# 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) $(x+y)a = xa + ya \quad \forall x, y \in M \ \forall a \in A$
2) $x(a+b) = xa + xb \quad \forall x \in M \ \forall a, b \in A$
3) $x(ab) = (xa)b \quad \forall x \in M \ \forall a, b \in A$
4) $x1 = x \quad \forall x \in M$ ($1$ - единица кольца $A$).

Аналогично определяется левый $A$-модуль, в этом случае используется умножение на эл-ты из $A$ слева.

В случае, когда $A$ — коммутативно, разницы между левыми и правыми модулями нет.

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 $\mathcal{L}(V)$ — всех лин. пр-й пр. за $V$.

5) Если $M$ - абелева группа, то мн-во $A = End(M) = Hom(M, M)$ всех гом-змов из $M$ в $M$ образует кольцо (ассоц. и с 1) отн-но операций сложения $x(\varphi+\psi) = x\varphi + x\psi$ и композиции $x(\varphi\psi) = (x\varphi)\psi$.

Легко проверить, что $M$ — $A$-модуль.

6) Пусть $F[t]$ - кольцо мн-нов от одной переменной над полем $t$, $V$ - в.п. над полем $F$, $\varphi \in \mathcal{L}(V)$. Положим $xf(t) = xf(\varphi)$, т.е. в частности $x \cdot t = x\varphi$. Тогда аддитивная группа $V$ — это $F[t]$-модуль.

Обратно, если $M$ - некоторый $F[t]$-модуль, то в силу определения модуля $M$ — в.п. над $F$ (рассмотрите умножение на скаляры), пр-е пр-ва $M$ $x \mapsto xt$, $x \in M$, явл-ся линейным, т.е. каждый $F[t]$-модуль — это в.п. 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 группы $G$ на разл. мн-вах $\Omega$, сравни с опр. 9.6. из [BM]

**Опр 2** Подмн-во $N$ модуля $M$ над кольцом $A$ наз-ся **подмодулем**, если $N$ – подгруппа в $M$, замкнутая отн-но умножения на эл-ты кольца $A$.

**Предл 1** Подмодуль $A$-модуля – сам $A$-модуль.

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

**Зад 1** Д-ть, что в примере 4 $0$ и $V$ – единств. подмодули. Верно ли аналогичное утв-е в примере 5?

**Предл 2** Если $N$ — подмодуль $A$-модуля $M$, то $a(x+N) = ax+N$ $\forall x \in M$, $a \in A$. В частности, факторгруппа $M/N$ явл-ся $A$-модулем.

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

**Опр 4** Пусть $M, N$ — модули над кольцом $A$. От-е $\varphi: M \to N$ — гом-зм (модулей), если $(x+y)\varphi = x\varphi + y\varphi$ и $(xa)\varphi = (x\varphi)a$ $\forall x,y \in M$ $\forall a \in A$.

---

Если $N$ — подмодуль в $M$, то $\pi: M \to M/N$, $x \mapsto x+N$ — канонический гом-зм.

<u>Т. 1</u> (о гом-зме модулей) Ф-ка ничем не отл. от ф-к для колец (см. также т. 9.3.1 из [ВиН]).

<u>Опр 5</u> Пусть $M$ — $A$-модуль, $S \subseteq M$. Мн-во $\langle S \rangle = \{x_1 a_1 + \ldots + x_s a_s,\ x_i \in S,\ a_i \in A,\ s \in \mathbb{N}\}$ явл-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 порожденным**. Модуль, порожд. одним эл-том, наз-ся **циклическим**.

**Предл 3** Подмн-во $\mathrm{Ann}\, M = \{a \in A : Ma = 0\} \trianglelefteq A$.

**Опр 6** $\mathrm{Ann}\, M$ — аннулятор модуля $M$ (в кольце $A$).
Если $\mathrm{Ann}\, M \neq 0$, то $M$ — периодический модуль.

**Пример** НОК порядков эл-тов группы (если он сущ.) наз-ся её экспонентой (или периодом).
Если $M$ - абелева группа, рассм. как $\mathbb{Z}$-модуль, то $\mathrm{Ann}\, M = (n\mathbb{Z})$, где $n$ ~~—~~ экспонента $M$.

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

$\underline{\text{Д-во}}$: Пусть $M = \langle x \rangle$. Тогда от-е $\varphi: A \to M$, $a \mapsto xa$, — гом-зм $A$-модулей, причём $\operatorname{Im}\varphi = M$.

В силу т. 1 $A/I \simeq M$, где $I = \operatorname{Ker}\varphi$.

Пусть $A$ - комм. Т.к. $M$ - цикл, то $\forall y \in M\ \exists b \in A$: $y = xb$. Если $a \in I = \operatorname{Ker}\varphi$, то $ya = (xb)a \overset{\text{ком-сть}}{=} (xa)b = 0 \cdot b = 0$. $\blacksquare$

$\underline{\text{Опр 7}}$ Система $\{x_1, \ldots x_n\}$ эл-тов модуля $M$ наз-ся лин. независимой, если $x_1 a_1 + \ldots + x_n a_n = 0 \Rightarrow a_1 = \ldots = a_n = 0$ $\forall a_1 \ldots a_n \in A$. Если эта система порождает $M$, то она наз-ся **базисом** модуля $M$.

К.п. модуль $M$ наз-ся **свободным**, если он обладает базисом.

**Предл 4** Свободный цикл. $A$-модуль изоморфен $A$.

**Д-во:** Применить Т-му 2

Всюду далее $A$ — кольцо главных идеалов.
Заметим, что кольца $A$ 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 (оно наз-ся **рангом** и обозн. $\operatorname{rk} L$.

**Д-во:** Если $p$ — простой эл-т кольца $A$, то $F = A/(p)$ — поле по т. 3 из §2, а $V = L/pL$ — в.п. над $F$. Если $e_1, \dots, e_n$ — базис $L$, то $e_1 + pL, \dots, e_n + pL$ — базис в.п. $V \Rightarrow$ $n = \dim V$ и не зависит от выбора базиса

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

Д-во: См. Д-во Т. 9.3.4 из [ВИН].

Изучим теперь строение 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 $p^k \in \mathrm{Ann}\, M$ для некот. $k \in \mathbb{N}$.

Т.к. $A$ — кольцо гл. идеалов, то по Т. 2 каждый цикл. $A$-модуль $M$ изоморфен либо $A$, либо $A/(n)$ где $n$ — необр. ненул. 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-тов)

В силу Т. 4 из §2 имеем $A/(n) \simeq A/(p_1^{k_1}) \oplus \dots \oplus A/(p_s^{k_s})$

$\Rightarrow$ Предл. 5 Периодич. цикл. модуль есть прямая сумма примарных цикл. модулей и это разложение единственно с точностью до перест. слагаемых.

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

модулей определен однозначно.

<u>Д-во:</u> аналогично док-ву Т. о к.п. абелевых групп. Используя Т. 4, имеем

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

где $u_i \mid u_{i+1}$ $i = 1..m-1$, причем число $m$ и $u_1, \dots u_m$ определены однозначно в силу леммы о приведении м-цы к кан. виду (над кольцом гл. идеалов). Остаётся применить предл. 5.

<u>Зад 2</u> Записать полное док-во.

Как уже говорилось, эл-ты $u_1, \dots u_m$ из кольца $A$ (см (*)) определяется (с точностью до ассоциированности, т.е умножения на обр. эл-т) по модулю $M$ однозначно. Они наз-ся **инвариантными множителями** модуля $M$. При этом у последнего из них есть простой смысл.

<u>Предл 6</u> Если $M$-периодический, то $(u_m) = \mathrm{Ann}\, M$.

<u>Следствие</u> экспонента конечной абелевой группы $G$ равна её последнему инв. мн-лю $u_m$ (здесь $G$ — $\mathbb{Z}$-модуль). Кон. абелева группа циклическая $\Leftrightarrow$ её порядок и экспонента совпадают.

Зад 3 Д-ть следствие.

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

Д-во: Пусть экспонента подгр. $G$ гр $F^*$ равна $m$.

Тогда $g^m = 1$ $\forall g \in G$. 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 развитая нами теория означает для примера 6 из начала параграфа.

Пусть $\varphi$ — л.п. к.м. в.п. $V$ над полем $F$. Пусть $A = F[t]$. Рассмотрим $V$ как $A$-модуль, полагая $x \cdot t = x\varphi$ $\forall x \in V$, откуда $x f(t) = x f(\varphi)$ $\forall f \in A$.

Т.к. $\dim V = n < \infty$, то $V$ — к.п. модуль. Применим к нему Т.5. Заметим, что в разложении $(*)$ не может быть своб. цикл. модулей, т.е. $m=n$, т.к. $A = F[t]$ имеет беск. размерность над $F$.

Предположим, что $F$ алг. замкнуто. Тогда простые эл-ты в $A$ — это линейные мн-ны вида $\Rightarrow$ $M$ есть прямая сумма примарных цикл. модулей вида $\overline{W} = A/(u)$, где $u = (t-\lambda)^m$, $\lambda \in F$.

Модуль $W$ – $m$-мерное векторное пр-во над $F$ с базисом $\{1+(\pi), (t-\lambda)+(\pi), \ldots (t-\lambda)^{m-1}+(\pi)\}$

Опер-р умножения $t-\lambda$ – это нильпотент!

Поэтому в этом базисе умножение на $t$ (т.е действие оператора $\varphi$) записывается м-цей

$$\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & 1 & \\ 0 & & \ddots & 1 \\ & & & \lambda \end{pmatrix},$$ т.е жорд. клеткой,

Таким образом, Т-ма о жорд. форме (и её единственности с точностью до перестановки жорд. клеток) есть прямое следствие Т-мы Б.

Посмотрим также на представление (*) в этом случае $V \simeq A/_{(u_1)} \oplus \quad \oplus A/_{(u_n)}$ (здесь и т.т.!)

Поскольку $(u_n) = \mathrm{Ann}(V) = (g(t))$, где $g(t)$ — мин. мн-н такой, что $xg(t) = 0 \ \forall x \in V$, то $u_n = g(t)$ — мин. аннул. мн-н. Причем, этот факт не зависит от того явл-ся ли поле $F$ алгебр. замкнутым или нет. В частности, это дает уточнение т. о мин. о мин. аннул. многочлене (см. т. 6.7.1 из [BM]).

<u>Зад 4.</u> Покажите, что характ. мн-н $f_\varphi(t)$ лин. пр-я $\varphi$ — это $\prod_{i=1}^{n} u_i$.