§ 2. Модули над кольцами главных идеалов

В этом параграфе мы предполагаем, что R — целостное кольцо главных идеалов. Все рассматриваемые модули и гомоморфизмы являются, если не оговорено противное, модулями над R и R-гомоморфизмами.

Теоремы этого параграфа обобщают утверждения, доказанные в гл. I для абелевых групп. Мы будем также указывать, как следует видоизменить доказательства из гл. I, чтобы после изменения терминологии получить доказательства для настоящего случая.

Пусть F — свободный модуль над R с базисом $\{x_i\}_{i \in I}$. Тогда мощность I однозначно определена (и называется размерностью F). Напомним, что это доказывается, скажем, рассмотрением простого элемента p в R и тем наблюдением, что F/pF есть векторное пространство над полем R/pR, размерность которого в точности равна мощности I. Таким образом, мы можем говорить о размерности свободного модуля над R.

Теорема 1. *Пусть F — свободный модуль и M — некоторый его подмодуль. Тогда M свободен и его размерность меньше или равна размерности F.*

Доказательство. Для простоты мы дадим доказательство для случая, когда F имеет конечный базис $\{x_i\}$, $i = 1, \ldots, n$. Пусть M_r — пересечение M с $(x_1, \ldots, x_r)$ — модулем, порожденным элементами $x_1, \ldots, x_r$. Тогда $M_1 = M \cap (x_1)$ — подмодуль в (x_1), а потому имеет вид $(a_1 x_1)$ для некоторого $a_1 \in R$. Следовательно, M_1 либо нулевой, либо свободный размерности 1. Предположим по индукции, что M_r — свободный модуль размерности $\leqslant r$. Пусть $\mathfrak{a}$ — множество, состоящее из всех элементов $a \in R$, таких, что существует элемент $x \in M$, который может быть записан в виде

$$x = b_1 x_1 + \ldots + b_r x_r + a x_{r+1},$$

где $b_i \in R$. Тогда, очевидно, $\mathfrak{a}$ — идеал, и, следовательно, главный идеал, порожденный некоторым элементом a_{r+1}. Если $a_{r+1} = 0$, то $M_{r+1} = M_r$ и индуктивный шаг сделан. Если $a_{r+1} \neq 0$, то пусть элемент $w \in M_{r+1}$ таков, что его коэффициент при x_{r+1} равен a_{r+1}. Если элемент $x \in M_{r+1}$, то его коэффициент при x_{r+1} делится на a_{r+1} и, значит, существует элемент $c \in R$, такой, что $x - cw$ лежит в M_r. Следовательно,

$$M = M_r + (w).$$

С другой стороны, ясно, что $M_r \cap (w)$ есть 0 и, следовательно, эта сумма прямая, что и доказывает нашу теорему. Отметим, что это доказательство с заменой простой индукции трансфинитной остается справедливым и в бесконечном случае.

Следствие. *Всякий подмодуль E' конечно порожденного модуля E конечно порожденный.*

Доказательство. Мы можем представить E как фактор-модуль свободного модуля с конечным числом образующих; если $v_1, \ldots, v_n$ — образующие E, то возьмем свободный модуль F с базисом $\{x_1, \ldots, x_n\}$ и отобразим x_i на v_i. Прообраз E' в F свободен и конечно порожден, согласно теореме. Следовательно, E' — конечно порожденный модуль. Утверждение вытекает также из простейших свойств нетеровых колец и модулей.

Если желать перенести на модули над кольцом главных идеалов доказательства из гл. I, то нужно принять следующие определения. Свободный одномерный модуль над R называется *бесконечным циклическим*. Бесконечный циклический модуль изоморфен кольцу R, рассматриваемому как модуль над собой. Таким образом, всякий ненулевой подмодуль бесконечного циклического модуля является бесконечным циклическим. Доказательство, данное в гл. I для аналога теоремы 1, применимо теперь без дальнейших изменений.

Пусть E — модуль. Элемент x модуля E называется *периодическим*, если существует элемент $a \in R$, $a \neq 0$, для которого $ax = 0$. Мы говорим, что E — *периодический* модуль, если все его элементы периодические. Обобщением *конечной абелевой группы* служит *конечно порожденный периодический модуль*.

Пусть E — модуль. Обозначим через E_t подмодуль, состоящий из всех периодических элементов E; мы будем называть его *подмодулем кручения* модуля E. Если $E_t = 0$, то мы будем говорить, что E — *модуль без кручения*.

Теорема 2. *Пусть E — конечно порожденный модуль. Тогда модуль E/E_t свободный. Существует свободный подмодуль F в E, такой, что E есть прямая сумма*

$$E = E_t \oplus F.$$

Размерность такого подмодуля F однозначно определена.

Доказательство. Докажем сначала, что модуль E/E_t без кручения. Обозначим через $\bar{x}$ класс вычетов элемента $x \in E$ по модулю E_t. Пусть элемент $b \in R$, $b \neq 0$, таков, что $b\bar{x} = 0$. Тогда $bx \in E_t$ и, значит, существует элемент $c \in R$, $c \neq 0$, для которого $cbx = 0$. Следовательно, $x \in E_t$ и $\bar{x} = 0$, что доказывает отсутствие кручения у модуля E/E_t. Этот модуль является также конечно порожденным. Предположим теперь, что M — конечно порожденный модуль без кручения. Пусть $\{v_1, \ldots, v_n\}$ — максимальное множество элементов в M среди данного конечного множества образующих $\{y_1, \ldots, y_m\}$, такое, что множество $\{v_1, \ldots, v_n\}$ линейно независимо.

Если y — одна из образующих, то найдутся элементы $a, b_1, \ldots, b_n \in R$, не все равные 0, такие, что

$$ay + b_1v_1 + \ldots + b_nv_n = 0.$$

Тогда $a \neq 0$ (иначе мы придем в противоречие с линейной независимостью $v_1, \ldots, v_n$). Следовательно, ay лежит в $(v_1, \ldots, v_n)$. Таким образом, для каждого $j = 1, \ldots, m$ мы можем найти элемент $a_j \in R$, $a_j \neq 0$, такой, что a_jy_j лежит в $(v_1, \ldots, v_n)$. Пусть $a = a_1 \ldots \ldots a_m$ — произведение этих элементов. Тогда aM содержится в $(v_1, \ldots, v_n)$ и $a \neq 0$. Отображение

$$x \longmapsto ax$$

является инъективным гомоморфизмом, образ которого содержится в свободном модуле, а потому в силу теоремы 1 свободен. Этот образ изоморфен M, и мы заключаем, что модуль M свободен, что и требовалось доказать.

Чтобы теперь получить подмодуль F, нам нужна лемма.

Лемма 1. *Пусть E, E' — модули, причем модуль E' свободен. Пусть $f\colon E \to E'$ — сюръективный гомоморфизм. Тогда существует свободный подмодуль F в B, такой, что ограничение f на F индуцирует изоморфизм F с E', и такой, что $E = F \oplus \operatorname{Ker} f$.*

Доказательство. Пусть $\{x'_i\}_{i \in I}$ — базис модуля E'. Обозначим через x_i, $i \in I$, элемент из E, для которого $f(x_i) = x'_i$. Пусть F — подмодуль в E, порожденный всеми элементами x_i, $i \in I$. Тогда сразу же видно, что семейство элементов $\{x_i\}_{i \in I}$ линейно независимо и поэтому модуль F свободен. Для заданного $x \in E$ существуют элементы $a_i \in R$, такие, что

$$f(x) = \sum a_i x'_i.$$

Тогда $x - \sum a_i x_i$ лежит в ядре f, а потому $E = \operatorname{Ker} f + F$. Ясно, что $\operatorname{Ker} f \cap F = 0$ и, следовательно, эта сумма прямая, что и доказывает лемму.

Применив лемму к гомоморфизму $E \to E/E_t$ в теореме 2, получим наше разложение $E = E_t \oplus F$. Размерность F однозначно определена, поскольку для любого такого разложения E в прямую сумму модуль F изоморфен E/E_t.

Размерность свободного модуля F в теореме 2 называется *рангом* модуля E.

Чтобы получить структурную теорему для конечно порожденных модулей над R, можно действовать дальше точно так же, как в слу-

чае абелевых групп. Мы приведем словарь, который позволит нам перенести доказательства по существу без всяких изменений.

Пусть E — модуль над R, $x \in E$. Отображение $a \longmapsto ax$ является гомоморфизмом R на подмодуль, порожденный элементом x, и ядро этого гомоморфизма является главным идеалом, порожденным некоторым элементом $m \in R$. Мы будем говорить, что m — *период* элемента x. Отметим, что период m определен однозначно с точностью до умножения на единицу (если $m \neq 0$). Элемент $c \in R$, $c \neq 0$, называется *показателем* модуля E (соответственно элемента x), если $cE = 0$ (соответственно $cx = 0$).

Пусть p — простой элемент. Обозначим через $E(p)$ подмодуль в E, состоящий из всех элементов x, обладающих показателем вида p^r $(r \geqslant 1)$. Подмодуль, содержащийся в $E(p)$, называется *p-подмодулем* в E.

Выберем раз и навсегда некоторую систему представителей для простых элементов кольца R (по модулю единиц). Например, если R — кольцо многочленов от одного переменного над полем, то возьмем в качестве представителей неприводимые многочлены со старшим коэффициентом 1.

Пусть $m \in R$, $m \neq 0$. Обозначим через E_m ядро отображения $x \longmapsto mx$. Оно состоит из всех элементов модуля E, имеющих показатель m.

Модуль E называется *циклическим*, если он изоморфен фактормодулю $R/(a)$ для некоторого элемента $a \in R$. Не теряя общности, мы можем считать, что a является произведением простых элементов из нашей системы представителей (если $a \neq 0$). Мы могли бы сказать, что a есть порядок нашего модуля.

Пусть $r_1, \ldots, r_s$ — целые числа $\geqslant 1$. Модулем *типа*

$$(p^{r_1}, \ldots, p^{r_s})$$

называется p-модуль E, изоморфный прямому произведению циклических модулей $R/(p^{r_i})$ $(i = 1, \ldots, s)$. Если простой элемент p фиксирован, то можно говорить, что модуль имеет тип $(r_1, \ldots, r_s)$ (относительно p).

Все доказательства из гл. I, § 10, проходят теперь без изменений. Там, где раньше мы оперировали с величиной какого-либо целого положительного числа m, теперь мы будем в аналогичном рассуждении оперировать с числом простых сомножителей в простом разложении элемента. Имея дело со степенью p^r простого элемента, можно считать, что порядок определяется числом r. Читатель проверит дальше сам, что все доказательства из гл. I, § 10 теперь применимы.

Однако мы будем развивать теорию заново, не предполагая ничего известным из гл. I, § 10. Таким образом, наше изложение будет независимым.

Теорема 3. *Пусть E — конечно порожденный периодический модуль $\neq 0$. Тогда E будет прямой суммой*

$$E = \prod_p E(p),$$

взятой по всем простым p, таким, что $E(p) \neq 0$. Каждый модуль $E(p)$ может быть записан в виде прямой суммы

$$E(p) = R/(p^{\nu_1}) \oplus \ldots \oplus R/(p^{\nu_s}),$$

где $1 \leqslant \nu_1 \leqslant \ldots \leqslant \nu_s$. Последовательность $\nu_1, \ldots, \nu_s$ однозначно определена.

Доказательство. Пусть a — некоторый показатель для E. Допустим, что $a = bc$, где $(b, c) = (1)$. Пусть $x, y \in R$ — такие элементы, что

$$1 = xb + yc.$$

Мы утверждаем, что $E = E_b \oplus E_c$. Наше первое утверждение получится затем по индукции из представления a в виде произведения степеней простых элементов. Пусть $v \in E$. Тогда

$$v = xbv + ycv.$$

Здесь $xbv \in E_c$, так как $cxbv = xav = 0$. Аналогично $ycv \in E_b$. Наконец, непосредственно видно, что $E_b \cap E_c = 0$. Следовательно, E есть прямая сумма E_b и E_c.

Теперь мы должны доказать, что $E(p)$ является прямой суммой указанного выше вида. Будем говорить, что элементы $y_1, \ldots, y_m$ некоторого модуля *независимы*, если, каково бы ни было соотношение

$$a_1 y_1 + \ldots + a_m y_m = 0,$$

где $a_i \in R$, мы должны иметь $a_i y_i = 0$ для всех i. (Отметим, что *независимость* не означает *линейной независимости*.) Тотчас видно, что элементы $y_1, \ldots, y_m$ тогда и только тогда независимы, когда модуль $(y_1, \ldots, y_m)$ обладает разложением в прямую сумму

$$(y_1, \ldots, y_m) = (y_1) \oplus \ldots \oplus (y_m)$$

циклических модулей (y_i), $i = 1, \ldots, m$.

Теперь нам нужен аналог леммы 1 для модулей, имеющих показатель, равный степени простого элемента.

Лемма 2. *Пусть E — периодический модуль показателя p^r $(r \geqslant 1)$, где p — некоторый простой элемент. Пусть $x_1 \in E$ — элемент периода p^r, $\bar{E} = E/(x_1)$ и $\bar{y}_1, \ldots, \bar{y}_m$ — независимые элементы из $\bar{E}$. Для всякого i существует представитель $y_i \in E$ класса $\bar{y}_i$, такой, что период y_i равен периоду $\bar{y}_i$. Элементы $x_1, y_1, \ldots, y_m$ независимы.*

Доказательство. Пусть элемент $\bar{y} \in \bar{E}$ имеет период p^n для некоторого $n \geqslant 1$ и y — представитель класса $\bar{y}$ в E. Тогда $p^n y \in (x_1)$ и, следовательно,

$$p^n y = p^s c x_1, \quad c \in R, \quad p \nmid c$$

для некоторого $s \leqslant r$. Если $s = r$, то мы видим, что y имеет тот же период, что и $\bar{y}$. Если $s < r$, то $p^s c x_1$ имеет период p^{r-s} и, следовательно, y имеет период p^{n+r-s}. Должно выполняться неравенство

$$n + r - s \leqslant r,$$

поскольку p^r — показатель для E. Таким образом, $s \geqslant n$ и мы видим, что

$$y - p^{s-n} c x_1$$

есть представитель для $\bar{y}$, период которого равен p^n.

Пусть y_i — представитель для $\bar{y}_i$, имеющий тот же период. Докажем, что элементы $x_1, y_1, \ldots, y_m$ независимы. Допустим, что $a, a_1, \ldots, a_m \in R$ такие элементы, что

$$a x_1 + a_1 y_1 + \ldots + a_m y_m = 0.$$

Тогда

$$a_1 \bar{y}_1 + \ldots + a_m \bar{y}_m = 0.$$

По предположению $a_i \bar{y}_i = 0$ для всякого i. Если p^{r_i} — период $\bar{y}_i$, то p^{r_i} делит a_i. Отсюда заключаем, что $a_i y_i = 0$ для всякого i и что, следовательно, $a x_1 = 0$; тем самым требуемая независимость доказана.

Чтобы теперь получить разложение $E(p)$ в прямую сумму, заметим сперва, что модуль $E(p)$ — конечно порожденный. Мы можем предполагать, не теряя общности, что $E = E(p)$. Пусть x_1 — элемент из E, период которого p^{r_1} таков, что число r_1 максимально. Пусть $\bar{E} = E/(x_1)$. Мы утверждаем, что $\dim \bar{E}_p$ как векторного пространства над R/pR строго меньше, чем $\dim E_p$. Действительно, если $\bar{y}_1, \ldots, \bar{y}_m$ — линейно независимые элементы из $\bar{E}_p$ над R/pR, то из леммы 2 вытекает, что $\dim E_p \geqslant m + 1$, так как мы всегда можем найти в (x_1) элемент, имеющий период p и не зависимый от $y_1, \ldots, y_m$. Следовательно, $\dim \bar{E}_p < \dim E_p$. Поэтому мы можем доказать существование разложения в прямую сумму по индукции. Если $\bar{E} \neq 0$, то существуют элементы $\bar{x}_2, \ldots, \bar{x}_s$, имеющие соответственно периоды $p^{r_2}, \ldots, p^{r_s}$ и такие, что $r_2 \geqslant \ldots \geqslant r_s$. В силу леммы 2 существуют представители $x_2, \ldots, x_s$ в E, такие, что x_i имеет период p^{r_i} и $x_1, \ldots, x_s$ независимы. Поскольку период p^{r_1}

был выбран максимальным, мы имеем неравенство $r_1 \geqslant r_2$ и наше разложение получено.

Единственность будет следствием более общей теоремы единственности, которую мы сейчас сформулируем.

Теорема 4. *Пусть E — конечно порожденный периодический модуль, $E \neq 0$. Тогда E изоморфен прямой сумме ненулевых слагаемых*

$$R/(q_1) \oplus \ldots \oplus R/(q_r),$$

где $q_1, \ldots, q_r$ — ненулевые элементы из R и $q_1 | q_2 | \ldots | q_r$. Последовательность идеалов $(q_1), \ldots, (q_r)$ однозначно определена предыдущими условиями.

Доказательство. Используя теорему 3, разложим E в прямую сумму p-подмодулей, скажем $E(p_1) \oplus \ldots \oplus E(p_l)$, а затем разложим каждый $E(p_i)$ в прямую сумму циклических подмодулей периодов $p_i^{r_{ij}}$. Символически мы изображаем это следующей диаграммой:

$$\begin{array}{l} E(p_1):\ r_{11} \leqslant r_{12} \leqslant \ldots \\ E(p_2):\ r_{21} \leqslant r_{22} \leqslant \ldots \\ \ldots\ldots\ldots\ldots \\ E(p_l):\ r_{l1} \leqslant r_{l2} \leqslant \ldots \end{array}$$

Предполагается, что горизонтальные строки имеют одинаковую длину, причем хотя бы одна из них состоит из ненулевых элементов. В начале же некоторых строк могут стоять показатели r_{ij}, равные нулю. Строки с исключенными из них нулями описывают типы модулей относительно простых элементов, указанных слева. Показатели r_{ij} расположены в возрастающем порядке, для всякого фиксированного $i = 1, \ldots, l$. Пусть $q_1, \ldots, q_r$ соответствуют столбцам этой матрицы показателей; другими словами, положим

$$\begin{array}{l} q_1 = p_1^{r_{11}} p_2^{r_{21}} \ldots p_l^{r_{l1}}, \\ q_2 = p_1^{r_{12}} p_2^{r_{22}} \ldots p_l^{r_{l2}} \\ \ldots\ldots\ldots\ldots \end{array}$$ [1])

Прямая сумма циклических модулей, представляемых первым столбцом, изоморфна $R/(q_1)$, потому что, как и в случае абелевых групп, прямая сумма циклических модулей, периоды которых взаимно просты, также является циклическим модулем. Аналогичное замечание справедливо для каждого столбца. Заметим, кроме того, что

[1]) Выписав последний элемент q_r, мы столкнулись бы с нелепыми показателями r_{ir}; к счастью, в явном виде они далее не выступают, так что особой необходимости в замене индекса r не ощущается. — *Прим. ред.*

наше доказательство в действительности располагает q_i в порядке возрастающей делимости, что и требовалось.

Теперь займемся единственностью. Пусть p — произвольный простой элемент. Предположим, что $E = R/(pb)$ для некоторого $b \in R$, $b \neq 0$. Тогда E_p есть подмодуль $bR/(pb)$, как это следует немедленно из однозначной разложимости на множители в R. Но ядром композиции отображений

$$R \to bR \to bR/(pb)$$

служит в точности (p). Таким образом, имеем изоморфизм

$$R/(p) \approx bR/(pb).$$

Пусть теперь модуль E представлен, как сказано в теореме, в виде прямой суммы из r членов. Элемент

$$v = v_1 \oplus \ldots \oplus v_r, \qquad v_i \in R/(q_i),$$

лежит в E_p в том и только в том случае, если $pv_i = 0$ для всех i. Следовательно, E_p есть прямая сумма ядер умножения на p в каждом члене. Но E_p — векторное пространство над $R/(p)$, и его размерность равна, таким образом, числу членов $R/(q_i)$, таких, что p делит q_i.

Предположим, что p — простой элемент, делящий q_1, а значит и q_i, для всех $i = 1, \ldots, r$. Пусть E имеет разложение в прямую сумму из s членов, удовлетворяющее условиям теоремы, скажем

$$E = R/(q'_1) \oplus \ldots \oplus R/(q'_s).$$

Тогда элемент p должен делить по крайней мере r элементов q'_j, откуда $r \leqslant s$. По симметрии $r = s$ и p делит q'_j для всех j.

Рассмотрим модуль pE. В силу предыдущего замечания, записав $q_i = pb_i$, мы будем иметь

$$pE \approx R/(b_1) \oplus \ldots \oplus R/(b_r)$$

и $b_1 \mid \ldots \mid b_r$. Некоторые из b_i могут быть единицами, но те, которые не являются единицами, по индукции определяют свой главный идеал однозначно. Следовательно, если $(b_1) = \ldots = (b_j) = 1$, но $(b_{j+1}) \neq 1$, то последовательность идеалов

$$(b_{j+1}), \ldots, (b_r)$$

однозначно определена. Это доказывает наше утверждение о единственности и завершает доказательство теоремы 4.

Идеалы $(q_1), \ldots, (q_r)$ называются *инвариантами* модуля E.

Следующую теорему можно было бы рассматривать как следствие теоремы 4. Мы дадим для нее независимое доказательство. Использоваться в дальнейшем она не будет.

Теорема 5. *Пусть F — свободный модуль над R и M — его конечно порожденный подмодуль $\neq 0$. Тогда существуют базис $\mathscr{B}$ модуля F, элементы этого базиса $e_1, \ldots, e_r$ и ненулевые элементы $a_1, \ldots, a_r \in R$, такие, что*

(i) *элементы $a_1e_1, \ldots, a_re_r$ образуют базис M над R;*

(ii) $a_i \mid a_{i+1}$ *для* $i = 1, \ldots, r-1$.

Последовательность идеалов $(a_1), \ldots, (a_r)$ однозначно определена предыдущими условиями.

Доказательство. Пусть λ — некоторый функционал на F, другими словами, элемент из $\mathrm{Hom}_R(F, R)$. Положим $J_\lambda = \lambda(M)$. Тогда J_λ есть идеал в R. Выберем λ_1 так, чтобы идеал $\lambda_1(M)$ был максимален в множестве идеалов $\{J_\lambda\}$, т. е. чтобы в множестве $\{J_\lambda\}$ не было строго большего идеала.

Пусть $\lambda_1(M) = (a_1)$. Тогда $a_1 \neq 0$. Действительно, в M имеется ненулевой элемент; в выражении этого элемента через какой-нибудь базис модуля F над R имеется ненулевая координата; беря проекцию на эту координату, мы получим функционал, значение которого на M не равно 0. Пусть $x_1 \in M$ — элемент, для которого $\lambda_1(x_1) = a_1$. Для любого функционала g мы должны иметь $g(x_1) \in (a_1)$ [непосредственно вытекает из максимальности $\lambda_1(M)$]. Записав x_1 через любой базис в F, мы увидим, что все его коэффициенты должны делиться на a_1. (Если некоторый коэффициент не делится на a_1, то спроектируем на этот коэффициент и получим невозможный функционал.) Поэтому мы можем записать $x_1 = a_1e_1$ для некоторого элемента $e_1 \in F$.

Теперь докажем, что F есть прямая сумма

$$F = Re_1 \oplus \mathrm{Ker}\,\lambda_1.$$

Так как $\lambda_1(e_1) = 1$, то ясно, что $R(e_1) \cap \mathrm{Ker}\,\lambda_1 = 0$. Кроме того, для всякого $x \in F$ разность $x - \lambda_1(x)e_1$ лежит в ядре λ_1. Следовательно, F есть сумма указанных подмодулей, которая должна быть прямой.

Отметим, что модуль $\mathrm{Ker}\,\lambda_1$ — свободный как подмодуль свободного модуля (теорема 1). Положим

$$F_1 = \mathrm{Ker}\,\lambda_1 \quad \text{и} \quad M_1 = M \cap \mathrm{Ker}\,\lambda_1.$$

Тогда видно, что

$$M = Rx_1 \oplus M_1.$$

Таким образом, M_1 — подмодуль в F_1, причем его размерность на единицу меньше, чем размерность модуля M. Мы можем поэтому закончить доказательство по индукции. Читателю предлагается проверить справедливость утверждения (ii).

Чтобы получить единственность, мы должны охарактеризовать нашу последовательность идеалов $(a_1), \ldots, (a_r)$ всецело в терминах F и M.

Лемма 3. *Пусть L_a^s — множество всех s-линейных знакопеременных форм на F, J_s — идеал в R, порожденный всеми элементами $f(y_1, \ldots, y_s)$, где $f \in L_a^s$ и $y_1, \ldots, y_s \in M$. Тогда*

$$J_s = (a_1 \ldots a_s).$$

Доказательство. Покажем сначала, что $J_s \subset (a_1 \ldots a_s)$. Действительно, всякий элемент $y \in M$ может быть записан в виде

$$y_1 = c_1 a_1 e_1 + \ldots + c_r a_r e_r.$$

Следовательно, если $y_1, \ldots, y_s \in M$ и f — полилинейная знакопеременная форма на F, то элемент $f(J_1, \ldots, J_s)$ равен сумме членов вида

$$c_{i_1} \ldots c_{i_s} a_{i_1} \ldots a_{i_s} f(e_{i_1}, \ldots, e_{i_s}).$$

Такой член отличен от нуля, только когда $e_{i_1}, \ldots, e_{i_s}$ различны, а в этом случае он делится на $a_1 \ldots a_s$ и, следовательно, J_s содержится в указанном идеале.

Обратно, покажем, что существует s-линейная знакопеременная форма, которая дает в точности это произведение. Мы получим эту форму с помощью определителей. Мы можем записать F в виде прямой суммы

$$F = (e_1, \ldots, e_r) \oplus F_r$$

для некоторого подмодуля F_r. Пусть $f_i (i = 1, \ldots, r)$ — линейное отображение $F \to R$, для которого $f_i(e_j) = \delta_{ij}$, причем f_i имеет значение 0 на F_r. Для $v_1, \ldots, v_s \in F$ положим

$$f(v_1, \ldots, v_s) = \det(f_i(v_j)), \qquad i, j = 1, \ldots, s.$$

Тогда f — полилинейная знакопеременная форма, которая принимает значение

$$f(e_1, \ldots, e_s) = 1$$

и, следовательно, значение

$$f(a_1 e_1, \ldots, a_s e_s) = a_1 \ldots a_s.$$

Это доказывает нашу лемму.

Единственность, утверждаемая в теореме 5, теперь очевидна, так как прежде всего идеал (a_1) определен однозначно, затем идеал $(a_1 a_2)$ также определен однозначно и, следовательно, их частное (a_2) определено однозначно и т. д. по индукции. Теорема 5 доказана.

Мы будем называть $(a_1), \ldots, (a_r)$ *инвариантами* подмодуля M в F.