Независимый Московский Университет

Алгебра – I

Первый курс, весенний семестр 1998/99 г.
Лекции 5–6

Простейшие классификационные теоремы линейной алгебры

Пусть $\mathbb{k}$ — поле. Я предполагаю известными понятия векторного пространства над $\mathbb{k}$, линейной зависимости, базиса, размерности, линейного отображения. Также я буду пользоваться тем, что любое линейно независимое семейство векторов в конечномерном векторном пространстве можно дополнить до базиса.

Основная задача линейной алгебры — задача классификации (с точностью до изоморфизма). Простейшим примером такой классификации является

Теорема 1. *Любое конечномерное векторное пространство V над $\mathbb{k}$ изоморфно $\mathbb{k}^n$ для некоторого n, причем пространства $\mathbb{k}^n$ и $\mathbb{k}^m$ неизоморфны при $n \neq m$.*

Из этой теоремы следует, что размерность является единственным инвариантом конечномерных векторных пространств.

Будем рассматривать пары (U,V), где $U \subseteq V$. Назовем две пары $(U_1,V_1) \simeq (U_2,V_2)$ *изоморфными*, если существует изоморфизм $\varphi: \quad V_1 \to V_2$, такой что $\varphi(U_1) = U_2$.

Пусть $(u_1,\dots,u_k)$ — базис U. Дополним его до базиса пространства V векторами $v_1,\dots,v_l$. Пусть $n = \dim V = k + l$ и $(e_1,\dots,e_n)$ — базис $\mathbb{k}^n$. Тогда $\mathbb{k}^k$ — линейная оболочка первых k элементов этого базиса. Легко видеть, что $(\mathbb{k}^k,\mathbb{k}^n) \simeq (U,V)$:

$$\varphi(e_i) = \begin{cases} u_i, & i \leqslant k \\ v_{i-k}, & i > k. \end{cases}$$

Получилась

Теорема 2. *Любая пара (U,V), где V — конечномерное векторное пространство над $\mathbb{k}$, а $U \subseteq V$ — его подпространство, изоморфна паре вида $(\mathbb{k}^k,\mathbb{k}^n)$ для некоторых n и $k \leqslant n$.*

Пусть U и W — подпространства конечномерного векторного пространства V. Изоморфизмы троек (U,W,V) определяются аналогично тому, как определялись изоморфизмы пар (U,V).

Рассмотрим подпространство $U \cap W = \langle v_1, \ldots, v_k \rangle$, где $v_1, \ldots, v_k$ — его базис. Дополним его до базисов подпространств U и W векторами $v_{k+1}, \ldots, v_l$ и $v_{l+1}, \ldots, v_m$ соответственно. Пусть векторы линейно зависимы, т.е. $\sum\limits_{i=1}^{m} \alpha^i v_i = 0$, где α^i не все равны нулю. Тогда, очевидно,

$$\sum_{i=1}^{k} \alpha^i v_i + \sum_{i=k+1}^{l} \alpha^i v_i = -\sum_{i=l+1}^{m} \alpha^i v_i.$$

Вектор, стоящий в левой части равенства, лежит в U, а вектор, стоящий в правой части, — в W, а, значит, он принадлежит их пересечению. Следовательно, $\sum\limits_{i=l+1}^{m} \alpha^i v_i = \sum\limits_{j=1}^{k} \beta^j v_j$, а значит, $\alpha^i = 0 \quad \forall i \in \{l+1, \ldots, m\}$. Поэтому $\sum\limits_{i=1}^{k} \alpha^i v_i + \sum\limits_{i=k+1}^{l} \alpha^i v_i = 0$, и $\alpha^i = 0 \quad \forall i \in \{1, \ldots, l\}$ (так как $v_1, \ldots, v_l$ — базис U). Итак, $V = \langle v_1, \ldots, v_m \rangle$, то есть для любых двух подпространств конечномерного векторного пространства можно выбрать базис, согласованный с этой парой подпространств.

Сформулируем соответствующую классификационную теорему (несколько в ином стиле, чем две предыдущие).

Теорема 3. *Конечномерное пространство V и два его подпространства U и W определяются однозначно (с точностью до изоморфизма) следующими четырьмя инвариантами: $k = \dim V$, $l = \dim U$, $m = \dim W$ и $n = \dim(U \cap W)$, которые могут принимать любые неотрицательные целые значения, удовлетворяющие неравенствам $n \leqslant m \leqslant k$ и $n \leqslant l \leqslant k$.*

Рассмотрим, в чем состоит общий подход к задаче классификации.

Пусть нам надо классифицировать векторные пространства с некоторой дополнительной структурой (парой подпространств, или квадратичной формой, или чем-то ещё). Обозначим пространство V с этой дополнительной структурой через $\mathbf{V}$ и назовём *объектом*.

В любой классификационной задаче есть понятие изоморфизма объектов $\mathbf{V} \cong \mathbf{W}$. Обычно это просто линейный изоморфизм, «согласованный с дополнительной структурой». Определение согласованности, как правило, не вызывает затруднений.

Полное решение задачи классификации — это:

1) список *стандартных объектов* $\mathbf{V}_s$, где s пробегает некоторое множество индексов, такой, что любой объект $\mathbf{V}$ изоморфен ровно одному из объектов V_s;

2) список *инвариантов* φ_r, каждый из которых сопоставляет объекту $\mathbf{V}$ некоторое число $\varphi_r(\mathbf{V})$, такой, что $\mathbf{V} \cong \mathbf{W}$ тогда и только тогда, когда $\varphi_r(\mathbf{V}) = \varphi_r(\mathbf{W})$ для любого r.

Для получения полного списка стандартных объектов очень полезен следующий подход.

Пусть V и W — векторные пространства. Их *прямой суммой* $V \oplus W$ называется множество всевозможных пар (v, w), где $v \in V$, $w \in W$. На $V \oplus W$ вводится структура векторного пространства: $(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2)$ и $\lambda(v, w) = (\lambda v, \lambda w)$.

Если каждое из пространств V и W снабжено нашей «дополнительной структурой», то (для всех рассматривавшихся классификационных задач) на прямой сумме $V \oplus W$ тоже возникает естественная дополнительная структура. Например, если в пространствах V и W заданы подпространства V_0 и W_0 соответственно, то в $V \oplus W$ возникает подпространство $V_0 \oplus W_0$, и т. п. Таким образом, мы получаем понятие *прямой суммы объектов* $\mathbf{V} \oplus \mathbf{W}$.

Операция взятия прямой суммы объектов является коммутативной и ассоциативной (в смысле изоморфизма соответствующих прямых сумм; например, коммутативность — это изоморфизм $\mathbf{V} \oplus \mathbf{W} \cong \mathbf{W} \oplus \mathbf{V}$).

Объект $\mathbf{V}$ называется нулевым, если соответствующее векторное пространство V является нулевым. Объект $\mathbf{V}$ называется неразложимым, если он не изоморфен никакой прямой сумме ненулевых объектов.

Ясно, что любой ненулевой объект изоморфен прямой сумме нескольких неразложимых. Поэтому важной составной частью задачи классификации является нахождение всех (с точностью до изоморфизма) неразложимых объектов.

Упражнение 1. Докажите, что в задачах классификации пространств с k выделенными подпространствами ($k = 0, 1, 2$) каждый неразложимый объект представляют собой одномерное пространство (каждое из выделенных подпространств либо одномерно, либо нульмерно).

Список всех неразложимых объектов особенно полезен тогда, когда для каждого объекта любое его разложение в прямую сумму неразложимых содержит одни и те же слагаемые (с точностью до перестановки).

Упражнение 2. Проверьте, что во всех рассматривавшихся ранее задачах классификации это так.

Рассмотрим еще один тип классификационных задач.

Назовём *колчаном* произвольный ориентированный граф. *Представлением колчана над полем* $\mathbb{k}$ называется следующий набор данных: для каждой вершины i — некоторое конечномерное векторное пространство V_i над $\mathbb{k}$, а для каждой стрелки e из i в j — линейное отображение $\varphi_e : V_i \to V_j$. Представления (V_i, φ_e) и (W_i, ψ_e) данного колчана называются изоморфными, если для каждой вершины i колчана существует изоморфизм $f_i : V_i \to W_i$, причем $f_j \varphi_e = \psi_e f_i$ для любой стрелки из i в j.

Прямой суммой представлений (V_i, φ_e) и (W_i, ψ_e) данного колчана называется представление $(V_i \oplus W_i, \varphi_e \oplus \psi_e)$, где $\varphi_e \oplus \psi_e$ — отображение, переводящее каждую пару (v, w) в пару $(\varphi_e v, \psi_e w)$.

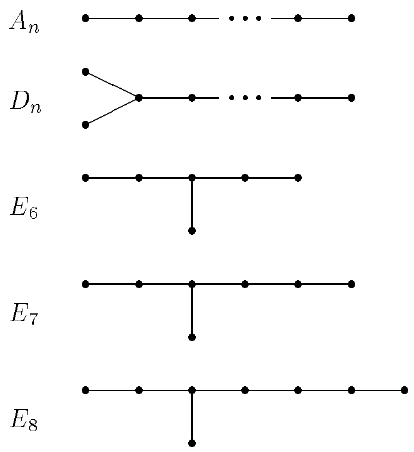

Рис. 1.

Колчаны, представления которых имеют «простую» классификацию, описываются знаменитой теоремой Габриэля. Часть утверждений этой теоремы можно сформулировать так:

Теорема 4. *Колчан* Γ *имеет лишь конечное число неизоморфных неразложимых представлений над* $\mathbb{R}$ *тогда и только тогда, когда каждая связная компонента* Γ *получается некоторой расстановкой стрелок в одном из графов на рис. 1. При этом набор неразложимых представлений, на которые раскладывается данное представление, определяется этим представлением однозначно.*

Полное доказательство этой теоремы я надеюсь рассказать в следующем году (если удастся), но часть доказательства можно объяснить и сейчас.

Обозначим вершины графа Γ натуральными числами от 1 до n. Ясно, что достаточно рассмотреть связные колчаны.

Размерность пространства $\mathcal{V}(d_1, \ldots, d_n)$ всех представлений колчана, для которых $V_i = \mathbb{R}^{d_i}$, равна, очевидно, $\sum_{e \in E} d_{i(e)} d_{j(e)}$, где E — множество стрелок колчана, а через $i(e)$ и $j(e)$ обозначены, соответственно, начало и конец стрелки e. Если число неизоморфных неразложимых представлений конечно, то конечно и число всех неизоморфных представлений с данным набором размерностей $d_1, \ldots, d_n$ пространств, отвечающих вершинам колчана. Это последнее число равно, очевидно, числу орбит группы $GL(d_1, \mathbb{R}) \times \cdots \times GL(d_n, \mathbb{R})$, действующей на пространстве $\mathcal{V}(d_1, \ldots, d_n)$ по формулам замены базиса: $(g_1, \ldots, g_n)\varphi_e = g_{j(e)}^{-1} \varphi_e g_{i(e)}$. Размерность каждой из орбит не больше $\sum_{i=1}^{n} d_i^2 - 1$ (так как стабилизатор каждой точки $\mathcal{V}(d_1, \ldots, d_n)$ содержит одномерную подгруппу, состоящую из элементов вида $(\lambda, \ldots, \lambda) \in GL(d_1, \mathbb{R}) \times \cdots \times GL(d_n, \mathbb{R})$). Поскольку пространство $\mathcal{V}(d_1, \ldots, d_n)$ покрыто конечным числом таких орбит, его размерность не может быть больше максимально возможной размерности орбиты, то есть функция $f(d_1, \ldots, d_n) = \sum_{i=1}^{n} d_i^2 - \sum_{e \in E} d_{i(e)} d_{j(e)}$ должна принимать положительное значение на любом ненулевом наборе неотрицательных целых чисел. Отсюда легко следует, что эта функция положительна на любом ненулевом наборе целых чисел, а следовательно и на любом ненулевом наборе рациональных (и даже действительных) чисел. Доказательство того, что все связные графы, для которых квадратичная форма f положительно определена, описываются ADE-классификацией, я оставляю в качестве упражнения (не очень простого).

Вышеприведенное рассуждение опирается на понятие размерности многообразия и на тот факт, что образ многообразия при гладком отображении не может покрыть многообразие большей размерности (это следует, например, из теоремы Сарда). Надеюсь, что всё это вы рано или поздно изучите в курсе математического анализа.

Классификация пространств с k выделенными подпространствами практически эквивалентна классификации представлений колчана из k стрелок, ведущих в одну вершину из k других. Из теоремы Габриэля следует, что простая классификация есть при $k \leq 3$. Классификация пространств с тройкой подпространств также оставляется в качестве упражнения.

Модули над кольцами

Определение 1. Пусть R — ассоциативное кольцо с единицей. *Левым модулем* над R (или *левым R-модулем*) называется абелева группа V (записываемая аддитивно), снабженная операцией левого умножения на элементы кольца R, удовлетворяющей условиям

1) $a(v + w) = av + aw$,

2) $(a + b)v = av + bv$,

3) $(ab)v = a(bv)$,

4) $1v = v$

для всех $a, b \in R$, $v, w \in V$.

Аналогично определяется *правый R-модуль*. Однако в ближайшее время правые модули нам почти не встретятся, поэтому вместо слов «левый модуль» я часто буду говорить просто «модуль».

Все кольца в дальнейшем предполагаются ассоциативными с единицей.

Пример 1. Любое линейное пространство над полем $\Bbbk$ является $\Bbbk$-модулем.

Пример 2. Любое кольцо R является левым R-модулем (а также правым R-модулем).

Пример 3. Любое левый идеал в кольце R является левым R-модулем. Любое правый идеал в кольце R является правым R-модулем.

Пример 4. Любая абелева группа является $\mathbb{Z}$-модулем.

Пример 5. Пусть H — абелева группа, а $\operatorname{End} H$ — множество эндоморфизмов группы H, то есть гомоморфизмов $H \to H$. Сумма и произведение (композиция) эндоморфизмов тоже являются эндоморфизмами, причем все аксиомы кольца легко проверяются. Легко видеть также, что применение эндоморфизма к элементу H задает на H структуру $\operatorname{End} H$-модуля.

Более того, задать на H структуру модуля над произвольным кольцом R — это то же самое, что задать гомоморфизм колец $R \to \operatorname{End} H$ (аналогично тому, что действие группы G на множестве M — это то же самое, что гомоморфизм группы G в симметрическую группу $S(M)$).

Пример 6. Пусть V — линейное пространство над полем $\Bbbk$ и $\mathcal{A} : V \to V$ — линейный оператор. Для любого многочлена $f(x) = a_0 + a_1 x + \dots + a_k x^k \in \Bbbk[x]$ рассмотрим оператор $f(\mathcal{A}) = a_0 \mathcal{E} + a_1 \mathcal{A} + \dots + a_k \mathcal{A}^k$ (через $\mathcal{E}$ обозначен единичный оператор). Положим $f(x)v = f(\mathcal{A})(v)$ для любого $v \in V$. Введенное таким образом умножение векторов из V на элементы кольца $\Bbbk[x]$ превращает V в $\Bbbk[x]$-модуль.

Пример 7. Классификация пространств с оператором — это классификация представлений колчана с одной вершиной и с одной стрелкой, представляющей собой петлю с началом и концом в этой вершине. На самом деле, изучение представлений любого колчана эквивалентно изучению модулей над некоторым кольцом. Например, для колчана, представляющего собой одну стрелку из вершины 2 в вершину 1, соответствующее кольцо представляет собой алгебру A верхнетреугольных матриц размера 2×2 над полем $\Bbbk$. Действительно, для любого представления V_1, V_2, φ нашего колчана рассмотрим пространство $V = V_1 \oplus V_2$ и определим на нем структуру A-модуля, положив $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} (v_1, v_2) = (av_1 + b\varphi v_2, cv_2)$. Проверьте, что это действительно A-модуль, и что по любому A-модулю можно построить соответствующее представление колчана.

Пример 8. Пусть V — линейное пространство над полем $\Bbbk$ и G — произвольная группа. Действие группы G на V линейными отображениями называется *линейным представлением* группы G в пространстве V. Рассмотрим векторное пространство $\Bbbk G$, базис которого составляют элементы группы G. Определим произведение элементов $\Bbbk G$ следующим образом:

$(\sum \alpha_i g_i)(\sum \beta_j g_j) = \sum \alpha_i \beta_j g_i g_j$. Легко проверить, что относительно этого произведения $\Bbbk G$ является ассоциативным кольцом с единицей. Оно называется *групповой алгеброй группы* G. Любое линейное представление группы G в пространстве V определяет на V структуру $\Bbbk G$-модуля. Наоборот, любой $\Bbbk G$-модуль представляет собой векторное пространство над $\Bbbk$, в котором задано представление группы G.

Довольно легко определить понятия гомоморфизма R-модулей, подмодуля, фактормодуля, а также сформулировать и доказать основную теорему о гомоморфизмах R-модулей (аналогичную теоремам о гомоморфизмах групп и колец). Это предлагается проделать самим в качестве обязательного упражнения.

При работе с фактормодулями полезны две простые теоремы, также имеющие свои аналоги для групп и колец. Докажите их сами.

Теорема 5 (об изоморфизме). *Пусть V — R-модуль, $U, W \subseteq V$ — подмодули. Тогда $U + W$ (то есть множество элементов из V, которые могут быть представлены в виде $u + w$ для некоторых $u \in U$, $w \in W$) является подмодулем модуля V, содержащим W, причем отображение $\varphi : u + (U \cap W) \mapsto u + W$ является изоморфизмом модулей $U/(U \cap W) \cong (U + W)/W$.*

Теорема 6 (о соответствии). *Пусть V — R-модуль, $W \subseteq V$ — подмодуль и $\pi : V \to V/W$ — каноническая проекция. Тогда $\overline{M} = M/W$ — подмодуль в $\overline{V} = V/W$ для любого подмодуля $M \subseteq V$ такого, что $W \subseteq M$, причем отображение $M \mapsto \overline{M}$ является биекцией между множеством подмодулей V, содержащих W, и множеством подмодулей $\overline{V}$. Кроме того, $V/M \cong \overline{V}/\overline{M} = (V/W)/(M/W)$.*

Определение 2. R-модуль V называется *простым*, если он не имеет собственных подмодулей, то есть никаких подмодулей, кроме себя и 0.

Упражнение 3. Доказать, что любой простой $\mathbb{Z}$-модуль изоморфен $\mathbb{Z}_p$ для некоторого простого p.

Определение 3. *Композиционным рядом* или *рядом Жордана–Гёльдера* R-модуля V называется конечная последовательность $V_0, V_1, \ldots, V_n$ подмодулей модуля V таких, что $0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$ и фактормодули V_i/V_{i-1} (называемые *композиционными факторами*) просты. Число n называется *длиной* композиционного ряда (V_i).

Если модуль V имеет композиционный ряд, то V называется *конечным модулем*.

Утверждение 1. *Пусть V является конечным R-модулем, а W — подмодуль модуля V. Тогда W и $\overline{V} = V/W$ — тоже конечные R-модули.*

Доказательство. Пусть $0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$ — композиционный ряд R-модуля V и пусть $\pi : V \to \overline{V}$ — каноническая проекция. Положим $W_i = W \cap V_i$ и $\overline{V}_i = \pi(V_i)$. Ясно, что $0 = W_0 \subseteq W_1 \subseteq \cdots \subseteq W_n = W$ и $0 = \overline{V}_0 \subseteq \overline{V}_1 \subseteq \cdots \subseteq \overline{V}_n = \overline{V}$.

Пусть $0 < i \leqslant n$. По теореме об изоморфизме,

$$W_i/W_{i-1} = W_i/(W_i \cap V_{i-1}) \cong (W_i + V_{i-1})/V_{i-1}.$$

С другой стороны, поскольку $\overline{V}_i = \pi(V_i) = \pi(V_i + W)$ и $\overline{V}_{i-1} = \pi(V_{i-1}) = \pi(V_{i-1} + W)$, то, по теореме о соответствии,

$$\overline{V}_i/\overline{V}_{i-1} \cong (V_i + W)/(V_{i-1} + W).$$

Ясно, что $V_i + W = V_i + (V_{i-1} + W)$. Кроме того, $V_i \cap (V_{i-1} + W) = V_{i-1} + W_i$. Действительно, если $v + w \in V_i$, где $v \in V_{i-1}$, а $w \in W$, то $w \in V_i \cap W$, т. к. $V_{i-1} \subset V_i$. Применяя теорему об изоморфизме, получаем

$$(V_i + W)/(V_{i-1} + W) \cong V_i/(V_{i-1} + W_i).$$

Итак, мы имеем изоморфизмы

$$W_i/W_{i-1} \cong (W_i + V_{i-1})/V_{i-1} \qquad \text{и} \qquad \overline{V}_i/\overline{V}_{i-1} \cong V_i/(W_i + V_{i-1}).$$

Однако из нестрогих включений $V_{i-1} \subseteq (W_i + V_{i-1}) \subseteq V_i$ одно является равенством (иначе образ $(W_i + V_{i-1})$ при канонической проекции на V_i/V_{i-1} был бы там собственным подмодулем, что невозможно в силу простоты модуля V_i/V_{i-1}). Значит, выполнено одно из двух: либо

$$W_i/W_{i-1} \cong V_i/V_{i-1} \qquad \text{и} \qquad \overline{V}_i/\overline{V}_{i-1} = 0,$$

либо

$$W_i/W_{i-1} = 0 \qquad \text{и} \qquad \overline{V}_i/\overline{V}_{i-1} \cong V_i/V_{i-1},$$

Итак, все ненулевые факторы вида W_i/W_{i-1} и $\overline{V}_i/\overline{V}_{i-1}$ просты ($i = 1, \ldots, n$). Вычеркивая из последовательностей $0 = W_0 \subseteq W_1 \subseteq \cdots \subseteq W_n = W$ и $0 = \overline{V}_0 \subseteq \overline{V}_1 \subseteq \cdots \subseteq \overline{V}_n = \overline{V}$ совпадающие члены, получаем композиционные ряды для модулей W и V/W, соответственно. $\square$

Утверждение 2. *Пусть V — R-модуль, а W — его подмодуль, причем известно, что как W, так и $\overline{V} = V/W$ — конечные модули. Тогда и V — конечный модуль.*

Доказательство. Пусть $0 = W_0 \subset W_1 \subset \cdots \subset W_k = W$ — композиционный ряд модуля W, а $0 = \overline{V}_0 \subset \overline{V}_1 \subset \cdots \subset \overline{V}_m = \overline{V}$ — композиционный ряд модуля $\overline{V}$. Через π обозначим каноническую проекцию $V \to \overline{V}$. Положим $n = k + m$ и

$$V_i = \begin{cases} W_i, & 0 \leqslant i \leqslant k; \\ \pi^{-1}(V_{i-k}) & k \leqslant i \leqslant n. \end{cases}$$

Заметим, что для $i = k$ оба варианта определения согласованы и дают $V_k = W$.

Докажем, что $0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$ — композиционный ряд R-модуля V. Действительно, при $i \leqslant k$ мы имеем $V_i/V_{i-1} = W_i/W_{i-1}$ — простой модуль, а при $i > k$, по теореме о соответствии, $V_i/V_{i-1} \cong \overline{V}_{i-k}/\overline{V}_{i-k-1}$ — тоже простой модуль. $\square$

Утверждение 3. *Пусть V — конечный R-модуль. Тогда любую последовательность вложенных подмодулей $W_1 \subset \cdots \subset W_k \subset V$ можно уплотнить до композиционного ряда, то есть можно найти композиционный ряд $0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$ такой, что $W_s = V_{i(s)}$ для каждого $s = 1, \ldots, k$.*

Доказательство. Воспользуемся индукцией по k. При $k = 0$ доказывать нечего. Пусть $k > 0$. Положим $W = W_1$, $\overline{V} = V/W$ и $\overline{W}_i = \pi(W_i)$, где $\pi : V \to \overline{V}$ — каноническая проекция. По предположению индукции существует композиционный ряд модуля $\overline{V}$, уплотняющий последовательность вложенных подмодулей $\overline{W}_2 \subset \overline{W}_k \subset \overline{V}$. По утверждению 1, существует композиционный ряд подмодуля W. «Сшивая» эти композиционные ряды, как в доказательстве утверждения 2, получаем композиционный ряд, уплотняющий последовательность $W_1 \subset \cdots \subset W_k \subset V$. $\square$

Теорема 7 (Жордана-Гёльдера). *Пусть V — R-модуль, а $0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$ и $0 = V_0' \subset V_1' \subset \cdots \subset V_m' = V$ — два его композиционных ряда. Тогда $n = m$ и найдется такая перестановка $\sigma \in S_n$, что $V_i/V_{i-1} \cong V_{\sigma(i)}/V_{\sigma(i)-1}$ для любого $i = 1, \ldots, n$.*

Доказательство. Воспользуемся индукцией по n — длине композиционного ряда (V_i).

Если $n = 1$, то модуль V прост, поэтому $V_1' = V = V_1$.

Пусть теперь $n > 1$. Положим $U_i = V_1' \cap V_i$. Тогда $0 = U_0 \subseteq U_1 \subseteq \cdots \subseteq U_n = V_1'$. Модуль V_1' прост, поэтому найдется i такое, что $U_i = V_1'$ и $U_{i-1} = 0$, следовательно, в V_i вложена прямая сумма $V_{i-1} \oplus V_1'$. Значит, модуль $(V_{i-1} \oplus V_1')/V_{i-1} \cong V_1'$ вложен в V_i/V_{i-1}. Последний модуль прост, поэтому $V_i = V_{i-1} \oplus V_1'$ и $V_i/V_{i-1} \cong V_1'$.

Положим теперь $\overline{V} = V/V_1'$. Обозначим через $\overline{V}_j$ образ V_j, а через $\overline{V}_j'$ — образ V_j' при канонической проекции $V \to \overline{V}$. Мы имеем (по теореме об изоморфизме)

$$\overline{V}_j \cong \begin{cases} V_j & \text{при } j < i, \\ V_j/V_1' & \text{при } j \geqslant i. \end{cases}$$

Поэтому

$$\overline{V}_j/\overline{V}_{j-1} \cong \begin{cases} V_j/V_{j-1} & \text{при } j \neq i, \\ 0 & \text{при } j = i \end{cases}$$

(по теореме о соответствии). Аналогично

$$\overline{V}'_j/\overline{V}'_{j-1} \cong \begin{cases} V'_j/V'_{j-1} & \text{при } j > 1, \\ 0 & \text{при } j = 1. \end{cases}$$

Итак, модуль $\overline{V}$ имеет два композиционных ряда: $0 = \overline{V}_0 \subset \overline{V}_1 \subset \cdots \subset \overline{V}_{i-1} \subset \overline{V}_{i+1} \subset \cdots \subset \overline{V}_n = \overline{V}$ длины $n-1$, и $0 = \overline{V}_0 \subset \overline{V}'_2 \subset \cdots \subset \overline{V}'_m = \overline{V}$ длины $m-1$. Остается применить предположение индукции. □

Мы доказали, что все композиционные ряды конечного модуля V имеют одну и ту же длину. Она называется *длиной модуля* V и обозначается через $l(V)$. Отметим, что для любого подмодуля $W \subseteq V$ выполнено равенство $l(V) = l(W) + l(V/W)$. Это равенство выражает свойство *аддитивности* длины.

Периодические модули

Всюду далее R — коммутативное кольцо.

Определение 4. *Аннулятором* элемента v R-модуля V называется множество $\mathrm{Ann}(v) = \{a \in R \mid av = 0\}$ (легко видеть, что это идеал). Элемент v называется *периодическим*, если $\mathrm{Ann}(v) \neq 0$. Модуль V называется периодическим, если все его элементы являются периодическими. Идеал $\mathrm{Ann}(V) = \bigcap\limits_{v \in V} \mathrm{Ann}(v)$ называется аннулятором модуля V.

Отметим, что если кольцо R является целостным, то для любого модуля V множество V_t его периодических элементов является подмодулем. Этот подмодуль называется *подмодулем кручения* модуля V. Соответственно периодический модуль V часто называют *модулем кручения* (так как для него $V_t = V$).

Определение 5. R-модуль V называется *циклическим*, если $V = Rv$ для некоторого $v \in V$. Элемент v называется *образующей* модуля V. R-модуль V называется *конечнопорожденным*, если $V = Rv_1 + \cdots + Rv_r$ для некоторых $v_1, \ldots, v_r \in V$.

Из теоремы о гомоморфизмах модулей следует, что циклический модуль $V = Rv$ изоморфен $R/\mathrm{Ann}(v)$. С другой стороны, очевидно, что для любого идеала $I \subset R$ модуль R/I является циклическим (с образующей $1 + I$).

Отметим, что конечнопорожденный модуль V над целостным кольцом R является периодическим тогда и только тогда, когда $\mathrm{Ann}(V) \neq 0$. Действительно, если $\mathrm{Ann}(V) \neq 0$, то V, очевидно, периодический. Если же V порождается элементами $v_1, \ldots, v_n$ и все они периодические, то существуют ненулевые элементы $a_i \in R$ такие, что $a_i v_i = 0$. Тогда $\mathrm{Ann}(V) \ni a_1 \cdot \cdots \cdot a_n \neq 0$.

Пример 9. Пусть V — абелева группа, то есть $\mathbb{Z}$-модуль. Тогда V_t — множество элементов V, порядок которых конечен. Конечная абелева группа является конечнопорожденным периодическим $\mathbb{Z}$-модулем.

Пример 10. Пусть V — n-мерное линейное пространство над полем $\Bbbk$ и $\mathcal{A} : V \to V$ — линейный оператор. Очевидно, что V как $\Bbbk[x]$-модуль конечнопорожден. Множество всех линейных операторов $V \to V$ является линейным пространством размерности n^2. Поэтому семейство $\mathcal{E}, \mathcal{A}, \mathcal{A}^2, \dots, \mathcal{A}^{n^2}$ является линейно зависимым, то есть найдется такой ненулевой многочлен $f(x)$ степени не выше n^2, что $f(x)v = 0$ для любого $v \in V$. Таким образом, $\Bbbk[x]$-модуль V является периодическим.

Многочлен $f(x)$ минимальной степени, аннулирующий модуль V, то есть такой, что $f(\mathcal{A}) = 0$, и нормированный условием, что старший коэффициент $f(x)$ равен единице, называется *минимальным многочленом* оператора $\mathcal{A}$. Условие минимальности степени, очевидно, эквивалентно тому, что $f(x)$ порождает идеал $\operatorname{Ann}(V)$, то есть любой многочлен, аннулирующий V, делится на $f(x)$.

Замечание. Любой R-модуль V всегда можно рассматривать как $R/\operatorname{Ann}(V)$-модуль относительно умножения $(a + \operatorname{Ann}(V))v = av$ для любых $a \in R$, $v \in V$. С другой стороны, для любого идеала $I \subset R$ любой R/I-модуль W можно рассматривать как R-модуль, полагая $aw = \pi(a)w$, где $\pi : R \to R/I$ — каноническая проекция.

Ясно, что любой простой модуль V является циклическим (возьмем произвольный ненулевой элемент $v \in V$, тогда Rv является ненулевым подмодулем модуля V, значит $V = Rv$).

Упражнение 4. Доказать, что модуль R/I прост тогда и только тогда, когда идеал I максимален.

Утверждение 4. *Пусть R — кольцо главных идеалов, не являющееся полем. R-модуль V является конечным модулем тогда и только тогда, когда он является конечнопорожденным периодическим модулем.*

Доказательство. Пусть V — конечный модуль и $0 = V_0 \subset V_1 \subset \dots \subset V_n = V$ — его композиционный ряд. Выберем $v_1, \dots, v_n \in V$ так, чтобы $v_i \in V_i \setminus V_{i-1}$. Тогда $V = Rv_1 + \dots + Rv_n$.

Поскольку R-модуль V_i/V_{i+1} прост, то он изоморфен $R/(p_i)$ для некоторого неприводимого элемента $p_i \in R$. Тогда $a = p_1 \dots p_n$ лежит в $\operatorname{Ann}(V)$, следовательно, V — периодический модуль.

Пусть, наоборот, V — конечнопорожденный периодический модуль. Рассмотрим, прежде всего, случай, когда $V = R/(a)$ — циклический модуль.

Пусть $a = p_1 \dots p_n$ — разложение a на простые множители. Положим $a_i = a/(p_1 \dots p_i)$ и $V_i = a_i V$, где $i = 0, \dots, n$. Тогда $0 = V_0 \subset V_1 \subset \dots \subset V_n = V$ — композиционный ряд модуля V.

Пусть теперь V — произвольный конечнопорожденный периодический модуль, $v_1, \dots, v_k$ — его образующие, и $\mathrm{Ann}(v_i) = (a_i)$ для $i = 1, \dots, k$. Рассмотрим R-модуль $W = R/(a_1) \oplus \dots \oplus R/(a_k)$. Это — конечный модуль (прямая сумма конечных модулей является, очевидно, конечным модулем).

Пусть $w = (\overline{r}_1, \dots, \overline{r}_k)$, где $\overline{r}_i = r_i + (a_i) \in R/(a_i)$. Тогда $\sum r_i v_i$ не зависит от выбора представителей r_i смежных классов $\overline{r}_i$, то есть существует корректно определенное отображение $(\overline{r}_1, \dots, \overline{r}_k) \mapsto \sum r_i v_i$. Ясно, что это отображение является сюръективным гомоморфизмом. По теореме о гомоморфизмах модулей V изоморфен фактормодулю модуля W и, следовательно, тоже является конечным модулем. □

Пример 11. Пусть V — n-мерное линейное пространство над алгебраически замкнутым полем $\Bbbk$ и $\mathcal{A} : V \to V$ — линейный оператор. Тогда V является конечнопорожденным модулем кручения над кольцом $\Bbbk[x]$. Любой максимальный идеал в кольце $\Bbbk[x]$ имеет вид $(x - \lambda)$ для некоторого $\lambda \in \Bbbk$. Простой $\Bbbk[x]$-модуль $\Bbbk[x]/(x - \lambda)$ — это одномерное векторное пространство, в котором x действует умножением на λ. Отсюда сразу следует, что длина $\Bbbk[x]$-модуля V равна $n = \dim V$. Ряд Жордана-Гёльдера $\Bbbk[x]$-модуля V — это последовательность подпространств $0 = V_0 \subset V_1 \subset \dots \subset V_n = V$ таких, что $\dim V_i = i$ и $(\mathcal{A} - \lambda_i \mathcal{E}) V_i \subseteq V_{i-1}$ для некоторых $\lambda_1, \dots, \lambda_n \in \Bbbk$. Выберем базис $v_1, \dots, v_n$ пространства V, согласованный с системой вложенных подпространств V_i, то есть такой, что $v_1, \dots, v_i$ составляют базис пространства V_i $(i = 1, \dots, n)$. В этом базисе матрица оператора $\mathcal{A}$ имеет верхнетреугольный вид с элементами $\lambda_1, \dots, \lambda_n$ на диагонали. Обратно, любой базис, в котором матрица оператора $\mathcal{A}$ имеет верхнетреугольный вид, задает ряд Жордана-Гёльдера $\Bbbk[x]$-модуля V.

Пусть A — матрица оператора $\mathcal{A}$ в некотором базисе. Многочлен $\det(\lambda E - A) \in \Bbbk[\lambda]$ называется *характеристическим многочленом* матрицы A. При переходе к другому базису матрица A заменяется на матрицу $C^{-1}AC$, где C — матрица замены базиса. При этом $\det(\lambda E - C^{-1}AC) = \det(C^{-1}(\lambda E - A)C) = \det(\lambda E - A)$, то есть характеристический многочлен не меняется при замене базиса и, значит, он зависит только от оператора $\mathcal{A}$. Для верхнотреугольной матрицы корнями характеристического многочлена являются диагональные элементы. Поэтому простой модуль $\Bbbk[x]/(x - a)$ встречается среди композиционных факторов $\Bbbk[x]$-модуля V столько раз, какова кратность a как корня характеристического многочлена оператора $\mathcal{A}$. Корни характеристического многочлена называются *собственными значениями* оператора $\mathcal{A}$.