α

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, поглощащий элемент, ассоциативность закона, коммутативность закона, теорема об ассоциативном коммутативном законе, внешний закон композици, согласованность внешнего закона.

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 $M \times M \to M$ 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

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

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, соответсвенно, операций объединения и пересечения подмножеств:

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

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:*

$$e_L = e_R \equiv e$$

►
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

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

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

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

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:

$$(X,Y) \to X \triangle Y = (X \setminus Y) \cup (Y \setminus X),$$
$$X \triangle X = \varnothing, \quad X \triangle \varnothing = X.$$

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

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 Внешний закон композиции

Внешним законом композиции элементов множества Ω, называемых множеством *операторов закона*, и элементов множества M называется отображение множества $\Omega \times M$ в некоторое множество N. Значение

$$(\alpha, x) \mapsto y,$$

называется композицией α и x относительно этого закона. Элементы из Ω называются **операторами** внешнего закона.

Nota bene Как правило, действие оператора $\alpha \in \Omega$ на элемент $x \in M$ обозначают следующим образом:

$$\alpha x, \quad \alpha(x), \quad x^{\alpha}, \quad \alpha \perp x.$$

Пусть M - множество, наделенное внутренним и внешним законами композиции. Говорят, что внешний закон композиции **согласован** с внутренним законом, если

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

β

Лекция 2

Группы и гомоморфизмы

Содержание лекции:
В настоящей лекции мы введем одно из центральных структур алгебры - группу. Рассматривая группу как иллюстративный пример множества с внутренним законом композиции, мы введем основные определения, связанные с этой структурой, а также подготовимся к формулировке одного из самых известных утверждений о группах - теоремы об изоморфизме.

Ключевые слова:
Магма, полугруппа, моноид, группа, коммутативная группа, гомоморфизм групп, изоморфизм, автоморфизм, ядро гомоморфизма, образ гомоморфизма, вложение.

Авторы курса:

Трифанов А.И. Москаленко М. А.

Ссылка на ресурсы:
mathdep.ifmo.ru/geolin

2.1 Основные структуры

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

Пример 2.1. Пусть множество M содержит только три элемента $\{-1, 0, 1\}$. Алгебраическую структуру магмы на S задает следующий закон композиции:

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

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

Пример 2.2. Множество натуральных чисел $\mathbb{N}$ с операцией операцией $\circ = " + "$ является полугруппой $(\mathbb{N}, " + ")$.

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

Пример 2.3. Множество натуральных чисел $\mathbb{N}$ с операцией операцией $\circ = " \cdot "$ является моноидом $(\mathbb{N}, 1, " \cdot ")$.

2.2 Определение группы

Непустое множество G называется **группой**, если на нем задан закон композиции $G \times G \to G$, 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 2.4. На практике группы чаще всего встречаются в виде *групп преобразований* каких-то обьектов:

- 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 2.5. 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 вещественныз 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;

2.3 Гомоморфизмы групп

Гомоморфизмом групп G и G' называется отображение $\sigma : G \to G'$, 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 $\mathrm{Hom}(G, G')$. Гомоморфизмы из G в G называются эндоморфизмами и их множество обозначается $\mathrm{End}(G) \triangleq \mathrm{Hom}(G, G)$.

Nota bene Напомним некоторые свойства отображений. Пусть M и N - два множества и $f : M \to N$. Отображение f называется *инъективным (или инъекцией)*, если имеет место свойство:

$$f(x) = f(y) \quad \Rightarrow \quad x = y.$$

Далее, отображение f называется *сюръективным (или сюръекцией)*, если

$$\forall y \in N \quad \exists\, x \in M : \quad f(x) = y.$$

И, наконец, f, будучи сюрьекцией и инъекцией называется *биекцией (или взаимнооднозначным отображением)*. В этом случае

$$\exists\, g : N \to M \quad : \quad g \circ f = \mathrm{id}_M, \quad f \circ g = \mathrm{id}_N\,.$$

Рассмотрим ситуацию, когда соответствующие множества имеют структуру группы.

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

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

Гомоморфизм σ называется **изоморфизмом**, если

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

Соответствующие группы при этом называются *изоморфными* (пишут $G \simeq G'$).

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

Пример 2.6. Множество $\mathrm{Aut}(G)$ вместе с операцией композиции и тождественным отображением id_G является группой (автоморфизмов группы G).

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

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

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

Лемма 2.3. *Гомоморфизм* $\sigma \in \mathrm{Hom}(G, G')$ *ядро которого тривиально иньективен.*

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

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

Лемма 2.4. *Образ* $\mathrm{Im}\, \sigma$ *является группой.*

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

$$G \simeq \mathrm{Im}\, \sigma \subset G'.$$

Лекция 3

Подгруппы и фактор-группы

Содержание лекции:
В данной лекции мы продолжим вводить понятия, связанные с групповой структурой. Также мы сформулируем ряд утверждений, связанных с гомоморфизмами групп. В конце лекции мы докажем теорему об изоморфизме.

Ключевые слова:
Подгруппа, отношение эквивалентности, правый (левый) смежный класс, нормальная подгруппа, фактор-группа, канонический гомоморфизм, теорема об изоморфизме.

Авторы курса:

Трифанов А.И. Москаленко М. А.

Ссылка на ресурсы:
mathdep.ifmo.ru/geolin

3.1 Подгруппа и смежные классы

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 3.1. Пусть $\sigma \in \hom(G, G')$, тогда $\ker\sigma \leq G$ и $\operatorname{Im}\sigma \leq G'$.

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

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

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 3.1. *Пусть G - группа и $H \leq G$. Тогда отношением эквивалентности является*

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

►
Проверим свойства:

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

◄

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

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

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

Лемма 3.2. *Смежные классы, Hx и Hy, имеющие хотя бы один общий элемент, совпадают.*

►

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

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

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 мальтипликативную, 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:

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

3.2 Нормальная подгруппа

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 3.3. *Пусть $\sigma \in \hom(G, G')$, тогда $\ker\sigma \triangleleft G$.*

►

Пусть $H = \ker\sigma$, тогда

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

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

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

◄

Лемма 3.4. *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

3.3 Теорема об изоморфизме

Лемма 3.5. *Пусть $H \triangleleft G$, тогда существует такой гомоморфизм φ (называемый каноническим), что $\ker \varphi = H$.*

▶

Рассмотрим отображение

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

и прямой проверкой убеждаемся, что

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

◀

Теорема 3.1. *(Об изоморфизме) Пусть $\sigma : G \to G'$ - гомоморфизм групп, тогда*

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

▶

Зададим отображение $\bar{\sigma} : G/\ker \sigma \to \operatorname{Im} \sigma$

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

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

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

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

◀

Лекция 4

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, аксиомы кольца, основные примеры колец, гомоморфизм колец, образ кольца, подкольцо, ядро кольцевого гомоморфизма.

Авторы курса:

Трифанов А.И. Москаленко М.А.

Ссылка на ресурсы:
mathdep.ifmo.ru/geolin

4.1 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 4.1. 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 $\circ$.

4.2 Определение кольца

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:

$$\forall x \in R \quad \exists\, (-x) : \quad x + (-1) = 0 = (-x) + x.$$

M1. Асоциативность 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 4.2. 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:

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

3. Кольцо доичных дробей:

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

4. Пифагорово кольцо:

$$\mathbb{Z}[\sqrt{2}] = \left\{x + \sqrt{2}y : \quad x, y \in \mathbb{Z}\right\} \tag{4.1}$$

5. Гауссово кольцо:

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

6. Кольцо многочленов над Z от одного или нескольких параметров:

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

7. Кольцо матриц - пример некоммутативного кольца.

4.3 Гомоморфизмы колец

Пусть R и R' - кольца. **Гомоморфизмом колец** называется отображение $f : R \to R'$, 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:

$$f(1_R) = 1_{R'}.$$

Nota bene Таким образом, гомоморфизм колец является гомоморфизмом абелевых групп $(R, +)$ и $(R', +)$, а также мультипликативных моноидов $(R, \cdot)$ и $(R', \cdot)$.

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

Nota bene Тот факт, что S является подкольцом в R обозначают $S \leqslant R$.

Лемма 4.1. *Образ* $\operatorname{Im} f$ *гомоморфизма* $f \in \operatorname{Hom}(R, R')$ *является подкольцом в* R'*:*

$$\operatorname{Im} f \leqslant R'.$$

Лемма 4.2. *Ядро* $\ker f$ *гомоморфизма* $f \in \operatorname{Hom}(R, R')$ *имеет следующие свойства:*

1. *является нормальной подгруппой:* $\ker f \trianglelefteq (R, +)$;
2. *обладает поглощением:* $\forall x \in R, \quad \forall y \in \ker f \quad x \cdot y \in \ker f$.

Пример 4.3. Приведем пример подмножества L кольца R, являющееся кольцом, но при этом подкольцом R не являющееся. Пусть

$$L = \mathbb{Z}, \quad R = \mathbb{Z} \times \mathbb{Z}.$$

Имеет место вложение $\mathbb{Z} \hookrightarrow \mathbb{Z} \times \mathbb{Z}$:

$$x \mapsto (x, 0).$$

Теперь остается заметить, что образом $1_L \in \mathbb{Z}$ является $(1, 0)$, тогда как $1_R = (1, 1)$.

δ

Лекция 5

Идеал, фактор-кольцо, поле

Содержание лекции:
В настоящей лекции мы продолжаем изучать структуру кольца и вводим центральные понятия его подструктуры - идеала и классов вычетов по модулю. Мы также определим некоторые свойства элементов кольца и, в конце, обсудим важнейший класс колец - поля.

Ключевые слова:
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

5.1 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 5.1. 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

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

Лемма 5.1. *Пусть $J \triangleleft R$, тогда следующее отношение является отношением эквивалентности на R:*

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

►
Утверждение следует из прямой проверки свойств:

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

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

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

◄

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

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

Лемма 5.2. *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. $\bar{x} + \bar{y} = (x + J) + (y + J) = (x + y) + J = \overline{x + y}$,
2. $\bar{x} \cdot \bar{y} = (x + J) \cdot (y + J) = xy + J = \overline{xy}$,
3. $\bar{0} \cdot \bar{x} = J \cdot (x + J) = J = \bar{0}$.

◄

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

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

является гомоморфизмом, который называется **каноническим**.

Пример 5.2. Элементами фактор-кольца $\mathbb{Z}/(m) \triangleq \mathbb{Z}/m\mathbb{Z}$ являются *классы вычетов по модулю* m:

$$\begin{gathered}\bar{0} = \{x \in \mathbb{Z} : \quad x = 0 \bmod(m)\}, \\ \bar{1} = \{x \in \mathbb{Z} : \quad x = 1 \bmod(m)\}, \\ \cdots\cdots\cdots \\ \overline{m-1} = \{x \in \mathbb{Z} : \quad x = (m-1) \bmod(m)\}.\end{gathered}$$

Лемма 5.3. *Пусть $f : R \to R'$ - гомоморфизм колец, тогда*

$$A/\ker f \simeq \operatorname{Im} f.$$

▶
Утверждение следует из биективности и линейности отображения:

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

◀

5.2 Делители нуля. Нильпотенты

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

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

Пример 5.3. 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 5.4. Областями целостности являются кольца $\mathbb{Z}$ и $\mathbb{Z}/p\mathbb{Z}$, где p - простое.

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

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

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

5.3 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 5.4. *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 5.5. *Имеет место эквивалентность:*

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

Полем называется ненулевое кольцо, в котором каждый ненулевой элемент обратим.

Лемма 5.6. *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.

Теорема 5.1. *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 $(1) = (x) \subseteq J \quad \Rightarrow \quad J = (1)$.

- (2) $\Rightarrow$ (3):
  Пусть $f : R \to B$ - кольцевой гомоморфизм. Тогда

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

  откуда следует инъективность.

- (3) $\Rightarrow$ (1)
  Пусть $x \notin R^*$, тогда

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

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

◀

δ

Лекция 6

Поле комплексных чисел

Содержание лекции:
В данной лекции мы которотко рассмотрим поле комплексных чисел, которое возникает как алгебраичекое замыкание поля $\mathbb{R}$. Обсуждая алгбраические 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

6.1 Определение 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:

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

Nota bene Имеет место свойство

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

Теорема 6.1. *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 непостредственно:
$$((a_1, b_1) \cdot (a_2, b_2)) \cdot (a_3, c_3) = (a_1, b_1) \cdot ((a_2, b_2) \cdot (a_3, c_3)).$$
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 6.1. *Отображение $\sigma : \mathbb{R} \to \mathbb{C}$, заданное формулой $\sigma(a) = (a, 0)$ является вложением $\mathbb{R}$ в $\mathbb{C}$.*

►

Покажем, что σ - гомоморфизм:

$$\sigma(a+b) = (a+b, 0) = (a, 0) + (b, 0) = \sigma(a) + \sigma(b),$$
$$\sigma(ab) = (ab, 0) = (a, 0) \cdot (b, 0) = \sigma(a) \cdot \sigma(b).$$

Далее σ инъективно:

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

Следовательно σ - вложение.

◄

6.2 Алгебраическая форма КЧ

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 6.2. *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.

6.3 Тригонометрическая форма КЧ

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 6.3. *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 6.2. *(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 6.1. 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

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

И значит

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

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

Лемма 6.4. *Множество корней уравнения* $z^n = 1$ *образует мультипликативную абелеву группу.*

▶

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

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

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 7

Начала 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

7.1 Основные определения

Nota bene Пусть $\Bbbk$ - некоторое поле.

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

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots,$$

в которой отличны от нуля только *некоторые* **коэффициенты** $a_0, a_1, a_2, \ldots \in \Bbbk$, а x называется **формальной переменной**.

Nota bene Множество многочленов от переменной x будем обозначать через $\Bbbk[x]$. Пусть далее $p, q \in \Bbbk[x]$, так что

$$p(x) = \sum_{n=0}^{\infty} a_n x^n, \quad q(x) = \sum_{m=0}^{\infty} b_m x^m,$$

Суммой двух многочленов p и q называется такой многочлен $h = p + q$, что

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

Произведением двух многочленов p и q называется такой многочлен $g = p \cdot q$, что

$$g(x) = \sum_{j=0}^{\infty} d_j x^j, \quad d_j = \sum_{i=0}^{j} a_i b_{j-i}.$$

Теорема 7.1. *Множество $\Bbbk[x]$, наделенное операциями сложения и умножения является коммутативным ассоциативным кольцом.*

►

Проверим аксиомы кольца:

- $(\Bbbk[x], +)$ - абелева группа, в которой
$$0(x) = 0, \quad (-p)(x) = -p(x).$$
- $(\Bbbk[x], \cdot)$ - коммутативный моноид, в котором $1(x) = 1$.
- Пусть $p, q, r \in \Bbbk[x]$, проверим дистрибутивность:
$$(p+q) \cdot r = \sum_{k=0} d_k x^k, \quad p \cdot r = \sum_{n=0} \alpha_n x^n, \quad q \cdot r = \sum_{m=0} \beta_m x^m.$$
тогда имеет место
$$d_k = \sum_{i=0}^{k} (a_i + b_i) c_{k-i} = \sum_{i=0}^{k} (a_i c_{k-i}) + \sum_{i=0}^{k} (b_i c_{k-i}) = \alpha_k + \beta_k,$$

◄

Лемма 7.1. *Отображение $\sigma : \Bbbk \to \Bbbk[x]$, так что $\alpha \mapsto \alpha \cdot 1(x)$, является вложением.*

►
Очевидно, что $\sigma \in \mathrm{Hom}(\Bbbk, \Bbbk[x])$ и далее

$$\alpha \in \ker \sigma \quad \Rightarrow \quad \sigma(\alpha) = \alpha \cdot 1(x) = \alpha \cdot 1 + 0 \cdot x + \ldots = 0.$$

◄

Nota bene Под записью $\alpha \cdot p(x), \alpha \in \Bbbk$ понимают многочлен $\sigma(\alpha) \cdot p(x)$.

Два многочлена p и q называются **ассоциированными** (обозначают $p \sim q$), если

$$\exists\, \alpha \in \Bbbk, \quad \alpha \neq 0 : \quad p = \alpha \cdot q.$$

Лемма 7.2. *Ассоциированность - отношение эквивалентности.*

Nota bene Классы в $\Bbbk[x]/_\sim$ по этому отношению составляют многочлены, отличающиеся на скалярный множитель.

7.2 Степень многочлена

Степенью $\deg(p)$ многочлена $p \in \Bbbk[x]$ называется максимальный номер его ненулевого коэффициента. Если $\deg p = n \in \mathbb{N}_0$ то коэффициент a_n называется **старшим коэффициентом** многочлена p.

Nota bene Для нулевого многочлена $0(x)$ положим $\deg(0) = -\infty$.

Лемма 7.3. *Пусть $p, q \in \Bbbk[t]$ тогда имеют место следующие свойства:*

$$\deg(p \cdot q) = \deg(p) + \deg(q), \quad \deg(p+q) \leq \max\{\deg(p), \deg(q)\}.$$

►
Пусть $\deg(p) = n$ и $\deg(q) = m$, и при этом

$$p = \sum_i a_i x^i, \quad q = \sum_j b_j x^j, \quad p \cdot q = \sum_k c_k x^k,$$

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, $\deg(p \cdot q) = n+m$.
При $k > \max\{\deg(p), \deg(q)\}$ следует доказательство второго свойства:

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

◄

7.3 Делимость в кольце многочленов

Теорема 7.2. *Пусть $p, q \in \Bbbk[x]$, причем $q \neq 0$, тогда*

$$\exists!\, g, r \in \Bbbk[x]: \quad p = g \cdot q + r, \quad \deg(r) < \deg(q).$$

▶
Пусть $\deg(p) = n$ и $\deg(q) = m$, а также

$$p(x) = a_n x^n + \ldots + a_0, \quad q(x) = b_m x^m + \ldots + b_0.$$

Используем индукцию по n. В качестве базы при $n < m$ подходит $g = 0, \quad r = p$. Пусть теперь $n \geq m$ и для многочленов степени меньшей n утверждеие доказано. Так как

$$\tilde{p}(x) = p(x) - \frac{a_n}{b_m} x^{n-m} q(x), \quad \deg(\tilde{p}) < n,$$

то по индукционному предположению

$$\tilde{p} = g_1 \cdot q + r, \quad \deg(r) < m \quad \Rightarrow \quad p(x) = \left(g_1(x) + \frac{a_n}{b_m} x^{n-m} \right) q(x) + r(x).$$

Теперь докажем единственность. Пусть

$$g_1 q + r_1 = p = g_2 q + r_2, \quad \deg(r_1) < m, \quad \deg(r_2) < m \quad \Rightarrow \quad r_1 - r_2 = q \cdot (g_2 - g_1).$$

При $g_1 \neq g_2$, имеем:

$$\deg\left((g_2 - g_1)q\right) = \deg(g_2 - g_1) + \deg(q) \geq m,$$
$$\deg(r_1 - r_2) \leq \max\left(\deg(r_1), \deg(r_2)\right) < m.$$

Противоречие. Значит $g_1 = g_2$ и $r_1 = r_2$.
◀

Говорят, что многочлен q **делит многочлен** p (пишут $q \,|\, p$), если существует такой многочлен h, что $p = h \cdot q$.

Лемма 7.4. *Свойства делимости в $\Bbbk[x]$:*

1. *Если $q \,|\, p$ и $r \,|\, q$, тогда $r \,|\, p$:*
$$f = pg, \quad g = qh \quad \Rightarrow \quad f = (pq)h.$$
2. *Пусть $r \,|\, p, q$, тогда $\quad \forall g_1, g_2 \in \Bbbk[t] \quad r \,|\, (g_1 p + g_2 q)$:*
$$p = \alpha \cdot r, \quad q = \beta \cdot r, \quad \alpha, \beta \in \Bbbk[x] \quad \Rightarrow \quad g_1 p + g_2 q = (\alpha \cdot g_1 + \beta \cdot g_2) \cdot r.$$
3. *Пусть $q \,|\, p$, причем $p, q \neq 0$, тогда $\deg(p) \geq \deg(q)$:*
$$p = gq, \quad g \in \Bbbk[t], \quad g \neq 0 \quad \Rightarrow \quad \deg(p) = \deg(g) + \deg(q) \geq \deg(g).$$

Лемма 7.5. *Ассоциированность и делимость:*

1. *Пусть $q \,|\, p, \quad p, q \neq 0$ и $\deg(p) = \deg(q)$, тогда $p \sim q$:*
$$\deg(q) = \deg(p) = \deg(g) + \deg(q) \quad \Rightarrow \quad \deg(g) = 0 \quad \Rightarrow \quad g \in \Bbbk.$$
2. *Пусть $q \,|\, p, \quad p, q \neq 0$ и $p \,|\, q$, тогда $p \sim q$:*
$$\deg(p) \geq \deg(q), \quad \deg(q) \geq \deg(p) \quad \Rightarrow \quad \deg(p) = \deg(q).$$

7.4 Корень многочлена

Пусть $p \in \Bbbk[x]$ и $\alpha \in \Bbbk$. Число α называется **корнем** многочлена p степени m, если

$$(x-\alpha)^m \mid (p(x), \quad (x-\alpha)^{m+1} \nmid p(x).$$

Теорема 7.3. *(Безу) Остаток от деления $p \in \Bbbk[x]$ на $(x-\alpha)$ равен $p(\alpha)$*

►

По теореме от делении с остатком имеем:

$$p(x) = (x-\alpha)g(x) + r(x), \quad \deg(r) \leq \deg(x-\alpha) = 1.$$

Следовательно, $r(x) = r \in \Bbbk$ и

$$p(\alpha) = 0 \cdot g(\alpha) + r.$$

◄

Nota bene Если $p \in \Bbbk[x]$ и α - корень $p(x)$, тогда $(x-\alpha) \mid p(x)$.

Теорема 7.4. *(ОТАр) Любой многочлен из $\mathbb{C}[x]$ имеет корень из $\mathbb{C}$.*

η

Лекция 8

Матрицы и определители

Содержание лекции:
В настоящей лекции мы начинаем рассматривать один из основных обьектов 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

8.1 Определения

Матрицей договоримся называть прямоугольную таблицу, составленную из элементов некоторого поля $\mathbb{k}$:

$$A_{m\times n} = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & a_{2,3} & \dots & a_{2,n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{m,1} & a_{m,2} & a_{m_3} & \dots & a_{m,n} \end{pmatrix}, \quad a_{ij} \in \mathbb{k},$$

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 *прямоугольных* $m \times n$ матриц с элементами из поля $\mathbb{k}$ будем обозначать $\mathrm{Mat}_{\mathbb{k}}(m, n)$.

Суммой матриц A и B, где $A, B \in \mathrm{Mat}_{\mathbb{k}}(m, n)$ называется матрица $C = A + B$, $C \in \mathrm{Mat}_{\mathbb{k}}(m, n)$ такая что:

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

Лемма 8.1. *Относительно операции сложения* $\mathrm{Mat}_{\mathbb{k}}(m, n)$ *- 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 $A \in \mathrm{Mat}_{\mathbb{k}}(m, p)$ и $B \in \mathrm{Mat}_{\mathbb{k}}(p, n)$ называется матрица $C = A \cdot B$, $C \in \mathrm{Mat}_{\mathbb{k}}(m, n)$, 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 8.2. *Операция умножения матриц ассоциативна и некоммутативна.*

8.2 Специальные виды матриц

Единичной матрицей $E \in \mathrm{Mat}_{\Bbbk}(m,n)$ 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 $A \in \mathrm{Mat}_{\Bbbk}(m,p)$, $B \in \mathrm{Mat}_{\Bbbk}(p,n)$ и $E \in \mathrm{Mat}_{\Bbbk}(p,p)$, тогда

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

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

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

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

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

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

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

Лемма 8.3. *На множестве квадратных матриц* $\mathrm{Mat}_{\Bbbk}(n)$ *операция умножения индуцирует структуру некоммутативного моноида.*

Теорема 8.1. *Операции сложения и умножения индуцируют на множестве квадратных матриц* $\mathrm{Mat}_{\Bbbk}(n,n)$ *структуру ассоциативного некоммутативного кольца.*

Пример 8.1. Приведем пример одного интересного изоморфизма. Рассмотрим множество комплексных чисел $\mathbb{C}$ и подмножество в $\mathrm{Mat}_{\mathbb{R}}(2)$ вещественных квадратных матриц вида:

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

Пусть $\sigma : \mathbb{C} \to \mathrm{Mat}_{\mathbb{R}}(2)$ - 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.

8.3 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 8.4. *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 (E3) 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 $A \in \mathrm{Mat}_{\Bbbk}(n, m)$ называется операция $A \mapsto A^T$ в результате которой получается матрица со следующим свойством:

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

Лемма 8.5. *Имеет место свойство:*

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

Теорема 8.2. *(критерий обратимости матрицы)*

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

θ

Лекция 9

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, кожффициенты 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

9.1 Основные определения

Линейным алгебраическим уравнением с неизвестными $x_1, x_2, \ldots, x_n$ над полем $\Bbbk$ называется уравнение вида

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b, \tag{9.1}$$

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

Решением линейного алгебраического уравнения называется упорядоченный набор чисел $y_1, y_2, \ldots, y_n \in \Bbbk$, который будучи подставленным в линейное уравнение (9.1) превращает его в тождество.

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

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \ldots a_{1,n}x_n = b_1, \\ a_{2,1}x_1 + a_{2,2}x_2 + \ldots a_{2,n}x_n = b_2, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots, \\ a_{m,1}x_1 + a_{m,2}x_2 + \ldots a_{m,n}x_n = b_m. \end{cases} \tag{9.2}$$

Решением системы линейных алгебраических уравнений (9.2) называется упорядоченный набор чисел $z_1, z_2, \ldots, z_n$, 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 (9.2) 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 9.1. *Отношение $\sim$ является отношением эквивалентности на $\mathcal{S}_n^m$.*

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

9.2 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 9.2. *В результате элементарных преобразований любая система S переходит в эквивалентную ей систему S'.*

Матрицей системы алгебраических уравнений называется матрица S системы (9.2), 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 9.3. *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 9.1. *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.

9.3 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 (9.2) можно записать в виде

$$A \cdot X = B. \tag{9.3}$$

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

$$U \cdot A \cdot X = U \cdot X, \tag{9.4}$$

и всякое решение (9.3) является также решением (9.4).

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 9.4. *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 9.5. *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 (9.3) слева на элементарные матрицы с целью приведения матрицы S к ступенчатому виду.

Лекция 10

Модуль над кольцом

Содержание лекции:
Настоящей лекцией мы вплотную приближаемся к центральному разделу нашего курса - линейным пространствам. Здесь мы обсудим понятие внешнего закона, дадим определение алгебраической структуры, а также сформулируем самые основные определения, связанные с линенми пространствами и их отображениями.

Ключевые слова:
Внешний закон композиции, оператор закона, согласованность закона со структурой, действие на структуре, алгебраическая структура, модуль над кольцом, левый (правый) R-модуль, линейное отображение, мономорфизм, эпиморфизм, ядро и образ линейного отображения, подмодуль, фактор модуль, коядро.

Авторы курса:

Трифанов А. И. Москаленко М. А.

Ссылка на ресурсы:
mathdep.ifmo.ru/geolin

10.1 Согласованное действие

Nota bene Напомним, что внешний закон композиции называется согласованным с внутренним законом, если

$$\forall x, y \in M, \quad \alpha \in \Omega, \quad \alpha\,(x \circ y) = \alpha(x) \circ \alpha(y).$$

Говорят, что алгебраическая структура Ω **действует на** алгебраической структуре M, если каждый элемент $\alpha \in \Omega$ является оператором внешнего закона на M и для любой пары элементов из $\alpha, \beta \in \Omega$ имеет место согласованное действие:

$$(\alpha * \beta)(x) = \alpha(\beta(x)), \quad \forall x \in M.$$

Говорят, что имеет место **согласованное действие** Ω на M, если

$$(\alpha * \beta)\,(x \circ y) = \alpha\,(\beta\,(x \circ y)) = \alpha\,(\beta x \circ \beta y) = \alpha\,(\beta x) \circ \alpha\,(\beta y)\,.$$

Пример 10.1. Внешний закон композиции, описанный в предыдущем примере согласован со структурой коммутативной группы $(\mathbb{Z},' +')$:

$$n(z_1 + z_2) = nz_1 + nz_2.$$

Если при этом множество $\mathbb{N}$ обладает алгебраической структурой мультипликативного моноида $(\mathbb{N},' \cdot')$, Тогда

$$(n \cdot m)(z_1 + z_2) = nmz_1 + nmz_2.$$

Алгебраической структурой на множестве M называется всякая структура, определяемая в M одним или несколькими внутренними законами композиции элементов из M и одним или несколькими внешними законами композиции из областей операторов $\Omega_1, \Omega_2, \ldots, \Omega_k$, согласованных с внутренними законами.

Пример 10.2. Рассмотрим алфавит $A = \{p, q\}$ и множество L всех формальных сумм элементов A с коммутативной операцией "+". Тогда произвольный элемент L имеет вид

$$p + p + \ldots + p + q + \ldots + q$$

Пусть $\mathbb{Z}$ множество операторов внешнего закона на L, согласованных с внутренним законом L:

$$n(p + q) = np + nq, n \in Z,$$
$$(n + m)(p + q) = n(p + q) + m(p + q),$$
$$(nm)p = n(mp).$$

Множество комбинаций L, наделенное алгебраической структурой коммутативного внутреннего закона и внешнего закона с множеством операторов из кольца $\mathbb{Z}$ называется **модулем над кольцом**.

10.2 Модуль над кольцом

Левым R-модулем (или левым модулем над кольцом R) называется абелева группа $(G,+)$ с заданной бинарной операцией $R\times G\to G$, записываемой как $(\alpha,x)\to\alpha x$ и согласованной действующей на групповой структуре на G:

L1. Действие кольца группе:

$$\forall\alpha,\beta\in R,\quad \forall x\in G$$
$$(\alpha+\beta)x=\alpha x+\beta x,\quad (\alpha\beta)x=\alpha(\beta x).$$

L2. Согласованное действие:

$$\forall\alpha\in R,\quad \forall x_1,x_2\in G\quad \alpha(x_1+x_2)=\alpha x_1+\alpha x_2$$

Nota bene Аналогично можно определить структуру **правого** R-модуля, если определена бинарная операция

$$G\times R\to G,\quad (x,\alpha)\mapsto x\alpha.$$

Если определены оба отображения, то говорят о **двустороннем** R-модуле.

Пример 10.3. Примеры R-модулей:

- Всякий $J\trianglelefteq R$ - идеал кольца R есть R-модуль.
- Любая абелева группа $(G,+)$ представляет собой $\mathbb{Z}$ - модуль, ибо

$$\forall x\in G\quad x+x+x+\ldots+x=zx,\quad z\in\mathbb{Z}.$$

- Пусть $\Bbbk$-поле, тогда структру модуля имеет $\Bbbk^n$ - множество столбиков вида

$$\xi=\left(\xi^1,\xi^2,\ldots,\xi^n\right)',\quad \xi^i\in\Bbbk.$$

Гомоморфизмом R-модулей X и Y (или R-линейным отображением) называется отображение $\sigma: X\to Y$, такое что:

$$\forall x,x_1,x_2\in X,\quad \forall\alpha\in R$$
$$\sigma(x_1+x_2)=\sigma(x_1)+\sigma(x_2),\quad \sigma(\alpha x)=\sigma(x)\alpha.$$

Nota bene Для множества R-линейных отображений между X и Y используют следующее обозначение $\mathrm{Hom}_R(X,Y)$.

Ядром линейного отображения $\sigma \in \mathrm{Hom}_R(X, Y)$ называется подмножество X, такое что:

$$\ker \sigma = \{x \in X : \quad \sigma(x) = 0\}$$

Лемма 10.1. *Ядро* $\ker \sigma$ *- модуль над кольцом.*

Образом линейного отображения $\sigma \in \mathrm{Hom}_R(X, Y)$ называется подмножество Y, такое что:

$$\mathrm{Im} = \{y \in Y : \quad \exists x \in X \quad \sigma(x) = y\} = \sigma(X).$$

Лемма 10.2. *Образ* $\mathrm{Im}\,\sigma$ *- модуль над кольцом.*

10.3 Подмодуль. Фактор-модуль

(1) Подмножество $L \subseteq X$ называется **подмодулем** R-модуля X, если L замкнуто относительно операций, индуцированных из X.

(2) Подмножество $L \subseteq X$ называется **подмодулем** R-модуля X, если L само является R-модулем относительно операций, индуцированных из X.

Лемма 10.3. *Определения (1) и (2) равносильны.*

Пример 10.4. Примеры подмодулей:

- Ядро линейного отображения $\sigma \in \mathrm{Hom}_R(X, Y)$ является подмодулем в X;
- Образ линейного отображения $\sigma \in \mathrm{Hom}_R(X, Y)$ является подмодулем в Y;
- Идеал $J \trianglelefteq R$ явлеяется подмодулем R-модуля R;
- Подмножество $\Bbbk^n$ столбиков ξ, у которых первый элемент $\xi^1 = 0$.

Nota bene На фактор группу X/L переносится структура R-модуля, если умножение определить формулой:

$$\alpha(x + L) = \alpha x + L, \quad \forall x \in X.$$

R-модуль X/L называется **фактор-модулем** X по L.

Коядром гомоморфизма $\sigma \in \mathrm{Hom}_R(X, Y)$ называется множество

$$\mathrm{Coker}\,\sigma = Y/\,\mathrm{Im}\,\sigma.$$

Лемма 10.4. *Коядро является фактор-модулем* Y*.*

Теорема 10.1. *Имеет место изоморфизм* R*-модулей:*

$$X/\ker \sigma \simeq \mathrm{Im}\,\sigma.$$