства достаточно проверить групповые аксиомы:

1. Пусть $\bar{x}, \bar{y}, \bar{z} \in G/H$, тогда $(\bar{x}\bar{y})\bar{z} = \bar{x}(\bar{y}\bar{z})$:

$$(\bar{x}\bar{y})\bar{z} = (xH \cdot yH) \cdot zH = (xy)H \cdot zH = (xy)zH = x(yz)H = \bar{x}(\bar{y}\bar{z}).$$

2. H - нейтральный элемент G/H :

$$xH \cdot H = xH.$$

3. $x^{-1}H$ - обратный элемент к xH :

$$x^{-1}H \cdot xH = x^{-1}xH = eH = H.$$



|| Группа G/H называется **фактор-группой** группы G по нормальной подгруппе H

Теорема 2.1. Пусть $H \triangleleft G$, тогда существует такой гомоморфизм φ (называемый каноническим), что $\ker \varphi = H$.



Рассмотрим отображение

$$\varphi : G \rightarrow G/H, \quad \varphi(x) = xH,$$

и прямой проверкой убеждаемся, что

$$\varphi \in \text{hom}(G, G/H), \quad \ker \varphi = H.$$



Теорема 2.2. (Об изоморфизме) Пусть $\sigma : G \rightarrow G'$ - гомоморфизм групп, тогда

$$G/\ker \sigma \simeq \text{Im } \sigma.$$



Зададим отображение $\bar{\sigma} : G/\ker \sigma \rightarrow \text{Im } \sigma$

$$\bar{\sigma}(\bar{x}) = \sigma(x),$$

и покажем, что оно определено корректно. Именно, пусть $\bar{x} = \bar{y}$, тогда

$$\bar{\sigma}(\bar{y}) = \sigma(y) = \sigma(xx^{-1}y) = \sigma(x)\sigma(x^{-1}y) = \sigma(x)e = \sigma(x) = \bar{\sigma}(\bar{x}).$$

Далее, $\bar{\sigma}$ - гомоморфизм:

$$\bar{\sigma}(\bar{x}\bar{y}) = \sigma(xy) = \sigma(x)\sigma(y) = \bar{\sigma}(\bar{x})\bar{\sigma}(\bar{y}).$$

Тривиально проверяется, что $\text{Im } \bar{\sigma} = \text{Im } \sigma$, и остается прямой проверкой убедиться, что ядро $\bar{\sigma}$ тривиально:

$$\bar{z} \in \ker \bar{\sigma} \Rightarrow \sigma(z) = \bar{\sigma}(\bar{z}) = e \Rightarrow z \in \ker \sigma \Rightarrow \bar{z} = \bar{e}.$$

Таким образом, мы показали, что $\bar{\sigma}$ - изоморфизм.





Лекция 2

Структура группы

Содержание лекции:

В настоящей лекции мы кратко рассмотрим основы теории групп, введем связанные объекты и понятия, которые будут необходимы в дальнейшем и в целом играют очень важную роль в приложениях. Лекция носит ознакомительный характер.

Ключевые слова:

Группа, коммутативная группа, гомоморфизм групп, изоморфизм, автоморфизм, ядро гомоморфизма, образ гомоморфизма, вложение, подгруппа, отношение эквивалентности, правый (левый) смежный класс, нормальная подгруппа, фактор-группа, канонический гомоморфизм, теорема об изоморфизме.

Авторы курса:

Трифанов А.И.

Ссылка на ресурсы:

mathdep.ifmo.ru/geolin

2.1 Определение. Примеры

Непустое множество G называется **группой**, если на нем задан закон композиции $G \times G \rightarrow G$, так что $(x, y) \mapsto xy$ и имеют место следующие три свойства:

G1. Ассоциативность закона:

$$\forall x, y, z \in G \quad (xy)z = x(yz).$$

G2. Существует нейтральный элемент:

$$\exists e \in G : \quad \forall x \in G \quad xe = x = ex.$$

G3. Существует обратный элемент:

$$\forall x \in G \quad \exists x^{-1} : \quad xx^{-1} = e = x^{-1}x.$$

Пример 2.1. На практике группы чаще всего встречаются в виде *групп преобразований* каких-то объектов:

- группа D_3 симметрий правильного треугольника;
- симметрическая группа S_n перестановок;
- группа Рубика - группа внутренних вращений кубика Рубика;

Коммутативной или **абелевой** называется такая группа, любые два элемента которой *коммутируют*:

$$\forall x, y \in G \quad xy = yx.$$

Пример 2.2. Примеры коммутативных групп:

1. Аддитивная группа целых чисел \mathbb{Z}^+ ;
2. Мультипликативная группа вещественных чисел $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$;
3. Группа углов (точек единичной окружности) - группа вещественных чисел \mathbb{R}^+ по модулю $2\pi\mathbb{Z}$. Групповая операция \oplus определяется следующим образом:

$$\begin{cases} x \oplus y = x + y, & x + y < 2\pi \\ x \oplus y = x + y - 2\pi, & x + y \geq 2\pi \end{cases}$$

4. Булева группа множества X - множество 2^X всех подмножеств множества X вместе с операцией симметрической разности Δ ;
5. Группа размерностей физических величин;

2.2 Гомоморфизмы групп

Гомоморфизмом групп G и G' называется отображение $\sigma : G \rightarrow G'$, обладающее следующими свойствами:

$$\forall x, y \in G \quad \sigma(xy) = \sigma(x)\sigma(y), \quad \sigma(e) = e'.$$

Nota bene Множество гомоморфизмов из группы G в группу G' принято обозначать $\text{Hom}(G, G')$. Гомоморфизмы из G в G называются эндоморфизмами и их множество обозначается $\text{End}(G) \triangleq \text{Hom}(G, G)$.

Лемма 2.1. Пусть $\sigma \in \text{Hom}(G, G')$, тогда

$$\forall x \in G \quad \sigma(x^{-1}) = \sigma(x)^{-1}.$$

Гомоморфизм σ называется **изоморфизмом**, если

$$\exists \chi \in \text{Hom}(G', G) : \quad \chi \circ \sigma = \text{id}_G, \quad \sigma \circ \chi = \text{id}_{G'}.$$

Nota bene Подмножество отображений в $\text{Hom}(G, G')$, являющихся изоморфизмами, принято обозначать $\text{Iso}(G, G')$. В случае $\text{Iso}(G, G)$ обычно пишут $\text{Aut}(G)$ и соответствующие отображения называют **автоморфизмами**.

Пример 2.3. Множество $\text{Aut}(G)$ вместе с операцией композиции и тождественным отображением id_G является группой (автоморфизмов группы G).

Ядром гомоморфизма $\sigma \in \text{Hom}(G, G')$ называется множество

$$\ker \sigma = \{g \in G : \sigma(g) = e'\}.$$

Лемма 2.2. Ядро $\ker \sigma$ является группой.

Лемма 2.3. Гомоморфизм $\sigma \in \text{Hom}(G, G')$ ядро которого тривиально инъективен.

Образом гомоморфизма $\sigma \in \text{Hom}(G, G')$ называется подмножество G' , такое что

$$\text{Im } \sigma = \{g' \in G' : \exists g \in G, \quad \sigma(g) = g'\}.$$

Лемма 2.4. Образ $\text{Im } \sigma$ является группой.

Вложением называется гомоморфизм $\sigma \in \text{Hom}(G, G')$, обладающий следующим свойством

$$G \simeq \text{Im } \sigma \subset G'.$$

2.3 Подгруппы

|| Подгруппой H группы G называется подмножество G , имеющее структуру группы, индуцированной групповым законом G .

Nota bene Подгруппа $\{e\}$ называется *тривиальной подгруппой*, G как подгруппа самой себя называется *несобственной*, остальные подгруппы G называются *собственными подгруппами*.

Пример 2.4. Пусть $\sigma \in \text{hom}(G, G')$, тогда $\ker \sigma \leq G$ и $\text{Im } \sigma \leq G'$.

Nota bene Напомним, что отношением эквивалентности на произвольном множестве называется отношение, удовлетворяющее свойствам:

- рефлексивность: $\forall x \in M \quad x \sim x$;
- симметричность: $\forall x, y \in M \quad x \sim y \Rightarrow y \sim x$;
- транзитивность: $\forall x, y, z \in M \quad x \sim y, \quad y \sim z \Rightarrow x \sim z$.

Отношение эквивалентности разбивает множество M на непересекающиеся подмножества (классы эквивалентности). Множество классов эквивалентности по заданному отношению, называется фактор-множеством множества M по отношению \sim и обозначается M/\sim .

Лемма 2.5. Пусть G - группа и $H \leq G$. Тогда отношением эквивалентности является

$$x \sim y \Rightarrow xy^{-1} \in H.$$

►

Проверим свойства:

- $x \sim x : \quad xx^{-1} = e \in H$;
- $x \sim y \Rightarrow xy^{-1} = (yx^{-1})^{-1} \in H \Rightarrow yx^{-1} \in H \Rightarrow y \sim x$.
- $x \sim y, \quad y \sim z \Rightarrow xy^{-1}, yz^{-1} \in H \Rightarrow xy^{-1}yz^{-1} = xz^{-1} \in H \Rightarrow x \sim z$.

◀

Nota bene Из того, что $xy^{-1} \in H$ получаем

$$x \in Hy = \{hy : h \in H\} \Rightarrow \exists h_x \in H : h_x y = x.$$

|| Множество Hy называется **правым смежным классом** G по подгруппе H .

Лемма 2.6. Смежные классы, Hx и Hu , имеющие хотя бы один общий элемент, совпадают.



Пусть $z \in Hx$ и $z \in Hu$, тогда существуют $u, v \in H$, такие что $z = ux = vy$ и мы имеем:

$$ux = vy \Rightarrow x = u^{-1} \cdot v \cdot y, \quad u^{-1}v \in H$$

и тогда

$$Hx = Hu^{-1}vy = Hy.$$



Nota bene Смежные классы, соответствующие различным элементам $x \in G$ не пересекаются.

Nota bene Так как существует только один правый смежный класс, которому принадлежит элемент $x \in G$ целесообразно выбрать данный элемент представителем этого класса и записывать $[x]_R$. В зависимости от ситуации мы будем использовать как мультипликативную, так и аддитивную (для абелевых групп) форму записи для правых смежных классов:

$$[x]_R = Hx, \quad [x]_R = H + x.$$

Nota bene Аналогично правым смежным классам, могут быть определены **левые смежные классы** группы G по подгруппе H :

$$[x]_L = xH, \quad [x]_L = x + H.$$

|| Подгруппа H группы G называется **нормальной**, если

$$\forall x \in G \quad xH = Hx.$$

Nota bene Если H - нормальная подгруппа в G , то обычно пишут $H \triangleleft G$.

Nota bene Нормальной является любая подгруппа абелевой группы.

Nota bene В случае нормальной подгруппы имеем

$$\forall x \in G \quad [x]_R = [x]_L = \bar{x}.$$

Лемма 2.7. Пусть $\sigma \in \text{hom}(G, G')$, тогда $\ker \sigma \triangleleft G$.



Пусть $H = \ker \sigma$, тогда

$$e' = \sigma(x \cdot x^{-1}) = \sigma(x)\sigma(H)\sigma(x^{-1}) = \sigma(x \cdot H \cdot x^{-1}) \Rightarrow x \cdot H \cdot x^{-1} \subset H.$$

Замена $x \leftrightarrow x^{-1}$ дает

$$H \subset x \cdot H \cdot x^{-1} \Rightarrow H = x \cdot H \cdot x^{-1}$$



Лемма 2.8. Пусть $H \triangleleft G$, тогда G/H имеет структуру группы.



Для доказательства достаточно проверить групповые аксиомы:

1. Пусть $\bar{x}, \bar{y}, \bar{z} \in G/H$, тогда $(\bar{x}\bar{y})\bar{z} = \bar{x}(\bar{y}\bar{z})$:

$$(\bar{x}\bar{y})\bar{z} = (xH \cdot yH) \cdot zH = (xy)H \cdot zH = (xy)zH = x(yz)H = \bar{x}(\bar{y}\bar{z}).$$

2. H - нейтральный элемент G/H :

$$xH \cdot H = xH.$$

3. $x^{-1}H$ - обратный элемент к xH :

$$x^{-1}H \cdot xH = x^{-1}xH = eH = H.$$



|| Группа G/H называется **фактор-группой** группы G по нормальной подгруппе H

Теорема 2.1. Пусть $H \triangleleft G$, тогда существует такой гомоморфизм φ (называемый каноническим), что $\ker \varphi = H$.



Рассмотрим отображение

$$\varphi : G \rightarrow G/H, \quad \varphi(x) = xH,$$

и прямой проверкой убеждаемся, что

$$\varphi \in \text{hom}(G, G/H), \quad \ker \varphi = H.$$



Теорема 2.2. (Об изоморфизме) Пусть $\sigma : G \rightarrow G'$ - гомоморфизм групп, тогда

$$G/\ker \sigma \simeq \text{Im } \sigma.$$



Зададим отображение $\bar{\sigma} : G/\ker \sigma \rightarrow \text{Im } \sigma$

$$\bar{\sigma}(\bar{x}) = \sigma(x),$$

и покажем, что оно определено корректно. Именно, пусть $\bar{x} = \bar{y}$, тогда

$$\bar{\sigma}(\bar{y}) = \sigma(y) = \sigma(xx^{-1}y) = \sigma(x)\sigma(x^{-1}y) = \sigma(x)e = \sigma(x) = \bar{\sigma}(\bar{x}).$$

Далее, $\bar{\sigma}$ - гомоморфизм:

$$\bar{\sigma}(\bar{x}\bar{y}) = \sigma(xy) = \sigma(x)\sigma(y) = \bar{\sigma}(\bar{x})\bar{\sigma}(\bar{y}).$$

Тривиально проверяется, что $\text{Im } \bar{\sigma} = \text{Im } \sigma$, и остается прямой проверкой убедиться, что ядро $\bar{\sigma}$ тривиально:

$$\bar{z} \in \ker \bar{\sigma} \Rightarrow \sigma(z) = \bar{\sigma}(\bar{z}) = e \Rightarrow z \in \ker \sigma \Rightarrow \bar{z} = \bar{e}.$$

Таким образом, мы показали, что $\bar{\sigma}$ - изоморфизм.





Лекция 3

Структура коммутативного кольца

Содержание лекции:

Алгебраическая структура кольца по своей важности и фундаментальности не уступает структуре группы. В этой лекции мы опишем данную структуру и дадим определения связанным с ней объектам. Лекция является ознакомительной, но понятия вводимые в ней окажутся крайне полезными в дальнейшем.

Ключевые слова:

Согласование законов, дистрибутивность, кольцо, гомоморфизм колец, подкольцо, идеал кольца, фактор-кольцо, канонический кольцевой гомоморфизм, класс вычетов, делитель нуля, область целостности, нильпотент, обратимый элемент, главный идеал, поле.

Авторы курса:

Трифанов А.И.

Москаленко М.А.

Ссылка на ресурсы:

mathdep.ifmo.ru/geolin

3.1 Согласование внутренних законов

Пусть на множестве M задано два всюду определенных закона композиции, обозначаемых через \circ и $*$. Закон композиции \circ называется **дистрибутивным слева** относительно закона $*$, если для любых элементов $x, y, z \in M$ имеет место равенство

$$x \circ (y * z) = (x \circ y) * (x \circ z).$$

Соответственно, **дистрибутивность справа** означает выполнение следующего равенства:

$$\forall x, y, z \in M \quad (y * z) \circ x = (y \circ x) * (z \circ x).$$

Закон, дистрибутивный и справа и слева называется **двояко дистрибутивным**.

Пример 3.1. Пусть на множестве M задано два всюду определенных закона композиции, обозначаемых через \circ и $*$, причем \circ наделяет M структурой группы. Если в M существует *нейтральный элемент* e относительно $*$ и \circ двояко дистрибутивен относительно $*$, тогда элемент e является *поглощающим* относительно закона \circ . Действительно, пусть $x, y \in M$, рассмотрим композицию

$$x \circ y = x \circ (e * y) = (x \circ e) * (x \circ y) = e * (x \circ y).$$

Вообще говоря, из выведенного равенства не следует, что $(x \circ e) = e$, так как не доказано свойство всеобщности - мы показали лишь, что это верно для подмножества M_z композиций вида $z = x \circ y$. Чтобы $M_z = M$ достаточно потребовать существования групповой структуры на M относительно закона \circ .

3.2 Кольца и гомоморфизмы колец

Nota bene На протяжении всего раздела под кольцом R мы будем понимать ассоциативное и коммутативное кольцо с единицей.

Кольцом R называется множество замкнутое относительно двух согласованно заданных на нем бинарных операций, удовлетворяющих следующим аксиомам:

A1. Ассоциативность сложения:

$$\forall x, y, z \in R \quad (x + y) + z = x + (y + z);$$

A2. Существование нуля:

$$\exists 0 \in R : \quad x + 0 = x = 0 + x \quad \forall x \in R$$

A3. Существование противоположного:

$$\forall x \in R \quad \exists (-x) : \quad x + (-x) = 0 = (-x) + x.$$

M1. Ассоциативность умножения:

$$\forall x, y, z \in R \quad (xy)z = x(yz);$$

M2. Существование единицы:

$$\exists 1 \in R : \quad 1 \cdot x = x = x \cdot 1, \quad \forall x \in R;$$

M3. Коммутативность:

$$\forall x, y \in R \quad x \cdot y = y \cdot x;$$

D1. Дистрибутивность слева:

$$\forall x, y, z \in R \quad x \cdot (y + z) = xy + xz;$$

D2. Дистрибутивность справа:

$$\forall x, y, z \in R \quad (x + y) \cdot z = xz + yz;$$

Пример 3.2. Примеры колец:

1. Нулевое кольцо:

$$R : \quad 0 = 1 \quad \Rightarrow \quad \forall x \in R \quad x = 1 \cdot x = 0 \cdot x = 0;$$

2. Целые числа:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots, \pm m, \dots\};$$

3. Кольцо доичных дробей:

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{ \frac{m}{2^n} : m \neq 2 \cdot k, \quad k \in \mathbb{Z} \right\}$$

4. Пифагорово кольцо:

$$\mathbb{Z}[\sqrt{2}] = \left\{ x + \sqrt{2}y : x, y \in \mathbb{Z} \right\} \quad (3.1)$$

5. Гауссово кольцо:

$$\mathbb{Z}[i] = \left\{ x + iy : x, y \in \mathbb{Z}, \quad i^2 = -1 \right\};$$

6. Кольцо многочленов над \mathbb{Z} от одного или нескольких параметров:

$$\mathbb{Z}[x] = \left\{ \sum a_j x^j : a_j \in \mathbb{Z} \right\}, \quad \mathbb{Z}[x_1, x_2, \dots, x_n] = \left\{ \sum a_{j_1, j_2, \dots, j_n} x_1^{j_1} x_2^{j_2} \dots x_n^{j_n} \right\}$$

7. Кольцо матриц - пример некоммутативного кольца.

Пусть A и B - кольца. **Гомоморфизмом колец** называется отображение $f : A \rightarrow B$, со следующими свойствами:

- сохранение сложения:

$$\forall x, y \in R \quad f(x + y) = f(x) + f(y);$$

- сохранение умножения:

$$\forall x, y \in R \quad f(xy) = f(x) \cdot f(y);$$

- сохранение единицы:

$$f(1_A) = 1_B.$$

Подмножество $S \subset R$ называется **подкольцом** кольца R , если оно является абелевой подгруппой R и содержит единицу R .

Nota bene Вложение - кольцевой гомоморфизм:

$$S < R \quad \Rightarrow \quad S \hookrightarrow R;$$

Лемма 3.1. Пусть A, B, C - кольца и

$$f : A \rightarrow B, \quad g : B \rightarrow C,$$

- кольцевые гомоморфизмы, тогда $g \circ f : A \rightarrow C$ - кольцевой гомоморфизм.

3.3 Идеалы и фактор-кольца

Идеалом J в кольце R называется аддитивная подгруппа со свойством

$$RJ \subset J \quad (\forall x \in R, \quad \forall y \in J \quad xy \in J).$$

Пример 3.3. Найдем идеалы в кольце \mathbb{Z} . Пусть m - наименьшее положительное число, лежащее в идеале $J \triangleleft \mathbb{Z}$. Тогда $(m) = m \cdot \mathbb{Z}$. Других идеалов в кольце \mathbb{Z} содержащих элемент m нет. Действительно, пусть

$$z \in J = m \cdot \mathbb{Z} \Rightarrow z = m \cdot u + r, \quad r \in J, \quad r < m \Rightarrow r = \min(J).$$

Лемма 3.2. Пусть $J \triangleleft R$, тогда следующее отношение является отношением эквивалентности на R :

$$x \sim y \Leftrightarrow x - y \in J.$$

►

Утверждение следует из прямой проверки свойств:

$$R. \quad x - x = 0 \in J \Rightarrow x \sim x;$$

$$S. \quad x \sim y \Rightarrow x - y \in J \Rightarrow y - x = -(x - y) \in J \Rightarrow x \sim y;$$

$$T. \quad x \sim y, \quad y \sim z \Rightarrow x - z = (x - y) + (y - z) \in J \Rightarrow x \sim z.$$

◄

Nota bene Фактор-множество R/J состоит из классов эквивалентности вида

$$\bar{x} = x + J.$$

Лемма 3.3. Фактор-множество R/J , наделенное операциями, индуцированными из R имеет структуру кольца:

$$\bar{x} + \bar{y} = \overline{x + y}, \quad \bar{x} \cdot \bar{y} = \overline{x \cdot y}, \quad \bar{0} = J.$$

►

Проверяем непосредственно свойства операций:

$$1. \quad \bar{x} + \bar{y} = (x + J) + (y + J) = (x + y) + J = \overline{x + y},$$

$$2. \quad \bar{x} \cdot \bar{y} = (x + J) \cdot (y + J) = xy + J = \overline{xy},$$

$$3. \quad \bar{0} \cdot \bar{x} = J \cdot (x + J) = J = \bar{0}.$$

◄

СТРУКТУРА КОММУТАТИВНОГО КОЛЬЦА

Множество R/J называется **фактор-кольцом** кольца R по идеалу J . Отображение $\varphi : R \rightarrow R/J$, действующее как

$$x \mapsto \bar{x} = x + J,$$

является гомоморфизмом, который называется **каноническим**.

Пример 3.4. Элементами фактор-кольца $\mathbb{Z}/(m) \triangleq \mathbb{Z}/m\mathbb{Z}$ являются *классы вычетов по модулю m* :

$$\begin{aligned}\bar{0} &= \{x \in \mathbb{Z} : x = 0 \pmod{m}\}, \\ \bar{1} &= \{x \in \mathbb{Z} : x = 1 \pmod{m}\}, \\ &\dots\dots\dots \\ \overline{m-1} &= \{x \in \mathbb{Z} : x = (m-1) \pmod{m}\}.\end{aligned}$$

Лемма 3.4. Пусть $f : A \rightarrow B$ - гомоморфизм колец, тогда

$$\begin{aligned}\ker f &\trianglelefteq A, \quad \operatorname{Im} f \leq B \\ A/\ker f &\simeq \operatorname{Im} f.\end{aligned}$$



Покажем, что $\ker f$ - идеал в кольце A :

$$x \in \ker f \Rightarrow f(x) = 0 \Rightarrow \forall y \in A \quad f(xy) = f(x)f(y) = 0 \Rightarrow xy \in \ker f.$$

То, что $\operatorname{Im} f$ - подкольцо в B следует из определения кольцевого гомоморфизма. Последнее утверждение следует из биективности и линейности отображения:

$$(x + \ker f) \mapsto f(x).$$



3.4 Делители нуля. Нильпотенты

Делителем нуля в кольце R называется всякий элемент $x \neq 0$, такой что

$$\exists y \neq 0 : xy = 0.$$

Пример 3.5. В кольце $\mathbb{Z}/6\mathbb{Z}$ делителями нуля являются элементы $\bar{2}$ и $\bar{3}$.

Областью целостности называется кольцо, в котором нет делителей нуля.

Пример 3.6. Областями целостности являются кольца \mathbb{Z} и $\mathbb{Z}/p\mathbb{Z}$, где p - простое.

|| Элемент $z \neq 0$ называется **нильпотентом**, если

$$\exists n \in \mathbb{N} : z^n = 0.$$

Nota bene Всякий нильпотент является делителем нуля. Обратное верно не всегда.

3.5 Обратимые элементы. Поле

|| **Обратимым элементом** кольца называется всякий элемент $u \in R$ такой что

$$\exists v \in R \quad u \cdot v = 1$$

Nota bene В паре u, v оба элемента являются обратимыми.

Лемма 3.5. Множество обратимых элементов кольца R образует мультипликативную группу, обозначаемую R^* .

|| Идеал вида $(x) = x \cdot R, x \in R$ называется **главным идеалом** кольца R .

Лемма 3.6. Имеет место эквивалентность:

$$x \in R^* \Leftrightarrow (x) = (1) \triangleq R.$$

|| **Поле** называется ненулевое кольцо, в котором каждый ненулевой элемент обратим.

Лемма 3.7. Всякое поле K является областью целостности.



Пусть $x, y \in K$ такие что $xy = 0$. По определению K имеем

$$\exists u, v : ux = 1, \quad yv = 1.$$

Откуда сразу получаем:

$$1 = (ux) \cdot (yv) = u \cdot (xy) \cdot v = 0.$$



Nota bene Обратное, вообще говоря не верно: \mathbb{Z} - область целостности, но не поле.

СТРУКТУРА КОММУТАТИВНОГО КОЛЬЦА

Теорема 3.1. Пусть R - ненулевое кольцо, тогда следующие утверждения равносильны:

- (1) R - поле;
- (2) в R нет идеалов, кроме (0) и (1) ;
- (3) любой гомоморфизм R в ненулевое кольцо инъективен.



Докажем соответствующие импликации:

- $(1) \Rightarrow (2)$:

Пусть $J \trianglelefteq R$ и $x \in J$, тогда $(1) = (x) \subseteq J \Rightarrow J = (1)$.

- $(2) \Rightarrow (3)$:

Пусть $f : R \rightarrow B$ - кольцевой гомоморфизм. Тогда

$$\ker f \trianglelefteq R, \quad \ker R \neq R \Rightarrow \ker f = 0,$$

откуда следует инъективность.

- $(3) \Rightarrow (1)$

Пусть $x \notin R^*$, тогда

$$(x) \neq (1) \Rightarrow B = R/(x) \neq 0, \quad \varphi : R \rightarrow R/(x)$$

Из инъективности канонического отображения φ следует, что $(x) = 0$ и $x = 0$.





Лекция 4

Поле комплексных чисел

Содержание лекции:

В данной лекции мы коротко рассмотрим поле комплексных чисел, которое возникает как алгебраическое замыкание поля \mathbb{R} . Обсуждая алгебраические операции с комплексными числами мы заложим основы для использования этих чисел в различных областях математики и ее приложений.

Ключевые слова:

Комплексное число, поле комплексных чисел, алгебраическая форма КЧ, комплексно сопряженное число, тригонометрическая форма КЧ, формула Муавра, показательная форма КЧ.

Авторы курса:

Трифанов А.И.

Москаленко М.А.

Ссылка на ресурсы:

mathdep.ifmo.ru/geolin

4.1 Алгебраическая форма комплексного числа

Комплексным числом называется элемент z декартова произведения $\mathbb{R} \times \mathbb{R}$:

$$z = (a, b), \quad a, b \in \mathbb{R},$$

снабженного двумя бинарными операциями, *индуцированными* из \mathbb{R} :

- $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$;
- $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1)$;

Nota bene Для множества комплексных чисел имеется специальное обозначение:

$$\mathbb{C} = \{(a, b) : a, b \in \mathbb{R}\}.$$

Nota bene Имеет место свойство

$$z_1 = z_2 \Leftrightarrow a_1 = a_2, \quad b_1 = b_2.$$

Теорема 4.1. Множество \mathbb{C} имеет алгебраическую структуру поля.



Сначала проверим свойства операции $+$:

1. ассоциативность очевидна в силу ассоциативности $+$ на множестве \mathbb{R} ;
2. нейтральный элемент $0_{\mathbb{C}} = (0, 0)$, действительно:

$$\forall z \in \mathbb{C} \quad z + 0_{\mathbb{C}} = z = 0_{\mathbb{C}} + z;$$

3. обратным элементом для $z = (a, b)$ является $(-z) = (-a, -b)$;

Далее, проверим свойства операции \cdot :

1. ассоциативность проверяется непосредственно:

$$((a_1, b_1) \cdot (a_2, b_2)) \cdot (a_3, c_3) = (a_1, b_1) \cdot ((a_2, b_2) \cdot (a_3, c_3)).$$

2. нейтральный элемент $1_{\mathbb{C}} = (1, 0)$:

$$1_{\mathbb{C}} \cdot z = (1, 0) \cdot (a, b) = (a, b).$$

3. обратным элементом для $z = (a, b) \neq (0, 0) = 0_{\mathbb{C}}$ является

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

Осталось проверить дистрибутивность введенных операций слева и справа, что проводится непосредственным вычислением:

$$z_1 \cdot (z_2 + z_3) = z_1 \cdot z_2 + z_1 \cdot z_3.$$



Лемма 4.1. Отображение $\sigma : \mathbb{R} \rightarrow \mathbb{C}$, заданное формулой $\sigma(a) = (a, 0)$ является вложением \mathbb{R} в \mathbb{C} .



Покажем, что σ - гомоморфизм:

$$\begin{aligned}\sigma(a+b) &= (a+b, 0) = (a, 0) + (b, 0) = \sigma(a) + \sigma(b), \\ \sigma(ab) &= (ab, 0) = (a, 0) \cdot (b, 0) = \sigma(a) \cdot \sigma(b).\end{aligned}$$

Далее σ инъективно:

$$\sigma(a) = \sigma(b) \Rightarrow \sigma(a-b) = (0, 0) \Rightarrow a-b=0.$$

Следовательно σ - вложение.



Алгебраической формой комплексного числа $z = (a, b) \in \mathbb{C}$ называется представление его в следующем виде:

$$z = a + ib,$$

где символ i называется **мнимой единицей** и обладает свойством $i^2 = -1 \in \mathbb{R}$.

Лемма 4.2. Отображение $(a, b) \mapsto a + ib$ является кольцевым изоморфизмом.

Nota bene Заметим, что $i' = -i$ также является мнимой единицей, что приводит к автоморфизму $z \mapsto \bar{z}$ поля \mathbb{C} , который называется **комплексным сопряжением**.

Пусть $z = a + ib \in \mathbb{C}$ - комплексное число, тогда

- $\Re z \triangleq a$ называется **вещественной частью** числа z ;
- $\Im z \triangleq b$ называется **мнимой частью** числа z ;
- $\bar{z} = a - ib$ называется числом, **комплексно сопряженным** к z ;
- $N(z) \triangleq z\bar{z} = a^2 + b^2$ называется **нормой** комплексного числа z ;
- $|z| = \sqrt{N(z)} = \sqrt{a^2 + b^2}$ называется **модулем** комплексного числа.

4.2 Тригонометрическая форма комплексного числа

Nota bene Пару вещественных чисел (a, b) , определяющих комплексное число z , можно интерпретировать как координаты некоторой точки на плоскости, которая называется *комплексной плоскостью*. Координаты на рассматриваемой плоскости - это *вещественная* \Re и *мнимая* \Im оси.

Аргументом комплексного числа z (обозначается $\arg(z)$) называется направленный угол от оси \Re до луча Oz , откладываемый против часовой стрелки с величиной, берущейся по модулю $2\pi k$.

Nota bene Альтернативно паре (a, b) можно использовать пару (ρ, ψ) , определяемую следующим образом:

$$a = \rho \cos \psi, \quad b = \rho \sin \psi, \\ \rho = \sqrt{a^2 + b^2} = |z|, \quad \cos \psi = a/|z|, \quad \sin \psi = b/|z|.$$

Пара (ρ, ψ) отвечает координатам точки z в *полярной системе координат*.

Тригонометрической формой комплексного числа $z \in \mathbb{C}$ называется представление его в следующем виде:

$$z = (\rho \cos \psi, \rho \sin \psi) = \rho(\cos \psi, \sin \psi).$$

Лемма 4.3. *Имеют место свойства:*

$$|z_1 z_2| = |z_1| |z_2|, \quad \arg(z_1 z_2) = \arg(z_1) + \arg(z_2).$$



Прямой проверкой убеждаемся, что

$$\rho_1(\cos \psi_1, \sin \psi_1) \cdot \rho_2(\cos \psi_2, \sin \psi_2) = \rho_1 \rho_2 (\cos(\psi_1 + \psi_2), \sin(\psi_1 + \psi_2)).$$



Теорема 4.2. (Формула Муавра) Пусть $z \in \mathbb{C}$ и $n \in \mathbb{N}$, тогда

$$|z^n| = |z|^n, \quad \arg(z^n) = n \cdot \arg(z).$$



Доказательство проводится индукцией по n .



Пример 4.1. Найдем решение уравнения

$$z^n = \omega, \quad z, \omega \in \mathbb{C}, \quad n \in \mathbb{N}.$$

Из формулы Муавра следует

$$|z|^n \cdot (\cos(n\psi), \sin(n\psi)) = |\omega| \cdot (\cos \chi, \sin \chi),$$

откуда получаем

$$|z| = \sqrt[n]{|\omega|}, \quad n\psi = \chi + 2\pi k, \quad k \in \mathbb{Z}.$$

И значит

$$z = \sqrt[n]{|\omega|} \left(\cos \frac{\chi + 2\pi k}{n}, \sin \frac{\chi + 2\pi k}{n} \right)$$

Nota bene Из примера видно, что все решения уравнения лежат на окружности радиуса $r = \sqrt[n]{|\omega|}$ в вершинах правильного n - угольника.

Лемма 4.4. Множество корней уравнения $z^n = 1$ образует мультипликативную абелеву группу.



Пусть S - множество решений данного уравнения. Покажем, что S замкнуто:

$$\varepsilon_1, \varepsilon_2 \in S \Rightarrow \varepsilon_1^n = 1, \quad \varepsilon_2^n = 1 \Rightarrow (\varepsilon_1 \varepsilon_2)^n = 1 \Rightarrow \varepsilon_1 \varepsilon_2 \in S.$$

Нейтральным элементом является $\varepsilon_0 = 1_{\mathbb{C}}$.

Обратный элемент к $\varepsilon \in S$ имеет вид $\varepsilon^{-1} = \varepsilon^{n-1}$.



Nota bene Альтернативная форма записи комплексного числа в тригонометрической форме имеет вид:

$$z = \rho \cdot (\cos \psi + i \sin \psi).$$

|| **Показательная форма** комплексного числа имеет вид

$$z = \rho \cdot e^{i\psi}, \quad \rho = |z|, \quad \psi = \arg(z), \quad i^2 = -1.$$

Nota bene (формулы Эйлера)

$$\cos \psi = \frac{e^{i\psi} + e^{-i\psi}}{2}, \quad \sin \psi = \frac{e^{i\psi} - e^{-i\psi}}{2i}.$$



Лекция 5

Начало алгебры многочленов

Содержание лекции:

В настоящей лекции мы кратко рассмотрим основные понятия, связанные с кольцом многочленов и операциями в нем. Данная структура является основополагающей ряда разделов математики и часто служит источником нетривиальных примеров для алгебры и анализа.

Ключевые слова:

Многочлен, коэффициенты многочлена, степень многочлена, сумма и произведение многочленов, ассоциированные многочлены, делимость, остаток от деления, корень многочлена.

Авторы курса:

Трифанов А.И.

Москаленко М.А.

Ссылка на ресурсы:

mathdep.ifmo.ru/geolin

5.1 Основные определения

Nota bene Пусть K - некоторое поле.

Многочленом от одной переменной с коэффициентами из поля K будем называть формальную бесконечную сумму следующего вида:

$$f(x) = a_0 + a_1t + a_2t^2 + \dots + a_nt^n + \dots,$$

в которой отличны от нуля только *некоторые коэффициенты* $a_0, a_1, a_2, \dots \in K$, а t называется **формальной переменной**.

Nota bene Множество многочленов от переменной t будем обозначать через $K[t]$. Пусть далее $f, g \in K[t]$, так что

$$f(t) = \sum_{n=0}^{\infty} a_nt^n, \quad g(t) = \sum_{m=0}^{\infty} b_mt^m,$$

Суммой двух многочленов f и g называется такой многочлен $h = f + g$, что

$$h(t) = \sum_{k=0}^{\infty} c_kt^k, \quad c_k = a_k + b_k.$$

Произведением двух многочленов f и g называется такой многочлен $p = fg$, что

$$p(t) = \sum_{j=0}^{\infty} d_jt^j, \quad d_j = \sum_{i=0}^j a_ib_{j-i}.$$

Теорема 5.1. Множество $K[t]$, наделенное операциями сложения и умножения является коммутативным ассоциативным кольцом.



- Прямой проверкой нетрудно убедиться, что $K[t]$ - абелева группа по сложению с нейтральным элементом $0(t)$ и обратным для каждого $f(t)$, представляющим собой элемент $-f(t)$.
- Также прямой проверкой можно убедиться, что произведение индуцирует на $K[t]$ структуру коммутативного моноида с нейтральным элементом $1(t)$.
- Проверим дистрибутивность: пусть $f, g, h \in K[t]$, и

$$(f + g)h = \sum_{k=0}^{\infty} d_kt^k, \quad fh = \sum_{n=0}^{\infty} p_nt^n, \quad gh = \sum_{m=0}^{\infty} q_mt^m.$$

тогда имеет место

$$d_k = \sum_i i = 0^k(a_i + b_i)c_{k-i} = \sum_i i = 0^k(a_ic_{k-i}) + \sum_i i = 0^k(b_ic_{k-i}) = p_k + q_k,$$

а это коэффициент многочлена $fh + gh$.



Nota bene Полное название кольца $K[t]$ звучит так: *ассоциативное коммутативное кольцо с единицей*.

Лемма 5.1. Пусть $\sigma : K \rightarrow K[t]$ определено формулой $\sigma(\alpha) = \alpha + 0 \cdot t + 0 \cdot t^2 + \dots$, тогда σ - вложение.



Прямой проверкой легко убедиться, что σ - гомоморфизм. Пусть далее

$$\alpha \in \ker \sigma \Rightarrow \sigma(\alpha) = \alpha + 0t + \dots = 0 + 0t + \dots \Rightarrow \alpha = 0.$$

Таким образом, σ - вложение.



Nota bene В дальнейшем договоримся записывать $\alpha f(t)$ понимая под этим $\sigma(\alpha)f(t)$

5.2 Делимость в кольце многочленов

|| Два многочлена f и g называются **ассоциированными** (обозначают $f \sim g$), если $f = \alpha \cdot g$, где $\alpha \in K$, $\alpha \neq 0$.

Лемма 5.2. Ассоциированность - отношение эквивалентности.



Проверим свойства отношения:

- рефлексивность: $f = 1 \cdot f \Rightarrow f \sim f$;
- симметричность: $f \sim g \Rightarrow f = \alpha g \Rightarrow g = \frac{1}{\alpha} f \Rightarrow g \sim f$;
- транзитивность:

$$f \sim g, \quad g \sim h \Rightarrow f = \alpha g, \quad g = \beta h \Rightarrow f = \alpha \beta h \Rightarrow f \sim h.$$



|| **Степенью** $\deg(f)$ многочлена $f \in K[t]$ называется максимальный номер его ненулевого коэффициента. Для нулевого многочлена $\theta(t)$ положим $\deg(\theta) = -\infty$. Если $\deg f = n \in \mathbb{N}_0$ то коэффициент a_n называется **старшим коэффициентом** многочлена f .

Лемма 5.3. Пусть $f, g \in K[t]$ тогда имеют место следующие свойства:

$$\deg(fg) = \deg(f) + \deg(g), \quad \deg(f + g) \leq \max \{ \deg(f), \deg(g) \}.$$



Пусть $\deg(f) = n$ и $\deg(g) = m$, и при этом

$$f = \sum_{i=0} a_i t^i \quad g = \sum_{j=0} b_j t^j, \quad fg = \sum_{k=0} c_k t^k,$$

тогда будем иметь

$$c_{n+m} = \sum_{i=0}^{n-1} a_i b_{n+m-i} + a_n b_m + \sum_{i=n+1}^{n+m} a_i b_{n+m-i} = a_n b_m \neq 0.$$

При $k > n + m$ имеем $c_k = 0$ и, следовательно, $\deg(fg) = n + m$.

Доказательство второго свойства следует из того, что при $k > \max\{\deg(f), \deg(g)\}$ имеем

$$a_k = b_k = 0 \quad \Rightarrow \quad c_k = a_k + b_k = 0.$$



Теорема 5.2. Пусть $f, g \in K[t]$, причем $g \neq 0$, тогда существуют единственные $q, r \in K[t]$, такие что

$$f = qg + r, \quad \deg(r) < \deg(g).$$



Пусть $\deg(f) = n$ и $\deg(g) = m$, а также

$$f(t) = a_n t^n + \dots + a_0, \quad g(t) = b_m t^m + \dots + b_0.$$

Далее используем индукцию по n . При $n < m$ в качестве базы подходит

$$q = 0, \quad r = f.$$

Пусть, далее $n \geq m$ и для многочленов степени меньшей n утверждение доказано. Так как

$$f_1(t) = f(t) - \frac{a_n}{b_m} t^{n-m} g(t), \quad \deg(f_1) < n,$$

то по индукционному предположению

$$f_1 = q_1 g + r, \quad \deg(r) < m,$$

но тогда

$$f(t) = \left(q_1(t) + \frac{a_n}{b_m} t^{n-m} \right) g(t) + r(t)$$

- искомое представление для $f(t)$.

Теперь докажем единственность. Пусть

$$q_1 g + r_1 = f = q_2 g + r_2, \quad \deg(r_1) < m, \quad \deg(r_2) < m.$$

Тогда

$$r_1 - r_2 = g(q_2 - q_1).$$

Пусть далее $q_1 \neq q_2$, имеем:

$$\deg((q_2 - q_1)g) = \deg(q_2 - q_1) + \deg(g) \geq m.$$

С другой стороны:

$$\deg(r_1 - r_2) \leq \max(\deg(r_1), \deg(r_2)) < m.$$

Противоречие. Значит $q_1 = q_2$ и $r_1 = r_2$. ◀

|| Говорят, что многочлен f **делится на многочлен** g (пишут $f \div g$), если существует такой многочлен h , что $f = gh$.

Лемма 5.4. Если $f \div g$ и $g \div h$, тогда $f \div h$.

►

Из условия следует, что

$$f = pg, \quad g = qh \quad \Rightarrow \quad f = (pq)h.$$

◀

Лемма 5.5. Пусть $f, g \div h$, тогда

$$\forall p, q \in K[t] \quad (pf + qg) \div h.$$

►

Имеем

$$f = \alpha h, \quad g = \beta h, \quad \alpha, \beta \in K[t] \quad \Rightarrow \quad fp + gq = (\alpha p + \beta q)h.$$

◀

Лемма 5.6. Пусть $f \div g$, причем $f, g \neq 0$, тогда

$$\deg(f) \geq \deg(g).$$

►

Из условия следует, что

$$f = gh, \quad g \in K[t], \quad h \neq 0 \quad \Rightarrow \quad \deg(f) = \deg(g) + \deg(h) \geq \deg(g).$$

◀

Лемма 5.7. Пусть $f \div g$, $f, g \neq 0$ и $\deg(f) = \deg(g)$, тогда $f \sim g$.

►

Из условий следует $f = gh$, $h \in K[t]$ и

$$\deg(g) = \deg(f) = \deg(g) + \deg(h) \quad \Rightarrow \quad \deg(h) = 0 \quad \Rightarrow \quad h \in K.$$

◀

Лемма 5.8. Пусть $f \dot{\vdots} g$, $f, g \neq 0$ и $g \dot{\vdots} f$, тогда $f \sim g$.



Имеем

$$\deg(f) \geq \deg(g), \quad \deg(g) \geq \deg(f) \quad \Rightarrow \quad \deg(f) = \deg(g).$$



5.3 Корень многочлена

Пусть $f \in K[t]$ и $\alpha \in K$. Число α называется **корнем** многочлена f степени m , если

$$f(t) \dot{\vdots} (t - \alpha)^m, \quad f(t) \not\dot{\vdots} (t - \alpha)^{m+1}.$$

Лемма 5.9. Остаток от деления $f \in K[t]$ на $(t - \alpha)$ равен $f(\alpha)$



По теореме от делении с остатком имеем:

$$f(t) = (t - \alpha)q(t) + r(t), \quad \deg(r) \leq \deg(t - \alpha) = 1$$

Следовательно, $r(t) = r \in K$ и

$$f(\alpha) = 0 \cdot q(\alpha) + r.$$



Nota bene Если $f \in K[t]$ и α - корень $f(t)$, тогда $f(t) \dot{\vdots} (t - \alpha)$.

Теорема 5.3. (основная теорема алгебры) Любой многочлен из $\mathbb{C}[t]$ имеет корень из \mathbb{C} .

Nota bene Пусть $f(t) \in \mathbb{C}[t]$, $\deg(f) = n$ и c - старший коэффициент f , тогда

$$f(t) = c(t - \alpha_1)(t - \alpha_2) \dots (t - \alpha_n), \quad \alpha_j \in \mathbb{C},$$

причем не обязательно все α_j различны.

Nota bene Рассмотрим автоморфизм $\sigma : \mathbb{C}[t] \rightarrow \mathbb{C}[t]$, индуцированный операцией комплексного сопряжения в \mathbb{C} :

$$\sigma(f(t)) = \bar{f}(t) = \bar{a}_n t^n + \dots + \bar{a}_1 t + \bar{a}_0, \quad f(t) = a_n t^n + \dots + a_1 t + a_0.$$

Лемма 5.10. Пусть $f \in \mathbb{C}[t]$ и $\alpha \in \mathbb{C}$ - корень f кратности m . Тогда $\bar{\alpha}$ - корень \bar{f} той же кратности m .



Из условия леммы имеем:

$$f(t) = (t - \alpha)^m g(t) \quad \Rightarrow \quad \bar{f}(\bar{t}) = (\bar{t} - \bar{\alpha})^m \cdot \bar{g}(\bar{t}).$$

Но это значит, что $\bar{\alpha}$ - корень \bar{f} кратности k не меньшей m . Далее, $\alpha = \bar{\bar{\alpha}}$ - корень $f = \bar{\bar{f}}$ кратности не меньшей k , откуда $k = m$. ◄

Теорема 5.4. Многочлен $f \in \mathbb{R}[t]$ степени $\deg(f) = n \geq 1$ со старшим коэффициентом c раскладывается в $\mathbb{R}[t]$ на множители:

$$f(t) = c(t - \alpha_1)^{k_1} \dots (t - \alpha_s)^{k_s} \cdot (t^2 + p_1t + q_1)^{m_1} \dots (t^2 + p_rt + q_r)^{m_r},$$
$$D(t^2 + p_it + q_i) = p_i^2 - 4q_i < 0, \quad i = 1 \dots r.$$

Лемма 5.11. Многочлен $f \in \mathbb{R}[t]$ нечетной степени всегда имеет действительный корень.



Согласно предыдущей теореме, сумма кратностей всех комплексных корней f равна $\deg(f)/2$, а сумма кратностей невещественных корней четна. Следовательно, кратность вещественных корней нечетна и значит такие корни есть.





Лекция 6

Матрицы и определители

Содержание лекции:

В настоящей лекции мы начинаем рассматривать один из основных объектов линейной алгебры - матрицу. Здесь мы введем основные определения, связанные с этим понятием и выведем некоторые интересные свойства и приведем ряд примеров. Исследование матриц по существу составляет основную часть настоящего курса.

Ключевые слова:

Матрица, сумма и произведение матриц, единичная матрица, нильпотентная матрица, обратимая матрица, определитель матрицы, дополнительный минор, элементарные преобразования, транспонированная матрица.

Авторы курса:

Трифанов А.И.

Москаленко М.А.

Ссылка на ресурсы:

mathdep.ifmo.ru/geolin

6.1 Определения

Матрицей договоримся называть прямоугольную таблицу, составленную из элементов некоторого поля K :

$$A_{m \times n} = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & \dots & a_{2,n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{m,1} & a_{m,2} & a_{m,3} & \dots & a_{m,n} \end{pmatrix}, \quad a_{ij} \in K,$$

совокупность элементов с фиксированным первым индексом называется **строкой матрицы**, а с фиксированным вторым индексом - **столбцом матрицы** A .

Nota bene Число m определяет, таким образом, число строк матрицы, а n - число ее столбцов. Матрица, у которой $m = n$ называется *квадратной*, в противном случае - *прямоугольной*.

Nota bene Множество $m \times n$ матриц с элементами из поля K будем обозначать $\mathcal{M}_{m \times n}(K)$.

Суммой матриц A и B , где $A, B \in \mathcal{M}_{m,n}(K)$ называется матрица $C = A + B$, $C \in \mathcal{M}_{m,n}(K)$ такая что:

$$c_{i,j} = a_{i,j} + b_{i,j}, \quad A = \{a_{i,j}\}, \quad B = \{b_{i,j}\}.$$

Лемма 6.1. Относительно операции сложения $\mathcal{M}_{m,n}(K)$ - абелева группа.



Проверим аксиомы группы:

- ассоциативность следует из определения и проверяется тривиально;
- нейтральный элемент - нулевая матрица θ : $\theta_{i,j} = 0$;
- противоположный элемент: $\forall A = \{a_{i,j}\} \quad \exists (-A) = \{-a_{i,j}\}$.



Произведением матриц $A \in \mathcal{M}_{m,p}(K)$ и $B \in \mathcal{M}_{p,n}(K)$ называется матрица $C = A \cdot B$, $C \in \mathcal{M}_{m,n}(K)$, такая что:

$$c_{i,j} = \sum_{k=1}^p a_{i,k} b_{k,j}, \quad A = \{a_{i,k}\}, \quad B = \{b_{k,j}\}.$$

Лемма 6.2. Операция умножения матриц ассоциативна и некоммутативна.

Единичной матрицей $E \in \mathcal{M}_{n,n}(K)$ называется матрица, для которой

$$e_{i,j} = \begin{cases} 1, & i = j; \\ 0, & i \neq j. \end{cases} \equiv \delta_{i,j}.$$

Nota bene Пусть $A \in \mathcal{M}_{m,p}(K)$, $B \in \mathcal{M}_{p,n}(K)$ и $E \in \mathcal{M}_{p,p}(K)$, тогда

$$A \cdot E = A, \quad E \cdot B = B.$$

Квадратная матрица N называется **нильпотентной матрицей порядка k** , если

$$N^m = N \cdot \dots \cdot N = \theta, \quad N^{m-1} \neq \theta.$$

Nota bene Пример nilпотентной матрицы порядка $k = 2$:

$$N = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Квадратная матрица $A \in \mathcal{M}_{n,n}(K)$ называется **обратимой**, если в $\mathcal{M}_{n,n}(K)$ существуют матрицы B и C , такие что

$$A \cdot B = E = C \cdot A.$$

Лемма 6.3. На множестве квадратных матриц $\mathcal{M}_{n,n}$ операция умножения индуцирует структуру некоммутативного моноида.

Теорема 6.1. Операции сложения и умножения индуцируют на множестве квадратных матриц $\mathcal{M}_{n,n}$ структуру ассоциативного некоммутативного кольца.

Пример 6.1. Приведем пример одного интересного изоморфизма. Рассмотрим множество комплексных чисел \mathbb{C} и множество $\mathcal{M}_2(\mathbb{R})$ 2×2 вещественных квадратных матриц вида:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Пусть $\sigma : \mathbb{C} \rightarrow \mathcal{M}_2$ - отображение со следующими свойствами:

$$\sigma(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma(i) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Проверьте, что σ - гомоморфно, сюръективно и инъективно.

6.2 Определитель матрицы

Определителем квадратной матрицы A договоримся называть число $\det(A)$, которое ставится ей в соответствие по следующим образом:

1. $\det A_1 = \det(a) = a$;
2. $\det A_2 = \det \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} = a_{1,1}a_{2,2} - a_{2,1}a_{1,2}$.
- ...
- m. $\det A_m = \sum_{i=1}^m (-1)^{i+j} \cdot a_{i,j} \cdot M_{i,j}$,

где $M_{i,j}$ - **дополнительный минор** элемента $a_{i,j}$ - определитель матрицы A' , полученной из матрицы A вычеркиванием строки и столбца, на пересечении которых находится элемент $a_{i,j}$.

Элементарными преобразованиями матрицы называются следующие:

- E1. Перестановка строк матрицы;
- E2. Произведение всех элементов некоторой строки на число $\lambda \neq 0$;
- E3. Поэлементное сложение одной строки с другой, умноженной на число λ .

Лемма 6.4. *Имеют место следующие свойства определителя:*

1. *при элементарном преобразовании (E1) определитель меняет знак;*
2. *общий множитель всех элементов строки может быть вынесен;*
3. *при элементарном преобразовании (E2) определитель сохраняется;*
4. *определитель с двумя одинаковыми строками равен нулю;*
5. *определитель произведения матриц равен произведению их определителей;*

Nota bene Прямой проверкой легко убедиться, что

$$\det(A + B) \neq \det A + \det B.$$

Транспонированием матрицы $A \in \mathcal{M}_{m,n}$ называется операция $()^T$ в результате которой получается матрица со следующим свойством:

$$A = \{a_{i,j}\}, \quad A^T = \{a'_{i,j}\}, \quad a'_{i,j} = a_{j,i}.$$

Лемма 6.5. *Имеет место свойство:*

$$\det(A^T) = \det(A).$$

Теорема 6.2. *(критерий обратимости матрицы)*

$$\exists A^{-1} \Leftrightarrow \det(A) \neq 0.$$



Лекция 7

Системы линейных уравнений

Содержание лекции:

Системы линейных алгебраических уравнений возникают в огромном количестве приложений. Здесь мы рассмотрим простейший случай существования единственного решения. Однако обсуждаемые здесь методы будут развиты в дальнейшем для более общих случаев и задач.

Ключевые слова:

Линейное алгебраическое уравнение, система уравнений, коэффициенты системы, решение системы, совместность системы, элементарные преобразования СЛАУ, матрица СЛАУ, расширенная матрица, ведущий элемент строки, ступенчатая матрица, метод Гаусса, элементарная матрица,

Авторы курса:

Трифанов А.И.

Москаленко М.А.

Ссылка на ресурсы:

mathdep.ifmo.ru/geolin

7.1 Основные определения

Линейным алгебраическим уравнением с неизвестными x_1, x_2, \dots, x_n над полем K называется уравнение вида

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b, \quad (7.1)$$

где $a_1, a_2, \dots, a_n \in K$ называются **коэффициентами**, а $b \in K$ **свободным членом** линейного уравнения.

Решением линейного алгебраического уравнения называется упорядоченный набор чисел $y_1, y_2, \dots, y_n \in K$, который будучи подставленным в линейное уравнение (7.1) превращает его в тождество.

Системой линейных алгебраических уравнений с m уравнениями и n неизвестными называется система вида

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,n}x_n = b_1, \\ a_{2,1}x_1 + a_{2,2}x_2 + \dots + a_{2,n}x_n = b_2, \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots, \\ a_{m,1}x_1 + a_{m,2}x_2 + \dots + a_{m,n}x_n = b_m. \end{cases} \quad (7.2)$$

Решением системы линейных алгебраических уравнений (7.2) называется упорядоченный набор чисел z_1, z_2, \dots, z_n , который является решением *каждого* линейного алгебраического уравнения системы

Nota bene Далее для удобства и общности линейные уравнения также будем считать системами, состоящими из одного уравнения.

Система (7.2) называется **совместной**, если она имеет хотя бы одно решение и **несовместной** в противном случае.

Nota bene Будем обозначать через \mathcal{S}_n^m множество всех систем линейных алгебраических уравнений, содержащих m уравнений и n неизвестных.

Nota bene Пусть $S_1, S_2 \in \mathcal{S}_n^m$ - две системы, будем писать $S_1 \sim S_2$ если множества решений этих систем совпадают.

Лемма 7.1. Отношение \sim является отношением эквивалентности на \mathcal{S}_n^m .

Nota bene Договоримся класс с представителем $S \in \mathcal{S}_n^m$ обозначать через $[S]$.

7.2 Элементарные преобразования СЛАУ

Элементарными преобразованиями системы линейных алгебраических уравнений называются преобразования следующих трех типов:

- L1. Прибавление к одному уравнению другого, умноженного на число;
- L2. Перестановка двух уравнений;
- L3. Умножение одного уравнения на число, отличное от нуля.

Лемма 7.2. В результате элементарных преобразований любая система S переходит в эквивалентную ей систему S' .

Матрицей системы алгебраических уравнений называется матрица S системы (7.2), составленная из коэффициентов этой системы. **Расширенной матрицей** матрицей называется матрица \tilde{S} системы, полученная приписыванием к матрице системы S столбца свободных членов:

$$S = \begin{pmatrix} a_{1,1} & a_{1,1} & \dots & a_{1,n} \\ a_{2,1} & a_{2,1} & \dots & a_{2,n} \\ \dots & \dots & \dots & \dots \\ a_{m,1} & a_{m,1} & \dots & a_{m,n} \end{pmatrix}, \quad \tilde{S} = \begin{pmatrix} a_{1,1} & a_{1,1} & \dots & a_{1,n} & b_1 \\ a_{2,1} & a_{2,1} & \dots & a_{2,n} & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{m,1} & a_{m,1} & \dots & a_{m,n} & b_m \end{pmatrix}.$$

Лемма 7.3. Элементарные преобразования системы линейных алгебраических уравнений - это в точности элементарные преобразования ее расширенной матрицы:

$$L_1 \leftrightarrow E_1, \quad L_2 \leftrightarrow E_2, \quad L_3 \leftrightarrow E_3.$$

Ведущим элементом строки матрицы S с номером k называется ее первый ненулевой элемент.

Матрица S называется **ступенчатой**, если

- 1. номера ведущих элементов ее ненулевых строк образуют строго возрастающую последовательность;
- 2. нулевые строки, если они есть, стоят в конце.

Теорема 7.1. Всякую матрицу с помощью элементарных преобразований можно привести к ступенчатому виду.



Алгоритм Гаусса.



Система линейных алгебраических уравнений называется **ступенчатой**, если ее расширенная матрица ступенчатая.

Nota bene Пусть $r(\tilde{r})$ - число ненулевых строк в матрице S (\tilde{S}), приведенной к ступенчатому виду, тогда возможны только три варианта:

1. $\tilde{r} = r + 1$ - система несовместна;
2. $\tilde{r} = r = n$ - система имеет единственное решение;
3. $\tilde{r} = r < n$ - система имеет множество решений.

7.3 Метод Гаусса. Элементарные матрицы

Nota bene Любую систему линейных алгебраических уравнений можно записать в матричной форме. Именно, пусть X - столбик неизвестных и B - столбик свободных членов:

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \quad B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

Тогда систему (7.2) можно записать в виде

$$A \cdot X = B. \quad (7.3)$$

Nota bene Пусть U - произвольная квадратная $m \times m$ матрица, тогда

$$U \cdot A \cdot X = U \cdot B, \quad (7.4)$$

и всякое решение (7.3) является также решением (7.4).

Рассмотрим следующие виды матриц, которые назовем **элементарными**:

$$e_{i,j}(\lambda) = E + \lambda E_{i,j}, \quad p_{i,j} = E + E_{i,j} + E_{j,i} - E_{i,i} - E_{j,j}, \quad q_{i,j}(\lambda) = E + (\lambda - 1)E_{i,i},$$

причем $i \neq j$ и $\lambda \neq 0$.

Лемма 7.4. Элементарные матрицы обратимы, причем:

$$e_{i,j}(\lambda)^{-1} = e_{i,j}(-\lambda), \quad p_{i,j}^{-1} = p_{i,j}, \quad q_{i,j}(\lambda)^{-1} = q_{i,j}(\lambda^{-1}).$$

Лемма 7.5. Имеет место следующее свойство:

$$E1(S) = e \cdot S, \quad E2(S) = p \cdot S, \quad E3(S) = q \cdot S.$$

Nota bene Таким образом, метод Гаусса в матричной интерпретации состоит в последовательном умножении уравнения (7.3) слева на элементарные матрицы с целью приведения матрицы S к ступенчатому виду.