

3. Модули над кольцами главных идеалов

Опр 1 Пусть A - ассоц. кольцо с 1.

(Правым) **модулем над кольцом A (A -модулем)**

называется абелева группа M с операцией умножения (справа) на элементы кольца A со след. свойствами:

$$1) (x+y)a = xa + ya \quad \forall x, y \in M \quad \forall a \in A$$

$$2) x(a+b) = xa + xb \quad \forall x \in M \quad \forall a, b \in A$$

$$3) x(ab) = (xa)b \quad \forall x \in M \quad \forall a, b \in A$$

$$4) x1 = x \quad \forall x \in M \quad (1 - \text{единица кольца } A).$$

Аналогично определяется **левый A -модуль**, в этом случае используется умножение на m -ти из A слева

В случае, когда A -коммутативно, различия нет. Левый и правый модули не.

Примеры 1) Аддитивная группа в.п. V над полем F — F -модуль (левый и правый)

2) Любая абелева группа \mathbb{Z} -модуль

3) Кольцо A (точнее его аддитивная группа) — модуль над самим собой, называемый **регулярным**.

4) Аддитивная группа в.п. V — модуль над кольцом $L(V)$ — всех л.л. ир. в V .

5) Если M - абелевская группа, то $\text{мн-во } A = \text{End}(M) = \text{Hom}(M, M)$ всех гом-измов из M в M образует кольцо (ассоц. и с 1) относительно операций сложения $\chi(\varphi + \psi) = \chi\varphi + \chi\psi$ и композиции $\chi(\varphi\psi) = (\chi\varphi)\psi$. Легко проверить, что M - A -модуль.

6) Пусть $F[t]$ - кольцо мн-ков от одной переменной над полем t , V - в.ч. над полем F , $\varphi \in L(V)$. Положим $\chi f(t) = \chi f(\varphi)$, т.е. в частности $\chi \cdot t = \chi\varphi$. Тогда аддитивная группа V - это $F[t]$ -модуль.

Обратно, если M -некоторый $F[t]$ -модуль, то всякую определенную модулем M -в.и. над F (рассмотрите умножение на скалярах), пр-е пр-ва $M \ni x \mapsto xt, x \in M$, явл-ся линейным, т.е. к-л. н-с-т $F[t]$ -модуль-ю в.и. над F с фикс. линейным оператором, играющим роль умножения на t .

Изучение модулей над кольцом A очень полезно, в частности, для изучения свойств кольца A , как изучение разл. действий групп G на разл. мн-вах Σ , сравн с опр. 9.6. [из [Вн]]

Опр 2 Подмодуль N модуля M над кольцом A наз-ся **поглощающим**, если N — подгруппа в M , замкнутая относительно умножения на эл-ты кольца A .

Предл 1 Подмодуль A -модуля — сам A -модуль.

В вышеприв. примерах: 1) подмодуль = подгруппа
2) подмодуль = подгруппа 3) подмодуль = идеал
6) Если $\varphi \in \mathcal{L}(V)$: $x \mapsto x\varphi$, то подмодуль
= φ -инв. подгруппа.

Зад 1 Доказать, что в примере 4 0 и V — единств. подмодули.

Верно ли аналогичное утв-е в примере 5?

Предл 2 Если N — нормальная A -подгруппа M , то

$(x + N)a = x\alpha_i + N \quad \forall x \in M, a \in A$. В частности, факторгруппа M/N явл-ся A -модулем.

Опр 3 Модуль M/N — **фактормодуль** модуля M по нормальной N .

Опр 4 Если M, N — модули из кольца A . От-е

$\varphi: M \rightarrow N$ — **гомо-ом (гомоморфизм)**, если

$$(x + y)\varphi = x\varphi + y\varphi \quad \text{и} \quad (xa)\varphi = (x\varphi)a \quad \forall x, y \in M, \forall a \in A.$$

Если N — нормальная в M , то $\pi: M \rightarrow M/N, x \mapsto x + N$ — канонический гом-ом.

Т. 1 (о том-же модуле) Ф-ка имеет на отл.
от ф-к для колец (см. также т. 9.3.1 из [Вик]).

Опр 5 Пусть M — A -модуль, $S \subseteq M$. МН-во
 $\langle S \rangle = \{ x_1 a_1 + \dots + x_s a_s, x_i \in S, a_i \in A, s \in \mathbb{N} \}$
наз-ся наим. подмодулем в M , сод. S , и наз-ся
подмодулем, **порожденным** МН-вом S .
Если $\langle S \rangle = M$, то M **порождается** МН-вом S , а
 S — **система порождающих** модуля M . Модуль,
имеющий конечную систему порождающих, наз-ся
конечно порождаемым. Модуль, порожд. одним
эл-том, наз-ся **циклическим**.

Препр 3 Подмодуль-во $\text{Ann } M = \{a \in A : Ma = 0\} \subseteq A$.

Опр 6 $\text{Ann } M$ — **аннулятор** модуля M (в кольце A).

Если $\text{Ann } M \neq 0$, то M — **периодический** модуль.

Пример НОК порядков n -ов группы (если он есть) называется **экспонентой** (или **периодом**).

Если M — адельеве группа, рассм. как \mathbb{Z} -модуль, то $\text{Ann } M = (n\mathbb{Z})$, где n — экспонента M .

Т. 2 Канонич. суж. (правый) A -модуль изоморфен модулю вида A/I , где I — (правый) идеал кольца A . Если A коммутативно, то $I = \text{Ann } M$ и тем самым определен модулем M однозначно.

Лемма 1 Пусть $M = \langle x \rangle$. Тогда экв-е $\varphi: A \rightarrow M, a \mapsto xa$,
— гом-зм A -модулей, причём $\text{Im } \varphi = M$.


В силу л. 1 $A/I \cong M$, где $I = \text{Ker } \varphi$.

Пусть A — комм. Тогда M — циклический, т.е. $\forall y \in M \exists b \in A$:

$$y = xb. \text{ Если } A \in I = \text{Ker } \varphi, \text{ то } ya = (xb)a = \underset{\substack{\uparrow \\ \text{комм. в } A}}{(xa)b} = 0 \cdot b = 0. \quad \square$$

Опр 2 Система $\{x_1, \dots, x_n\}$ A -модуля M
наз-ся минимально независимой, если $x_1 a_1 + \dots + x_n a_n = 0$
 $\Rightarrow a_1 = \dots = a_n = 0 \quad \forall a_1, \dots, a_n \in A$. Если эта система
переносится в M , то она наз-ся **базисом** модуля M .
Комм. модуль M наз-ся **свободным**, если он обладает базисом.

Предл 4 Свободный уикл. A - могут изолироваться A .


Δ -во: Применить Т-му 2 

Всюду далее A - кольцо главных идеалов.

Заметим, что кольца в примерах 1), 2), 6) - кольца главных идеалов. (и даже евкл. кольца)

Т. 3 Все базисы свободного A -модуля L содержат одно и то же число эл-тов (они наз-ся **рангом** и обозн. $rk L$).

Δ -во: Если p - простой эл-т кольца A , то $F = A/(p)$ - поле по Т. 3 из $\beta 2$, $A/pA \cong A/pA$ - в.ч. над F . Если

e_1, \dots, e_n - базис L , то $e_1 + pA, \dots, e_n + pA$ - базис в.ч. $V \Rightarrow$
 $n = \dim V$ и не зависит от выбора базиса 

Т. 4 Если N -подмодуль своб. A -модуля L ранга n , то N -своб. модуль ранга $m \leq n$, причем существуют базис $\{e_1, \dots, e_n\}$ модуля L и такие ненулевые эл-ты u_1, \dots, u_m кольца A , что $\{e_1 u_1, \dots, e_m u_m\}$ - базис N и $u_i \mid u_{i+1}$ при $i=1, \dots, m-1$.

Δ -во. см. Δ -во Т. 9.3.4 из [ВАН],

изучим теперь свойства к.п. A -модулей.

Опр 8 К.п. A -модуль M наз-ся **примарным** (или **p -примарным**), если найдется такой простой эл-т $p \in A$, что $p^k \in \text{Ann } M$ для некот. $k \in \mathbb{N}$.

Т.к. A — коммут. кольцо, то по Т. 2 каждый цикл A -модуль M изоморфен либо A , либо $A/(n)$ где n — необр. ненуль. эл-т кольца A , эл-т n имеет единств. разложение $n = p_1^{k_1} \dots p_s^{k_s}$ в произведение простых (с точностью до обр. эл-та) В силу Т. 4 из § 2 имеет $A/(n) \cong A/(p_1^{k_1}) \oplus \dots \oplus A/(p_s^{k_s})$

⇒ Предл. 5 Первос. циклич. модуль есть прямая сумма простых циклич. модулей и порождается единицей с точностью до перест. слагаемых.

Т. 5 Каждый конечно порожд. A -модуль M разлагается в прямую сумму простых и свободных циклических модулей, причем набор annihilаторов этих

могут быть определены однозначно.

Л-ВО: канонично гом-изм. θ к. и. абелевых групп. Используя т. 4, имеем

$$M \cong L/N \cong A/(u_1) \oplus \oplus A/(u_m) \oplus \underbrace{A \oplus \dots \oplus A}_{n-m} \quad (*)$$

где $u_i | u_{i+1}$ $i = 1 \dots m-1$, причем число m

и u_1, \dots, u_m определены однозначно в силу леммы о приведении m -чл. к к. и. чл. виду (из некоторого т. изложения). Осталось принять предп. 5 ~~11~~.

ЗАД 2 Записать полное гом-во.

Как уже говорилось, n -ты u_1, \dots, u_n из кольца A ($\text{см } *$)
определяется (с точностью до ассоциированности,
т.е. умножения на обр. n -го) n -модуль M
однозначно. Они наз-ся **инвариантами**
модуля M . При этом у
последних из них есть простой смысл.

Предл 6 Если M — периодический, то $(u_n) = \text{Ann } M$.

Следствие Экспонента конечной абелевой группы G
равна её последней инв. n -лю u_n (здесь G
— \mathbb{Z} -модуль). Кон. абелева группа циклическая \Leftrightarrow
её порядок и экспонента совпадают.

Зад 3 Δ -те следствие.

Т.6 Любая конечная подгруппа мультипликативной группы поля (в частности, мультипл. группа любого конечного поля) явл.ся циклической.

Д-во: Пусть экспонента подг. G в F^* равна m .

Тогда $g^m = 1 \quad \forall g \in G$. Ур-е $x^m = 1$ имеет не более m решений в поле $F \Rightarrow |G| \leq m$
 $\Rightarrow |G| = m$. По следствию G -циклическая.

Посмотрим теперь, что развоятся измн. Теория
означает для примера G из начала параграфа.

Пусть φ — л.н. к.м. в.н. V над полем F . Тогда
 $A = F[t]$. Рассмотрим V как A -модуль, порождая
 $x \cdot t = x\varphi \quad \forall x \in V$, откуда $x f(t) = x f(\varphi) \quad \forall f \in A$.
 Т.к. $\dim V = n < \infty$, то V — к.н. модуль. Применим
 к нему л. 5. Заметим, что в разложении (*)
 не может быть свобод. цикл. модулей, т.е. $m=n$,
 т.к. $A = F[t]$ имеет беск. размерности над F .
 Предположим, что F алг. замкнута. Тогда
 простые n -ик в A — это линейные m -ик
 вида \Rightarrow M есть прямая сумма примарных
 цикл. модулей вида $\bar{W} = A/(u)$, где $u = (t - \lambda)^m$, $\lambda \in F$.

Модуль W — m -мерное векторное \mathbb{C} -во $\mathbb{C}[t]$

с базисом $\{1 + (u), (t - \lambda) + (u), \dots, (t - \lambda)^{m-1} + (u)\}$

Отн-но умножению $t - \lambda$ — это ниль-сод!

Поэтому в этом базисе умножение на t
(т.е. действие оператора φ) записывается матрицей

$$\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & 1 & \\ & 0 & \ddots & 1 \\ & & & \lambda \end{pmatrix}, \text{ т.е. морз. клетки,}$$

Таким образом, T -м в морз. форме
(и её единственность с точностью до перестановки
морз. клеток) есть прямое сложение T -м B .

Посмотреть также на представление (*) в этом случае $V \cong A/(u_1) \oplus \dots \oplus A/(u_n)$ (здесь $n=m$!).

Поскольку $(u_n) = \text{Ann}(V) = (g(t))$, где $g(t)$ — мин. мн-н такой, что $tg(t) = 0 \quad \forall x \in V$, то $u_n = g(t)$ — мин. аннул. мн-н. При этом, этот факт не зависит от того два-ся ли поле F алгебр. Замкнутом или нет. В частности, это дает уточнение т. о мин. о мин. аннул. много-члене (см. т. 6.7.1 из [ВМ]).

Зад 4. Покажите, что харак. мн-н $f_F(t)$ — мин.
пр. 8 φ — это $\prod_{i=1}^n u_i$.

Пример. Пусть V -в.н. к-во \mathbb{C} , $\dim V = 2$ и $\varphi \in \mathcal{L}(V)$;

$[\varphi] = A = \begin{pmatrix} 3 & 1 \\ -1 & 1 \end{pmatrix}$ в нек-ой базисе. Найти ж.ф. T и мин. анн. многочлен, и доказать T -му 5.

Т.к. $\chi_A = \chi_{\varphi}$, то $\chi(A - tE) = 0$. Приведем многоч $A - tE \in M_2(\mathbb{C}[t])$ к норм. форме Смита:

$$\begin{pmatrix} 3-t & 1 \\ -1 & 1-t \end{pmatrix} \rightarrow \begin{pmatrix} 1 & t-3 \\ 1-t & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & t-3 \\ 0 & (t-3)(t-1)+1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & (t-2)^2 \end{pmatrix} = \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix}$$

Получили 2-хар. корень кратности 2 гл.д. φ и мин. анн. мн-н $g(t) = u_2 = (t-2)^2 \Rightarrow T = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$.