§6. Векторы

Всюду в этом параграфе K по умолчанию обозначает коммутативное кольцо с единицей, а $\Bbbk$ — произвольное поле.

6.1. Модули над коммутативными кольцами. Аддитивная абелева группа[1] M называется *модулем* над коммутативным кольцом K или K*-модулем*, если задана операция $K\times M \to M$, которая переводит пары $(x, v) \in K \times M$ в элементы $x \cdot v \in M$ и обладает известными из курса геометрии свойствами умножения векторов на числа[2]:

$$\forall\, x, y \in K \quad \forall\, v \in M \quad x \cdot (y \cdot v) = (xy) \cdot v \tag{6-1}$$

$$\forall\, x, y \in K \quad \forall\, v \in M \quad (x + y) \cdot v = x \cdot v + y \cdot v \tag{6-2}$$

$$\forall\, x \in K \quad \forall\, u, w \in M \quad x \cdot (v + w) = x \cdot v + x \cdot w\,. \tag{6-3}$$

Если в кольце K есть единица и выполняется дополнительное свойство

$$\forall\, v \in V \quad 1 \cdot v = v\,, \tag{6-4}$$

модуль M называется *унитальным*. Всюду в этом параграфе мы по умолчанию рассматриваем именно такие модули. Унитальные модули над полями принято называть *векторными пространствами*. Я очень рассчитываю на то, что читатель уже имеет некоторый опыт работы с векторными пространствами, полученный в параллельном курсе геометрии[3]. Какой бы ни была природа элементов абелевой группы M и кольца K, продуктивно представлять себе первые именно как «векторы», а вторые — как «скаляры». По этой причине мы часто будем называть элементы модуля M *векторами*, а операцию $K \times M \to M$ — *умножением векторов на скаляры* из K. Часто бывает удобно записывать произведение вектора $v \in M$ на скаляр $x \in K$ не как $x \cdot v$, а как $v \cdot x$. По определению, мы считаем эти две записи эквивалентными обозначениями для одного и того же вектора и, как это обычно принято, будем частенько опускать в произведениях точку, считая по умолчанию, что $xv = vx \stackrel{\text{def}}{=} x \cdot v$.

Упражнение 6.1. Выведите из свойств (6-1) – (6-3), что в любом K-модуле M для всех $v \in M$ и $x \in K$ выполняются равенства $0 \cdot v = 0$ и $x \cdot 0 = 0$, а в унитальном модуле над коммутативным кольцом с единицей — равенство[4] $(-1) \cdot v = -v$.

Аддитивная абелева подгруппа $N \subseteq M$ в K-модуле M называется K*-подмодулем*, если она образует K-модуль относительно имеющейся в M операции умножения векторов на скаляры. Для этого необходимо и достаточно, чтобы $xw \in N$ для всех $x \in K$ и $w \in N$. Подмодули $N \subsetneq M$ называются *собственными*. Собственный подмодуль 0, состоящий из одного нуля, называется *тривиальным*.

Пример 6.1 (кольцо как модуль над собой)
Каждое коммутативное кольцо K является модулем над самим собой, где сложение векторов и умножение векторов на скаляры задаются сложением и умножением в K. Если в K имеется

[1] См. n° 2.1.2 на стр. 20.

[2] В роли векторов выступают элементы модуля M, а в роли чисел — элементы кольца K.

[3] Вариант такого курса см. на http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/1617/list.html. Все необходимые нам факты о векторных пространствах будут собраны в n° 6.4 ниже.

[4] Слева стоит произведение вектора $v \in M$ на скаляр $-1 \in K$, а справа — противоположный к v вектор $-v \in M$.

единица, K-модуль K является унитальным. K-подмодули $I \subset K$ — это в точности идеалы кольца K. В частности, коммутативное кольцо K с единицей является полем если и только если в K-модуле K нет нетривиальных собственных подмодулей[1].

Пример 6.2 (координатный модуль K^r)
Декартово произведение r экземпляров кольца K обозначается $K^r = K \times \cdots \times K$ и состоит из строк $a = (a_1, \dots, a_r)$, в которых $a_i \in K$. Сложение таких строк и их умножение их на скаляры $x \in K$ происходит покоординатно: для $a = (a_1, \dots, a_r)$, $b = (b_1, \dots, b_r)$ и $x \in K$ мы полагаем

$$a + b \stackrel{\text{def}}{=} (a_1 + b_1, \dots, a_r + b_r) \quad \text{и} \quad xa \stackrel{\text{def}}{=} (xa_1, \dots, xa_r)\,.$$

Пример 6.3 (абелевы группы как $\mathbb{Z}$-модули)
Каждая аддитивно записываемая абелева группа A может рассматриваться как унитальный $\mathbb{Z}$-модуль, в котором сложение векторов есть сложение в A, а умножение векторов на числа $\pm n$, где $n \in \mathbb{N}$, задаётся правилом $(\pm n) \cdot a \stackrel{\text{def}}{=} \pm(a + \cdots + a)$ с n слагаемыми a в скобках.

Упражнение 6.2. Удостоверьтесь, что эти операции удовлетворяют аксиомам (6-1) – (6-4).

6.1.1. Прямые произведения и прямые суммы. Из любого семейства K-модулей M_ν, занумерованных элементами ν произвольного множества $\mathcal{N}$, можно образовать прямое произведение $\prod_{\nu\in\mathcal{N}} M_\nu$, состоящее из всевозможных семейств $v = (v_\nu)_{\nu\in\mathcal{N}}$ векторов $v_\nu \in M_\nu$, занумерованных элементами $\nu \in \mathcal{N}$, как в n° 2.5 на стр. 26. Такие семейства можно поэлементно складывать и умножать на скаляры точно также, как мы это делали в n° 2.5 в прямых произведениях абелевых групп и коммутативных колец. А именно, сумма $v + w$ семейств $v = (v_\nu)_{\nu\in\mathcal{N}}$ и $w = (w_\nu)_{\nu\in\mathcal{N}}$ имеет ν-тым членом элемент $v_\nu + w_\nu$, а на ν-тым членом произведения xv семейства $v = (v_\nu)_{\nu\in\mathcal{N}}$ на скаляр $x \in K$ является элемент xv_ν. Модуль $\prod_{\nu\in\mathcal{N}} M_\nu$ называется *прямым произведением* модулей M_ν, а его подмодуль $\bigoplus_{\nu\in\mathcal{N}} M_\nu$, состоящий из всех семейств $v = (v_\nu)_{\nu\in\mathcal{N}}$ с конечным числом ненулевых векторов v_ν называется *прямой суммой* модулей M_ν. Для конечных множеств $\mathcal{N}$ прямые суммы совпадают с прямыми произведениями. Так, координатный модуль K^r из прим. 6.2 является прямой суммой и прямым произведением r экземпляров K-модуля K.

Пример 6.4 (многочлены и степенные ряды)
Обозначим через Kt^n множество одночленов вида at^n, где $a \in K$, а t — переменная. Каждое множество Kt^n является K-модулем, изоморфным модулю K. Прямая сумма $\bigoplus_{n\geqslant 0} Kt^n$ изоморфна модулю многочленов $K[t]$, а прямое произведение $\prod_{n\geqslant 0} Kt^n$ — модулю формальных степенных рядов $K[\![t]\!]$.

6.1.2. Пересечения и суммы подмодулей. Пересечение любого множества подмодулей произвольного K-модуля M также является подмодулем в M. Пересечение всех подмодулей, содержащих заданное множество векторов $A \subset M$, называется *K-линейной оболочкой* множества A или K-подмодулем, *порождённым* множеством A, и обозначается $\mathrm{span}(A)$ или $\mathrm{span}_K(A)$, если важно подчеркнуть, из какого кольца берутся константы. Линейная оболочка является наименьшим по включению K-подмодулем в M, содержащим A, и может быть иначе описана как множество всех конечных линейных комбинаций $x_1a_1 + \cdots + x_na_n$ векторов $a_i \in A$ с коэффициентами $x_i \in K$, ибо все такие линейные комбинации образуют подмодуль в M и содержатся во всех подмодулях, содержащих A.

[1] См. предл. 5.1 на стр. 65.

В противоположность пересечениям, объединения подмодулей почти никогда не являются подмодулями.

Упражнение 6.3. Покажите, что объединение двух подгрупп в абелевой группе является подгруппой если и только если одна из подгрупп содержится в другой.

K-линейная оболочка объединения произвольного множества подмодулей $U_\nu \subset M$ называется *суммой* этих подмодулей и обозначается $\sum_\nu U_\nu \stackrel{\text{def}}{=} \operatorname{span} \bigcup_\nu U_\nu$. Таким образом, сумма подмодулей представляет собою множество всевозможных конечных сумм векторов, принадлежащих этим подмодулям. Например,

$$U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1\,,\ u_2 \in U_2\}$$
$$U_1 + U_2 + U_3 = \{u_1 + u_2 + u_3 \mid u_1 \in U_1\,,\ u_2 \in U_2\,,\ u_3 \in U_3\} \quad \text{и т.д.}$$

Если подмодули $U_1, \dots, U_m \subset M$ таковы, что гомоморфизм сложения

$$U_1 \oplus \dots \oplus U_n \to U_1 + \dots + U_n \subset M\,, \quad (u_1, \dots, u_n) \mapsto u_1 + \dots + u_n\,, \tag{6-5}$$

является биекцией между $U_1 \oplus \dots \oplus U_n$ и $U_1 + \dots + U_n$, то сумму $U_1 + \dots + U_n$ называют *прямой* и тоже обозначают $U_1 \oplus \dots \oplus U_n$, как и в n° 6.1.1 выше. Биективность отображения (6-5) эквивалентна тому, что каждый вектор $w \in U_1 + \dots + U_n$ имеет *единственное* разложение $w = u_1 + \dots + u_n$, в котором $u_i \in U_i$ при каждом i.

Предложение 6.1
Сумма подмодулей $U_1, \dots, U_n \subset V$ является прямой если и только если каждый из подмодулей имеет нулевое пересечение с суммой всех остальных. В частности, сумма $U + W$ двух подмодулей прямая тогда и только тогда, когда $U \cap W = 0$.

Доказательство. Обозначим через W_i сумму всех подмодулей U_ν за исключением i-того. Если пересечение $U_i \cap W_i$ содержит ненулевой вектор $u_i = u_1 + \dots + u_{i-1} + u_{i+1} + \dots + u_n$, где $u_i \in U_i$ при всех i, то у этого вектора имеется два различных представления[1]

$$0 + \dots + 0 + u_i + 0 + \dots + 0 = u_1 + \dots + u_{i-1} + 0 + u_{i+1} + \dots + u_n\,.$$

Поэтому такая сумма не прямая. Наоборот, если $U_i \cap W_i = 0$ при всех i, то переписывая равенство

$$u_1 + \dots + u_n = w_1 + \dots + w_n\,, \text{ где } u_\nu, w_\nu \in U_\nu \text{ при всех } i,$$

как $u_i - w_i = \sum_{\nu \neq i}(w_\nu - u_\nu)$, видим, что этот вектор лежит в $U_i \cap W_i = 0$. Поэтому $u_i = w_i$ для каждого $i = 1, \dots, n$. □

Следствие 6.1
Для того чтобы модуль M распадался в прямую сумму собственных подмодулей $L, N \subset M$ необходимо и достаточно, чтобы $L + N = M$ и $L \cap N = 0$. □

[1] В левом отлично от нуля только i-е слагаемое, а в правом оно нулевое.

6.1.3. Фактор модули. Для любых K-модуля M подмодуля $N \subseteq M$ можно образовать *фактор модуль* M/N, состоящий из классов $[m]_N = m + N = m \pmod N = \{m' \in M \mid m' - m \in N\} \subset M$, представляющих собою аддитивные сдвиги подмодуля N на всевозможные элементы $m \in M$ или, что тоже самое, классы эквивалентности по отношению $m \equiv n \pmod N$ сравнимости по модулю N, означающему, что $m' - m \in N$. Сложение классов и их умножение на элементы кольца определяются обычными формулами $[m_1]_N + [m_2]_N \stackrel{\text{def}}{=} [m_1 + m_2]_N$ и $x \cdot [m]_N \stackrel{\text{def}}{=} [xm]_N$.

Упражнение 6.4. Проверьте, что отношение сравнимости по модулю N является эквивалентностью, а операции корректно определены и удовлетворяют аксиомам (6-1) – (6-4).

В частности, фактор кольцо K/I кольца K по идеалу $I \subset K$ является фактором K-модуля K по его K-подмодулю I, ср. с прим. 6.1 выше.

Упражнение 6.5. Пусть модуль M является прямой суммой $M = L \oplus N$ подмодулей $L, N \subset M$. Покажите, что $M/N \simeq L$ и $M/L \simeq N$.

Пример 6.5 (фактор модуля по идеалу кольца)
Для любого идеала $I \subset K$ и произвольного K-модуля M обозначим через

$$IM \stackrel{\text{def}}{=} \{x_1a_1 + \cdots x_na_n \mid x_i \in I\,,\ a_i \in M\,,\ n \in \mathbb{N}\}$$

K-подмодуль, образованный всевозможными линейными комбинациями элементов модуля M с коэффициентами из идеала I.

Упражнение 6.6. Проверьте, что IM действительно является K-подмодулем в M.

Фактор модуль M/IM обладает канонической структурой модуля над фактор кольцом K/I, которая корректно задаётся правилом $[x]_I \cdot [w]_{[IM]} = [xw]_{[IM]}$, где $[x]_I$ и $[a]_{[IM]}$ означают классы элементов $\lambda \in K$ и $w \in M$ соответственно по модулю идеала $I \subset K$ и подмодуля $IM \subset M$.

Упражнение 6.7. Убедитесь, что это правило корректно, и если $M = N_1 \oplus \cdots \oplus N_m$, то

$$IM = IN_1 \oplus \cdots \oplus IN_m \quad \text{и} \quad M/IM = (N_1/IN_1) \oplus \cdots \oplus (N_m/IN_m)$$

для любого идеала $I \subset K$. В частности, $K^n/IK^n = (K/I)^n$.

Пример 6.6 (кручение)
Элемент m модуля M над целостным[1] кольцом K называется *элементом кручения*, если $xm = 0$ для некоторого ненулевого $x \in K$. Например, любой класс $[k] \in \mathbb{Z}/(n)$ является элементом кручения в $\mathbb{Z}$-модуле $\mathbb{Z}/(n)$, поскольку $n[k] = [nk] = [0]$.

Упражнение 6.8. Убедитесь, что элементы кручения составляют подмодуль в M.

Этот подмодуль обозначается $\operatorname{Tors} M \stackrel{\text{def}}{=} \{m \in M \mid \exists\, x \neq 0 : xm = 0\}$ и называется *подмодулем кручения*. Если $\operatorname{Tors} M = 0$, то говорят, что модуль M *не имеет кручения*. Например, любой идеал целостного кольца K и любой подмодуль в координатном модуле K^n над таким кольцом не имеют кручения. Если $\operatorname{Tors} M = M$, то M называется *модулем кручения*. Например, фактор K/I по любому ненулевому идеалу $I \subset K$ является K-модулем кручения, поскольку для любого класса $[a] \in K/I$ и любого ненулегого $x \in I$ класс $x[a] = [xa] = [0]$, так как $xa \in I$.

Предложение 6.2
Для любого модуля M над целостным кольцом K фактор модуль $M/\operatorname{Tors}(M)$ не имеет кручения.

[1] См. n° 2.4.1 на стр. 25.

Доказательство. При ненулевом $x \in K$ равенство $x[m] = [xm] = [0]$ в $M/\operatorname{Tors}(M)$ означает, что $xm \in \operatorname{Tors}(M)$, т. е. $yxm = 0$ для некоторого ненулевого $y \in K$. Поскольку $xy \neq 0$, так как в кольце K нет делителей нуля, $m \in \operatorname{Tors} M$ и $[m] = [0]$. □

6.1.4. Дополнительные подмодули и разложимость. Подмодули $L, N \subset M$ называются *дополнительными*, если $M = L \oplus N$. В этой ситуации модуль M называется *разложимым*, а про подмодули L, N говорят, что они *отщепляются* от M прямыми слагаемыми. Модуль M, не представимый в виде прямой суммы своих собственных подмодулей называется *неразложимым*. Например, $\mathbb{Z}$-модуль $\mathbb{Z}$ неразложим, хотя и имеет собственные $\mathbb{Z}$-подмодули. В самом деле, каждый собственный подмодуль $I \subset \mathbb{Z}$ представляет собою главный идеал $I = (d)$. Согласно упр. 6.5, разложение $\mathbb{Z} = (d) \oplus N$ означает наличие в $\mathbb{Z}$ подмодуля $N \subset \mathbb{Z}$, изоморфного модулю кручения $\mathbb{Z}/(d)$. Но это невозможно, поскольку в $\mathbb{Z}$ нет кручения.

Упражнение 6.9. Рассмотрим $\mathbb{Z}$-подмодуль $N \subset \mathbb{Z}^2$, порождённый векторами $(2,1)$ и $(1,2)$. Покажите, что $N \simeq \mathbb{Z}^2$, $M/N \simeq \mathbb{Z}/(3)$, и не существует подмодуля $L \subset M$, такого что $M = L \oplus N$.

6.2. Гомоморфизмы модулей. Отображение $\varphi : M \to N$ между K-модулями M и N называется *K-линейным* или *гомоморфизмом K-модулей*, если оно перестановочно со сложением векторов и умножением векторов на скаляры, т. е. для всех $x \in K$ и $u, w \in M$

$$\varphi(u + w) = \varphi(u) + \varphi(w) \quad \text{и} \quad \varphi(xu) = x\varphi(u). \tag{6-6}$$

Поскольку K-линейное отображение $\varphi : M \to N$ является гомоморфизмом абелевых групп, оно обладает всеми свойствами из n° 2.6 на стр. 27. В частности, $\varphi(0) = 0$ и $\varphi(-u) = -\varphi(u)$ для всех $u \in M$, а инъективность φ равносильна тому, что ядро

$$\ker \varphi = \varphi^{-1}(0) = \{u \in M \mid \varphi(u) = 0\}$$

состоит из одного нуля. Все непустые слои любого K-линейного гомоморфизма φ являются аддитивными сдвигами его ядра, т. е. $\varphi^{-1}(\varphi(u)) = u + \ker \varphi$ для всех $u \in M$.

Упражнение 6.10. Убедитесь, что ядро и образ K-линейного гомоморфизма $\varphi : M \to N$ являются подмодулями в M и в N соответственно, а сопоставление $[v]_{\ker \varphi} \mapsto \varphi(v)$ корректно задаёт изоморфизм K-модулей $M/\ker \varphi \to \operatorname{im} \varphi$.

Предостережение 6.1. Именуемое в школе «линейной функцией» отображение $\varphi : K \to K$, задаваемое правилом $\varphi(x) = ax + b$, где $a, b \in K$ фиксированы, является K-линейным в смысле предыдущего определения только при $b = 0$. Если же $b \neq 0$, то φ не перестановочно ни со сложением, ни с умножением на числа.

Пример 6.7 (дифференцирование)
Кольцо многочленов $K[x]$ с коэффициентами в коммутативном кольце K можно рассматривать и как K-модуль. Оператор дифференцирования $D = \frac{d}{dx} : K[x] \to K[x]$, $f(x) \mapsto f'(x)$, является гомоморфизмом K-модулей, поскольку перестановочен со сложением многочленов и умножением многочленов на константы, но не является гомоморфизмом колец, так как не перестановочен с умножением многочленов друг на друга.

6.2.1. Модули гомоморфизмов. Отображения $Z \to M$ из любого множества Z в произвольный K-модуль M можно складывать и умножать на числа из K, применяя эти операции к значениям рассматриваемых отображений в каждой точке $z \in Z$. А именно, для любой пары отображений $\varphi, \psi : X \to M$ и числа $x \in K$ сумма $\varphi+\psi : X \to M$ и произведение $x\varphi : X \to M$ действуют на точки $z \in Z$ по правилам

$$\varphi + \psi : z \mapsto \varphi(z) + \psi(z) \quad \text{и} \quad x\varphi : z \mapsto x\varphi(z). \tag{6-7}$$

Эти операции очевидно удовлетворяют аксиомам (6-1) – (6-4), поскольку все эти аксиомы выполняются в модуле M и проверяются отдельно над каждой точкой $z \in Z$. Таким образом, множество M^Z всех отображений $Z \to M$ является K-модулем. Нулевым элементом этого модуля служит *нулевое отображение*, переводящее все элементы множества Z в нуль.

Упражнение 6.11. Убедитесь, что K-модуль M^Z изоморфен прямому произведению[1] $\prod_{z\in Z} M_z$ одинаковых копий $M_z = M$ модуля M, занумерованных элементами $z \in Z$.

Если множество Z тоже является K-модулем, то сумма $\varphi + \psi$ двух K-линейных отображений $\varphi, \psi : N \to M$ и произведение $z\varphi$ гомоморфизма φ с любым скаляром $x \in K$ тоже K-линейны.

Упражнение 6.12. Убедитесь в этом.

Таким образом, K-линейные отображения K-модуля N в K-модуль M составляют в модуле M^N всех отображений из N в M K-подмодуль. Он обозначается $\mathrm{Hom}_K(M, N)$ и называется *модулем K-линейных гомоморфизмов* из M в N.

Упражнение 6.13. Покажите, что композиция K-линейных гомоморфизмов тоже K-линейна.

Пример 6.8 (гомоморфизмы абелевых групп)
Как мы видели в прим. 6.3 на стр. 79, любые две абелевы группы A и B могут рассматриваться как модули над кольцом $\mathbb{Z}$.

Упражнение 6.14. Убедитесь, что отображение множеств $A \to B$ является гомоморфизмом абелевых групп[2] если и только если оно $\mathbb{Z}$-линейно.

В аддитивной абелевой группе вычетов $\mathbb{Z}/(m)$, рассматриваемой как $\mathbb{Z}$-модуль, описанное в прим. 6.3 умножение класса $[k]_m \in \mathbb{Z}/(m)$ на число $z \in \mathbb{Z}$ происходит по правилу $z \cdot [k]_m = [zk]_m$. Тем самым, каждый класс $[k]_m = k \cdot [1]_m$ можно получить, умножая класс $[1]_m$ на подходящее целое число. Поэтому любой $\mathbb{Z}$-линейный гомоморфизм $\varphi : \mathbb{Z}/(m) \to N$ в произвольный $\mathbb{Z}$-модуль N однозначно восстанавливается по вектору $\varphi([1]_m) \in N$: значение φ на произвольном классе $[k]_m$ будет равно $\varphi([k]_m) = \varphi(k \cdot [1]_m) = k\varphi([1]_m)$. При этом вектор $\varphi([1]_m) \in N$ не может быть выбран произвольно: так как в $\mathbb{Z}/(m)$ выполняется соотношение $m \cdot [1]_m = [m]_m = 0$, в модуле N должно выполняться соотношение $m \cdot \varphi([1]_m) = \varphi(m \cdot [1]_m) = \varphi(0) = 0$. В частности, если в модуле N нет ненулевых векторов v с $mv = 0$, то $\varphi([1]_m) = 0$, и это означает, что из $\mathbb{Z}/(m)$ в N нет никаких $\mathbb{Z}$-линейных отображений, кроме нулевого. Например, это так для $N = \mathbb{Z}/(n)$, если $\mathrm{нод}(m, n) = 1$: в этом случае класс $[m]_n$ обратим в кольце $\mathbb{Z}/(n)$ и равенство $[0]_n = m[k]_n = [mk]_n = [m]_n[k]_n$ возможно только при[3] $[k]_n = [0]_n$. Мы заключаем, что $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(m), \mathbb{Z}/(n)) = 0$ при $\mathrm{нод}(m, n) = 1$, т. е. любой гомоморфизм абелевых групп $\mathbb{Z}/(m) \to \mathbb{Z}/(n)$ имеет при взаимно простых m и n нулевой образ.

[1] См. n° 6.1.1 на стр. 79.
[2] См. n° 2.6 на стр. 27.
[3] Чтобы убедиться в этом, надо умножить левую и правую части равенства в кольце $\mathbb{Z}/(n)$ на класс $[m]_n^{-1}$.

Упражнение 6.15. Покажите, что любой линейный гомоморфизм $\varphi : M \to N$ в свободный от кручения модуль N переводит $\mathrm{Tors}(M)$ в нуль.

Предложение 6.3
Для любых K-модулей M, N и подмодуля $L \subset M$ гомоморфизмы $f : M \to N$, тождественно зануляющиеся на подмодуле L, образуют в K-модуле $\mathrm{Hom}_K(M, N)$ подмодуль, изоморфный K-модулю $\mathrm{Hom}_K(M/L, N)$. Изоморфизм сопоставляет зануляющемуся на L гомоморфизму $f : M \to N$ гомоморфизм $f_L : M/L \to M$, корректно задаваемый правилом $[v]_L \mapsto f(v)$. Обратный изоморфизм сопоставляет K-линейному отображению $g : M/L \to M$ его композицию $f = g\pi_L$ с эпиморфизмом факторизации $\pi_L : M \twoheadrightarrow M/L$.

Доказательство. Если гомоморфизмы $f, g : M \to N$ переводят L в нуль, то любая их K-линейная комбинация $xf + yg$ тоже переводит L в нуль. Следовательно, такие гомоморфизмы образуют K-подмодуль в $\mathrm{Hom}_K(M, N)$. Если $f : M \to N$ переводят L в нуль, то правило $f_L : [v]_L \mapsto f(v)$ корректно задаёт гомоморфизм $f_L : M/L \to M$, поскольку для любого вектора $w = v + u$ с $u \in L$ имеем $f(w) = f(v) + f(u) = f(v)$, ибо $f(u) = 0$. Сопоставление $f \mapsto f_L$ задаёт K-линейный гомоморфизм $\mathrm{Hom}_K(M, N) \to \mathrm{Hom}_K(M/L, N)$ с нулевым ядром. Он сюръективен, поскольку любой K-линейный гомоморфизм $g : M/L \to N$ имеет вид $g = f_L$ для K-линейного гомоморфизма $f : M \to N$, который действует по правилу $f(v) = g([v]_L)$ и является композицией g с гомоморфизмом факторизации $\pi_L : M \twoheadrightarrow M/L$. □

Предложение 6.4
Рассмотрим семейство K-модулей M_μ, занумерованных элементами μ произвольного множества $\mathcal{M}$. Для любого K-модуля N имеется канонический изоморфизмом K-модулей

$$\prod_{\mu\in\mathcal{M}} \mathrm{Hom}_K(M_\mu, N) \xrightarrow{\sim} \mathrm{Hom}_K\Big(\bigoplus_{\mu\in\mathcal{M}} M_\mu,\, N\Big), \tag{6-8}$$

который переводит семейство K-линейных гомоморфизмов $f_\mu : M_\mu \to N$ в гомоморфизм

$$\bigoplus f_\mu : \bigoplus_{\mu\in\mathcal{M}} M_\mu \to N, \tag{6-9}$$

отображающий каждое семейство векторов $(w_\mu)_{\mu\in\mathcal{M}}$ с конечным числом ненулевых членов в сумму $\sum_{\mu\in\mathcal{M}} f_\mu(w_\mu)$ с конечным числом ненулевых слагаемых.

Доказательство. Отображение (6-8) очевидно является K-линейным гомоморфизмом. Обратное к (6-8) отображение переводит каждый K-линейный гомоморфизм $: \bigoplus_{\mu\in\mathcal{M}} M_\mu \to N$ в семейство гомоморфизмов $f_\mu : M_\mu \to N$, где каждый $f_\nu = f\iota_\nu$ является композицией f с вложением $\iota_\nu : M_\nu \hookrightarrow \bigoplus_{\mu\in\mathcal{M}} M_\mu$, отправляющем каждый вектор $u \in M_\nu$ в семейство $(w_\mu)_{\mu\in\mathcal{M}} \in \in \bigoplus_{\mu\in\mathcal{M}} M_\mu$, в котором $w_\nu = u$ и $w_\mu = 0$ при $\mu \neq \nu$. □

Пример 6.9 (продолжение прим. 6.4 на стр. 79)
В прим. 6.4 мы видели, что модуль многочленов $K[t] \simeq \bigoplus_{n\geqslant 0} Kt^n$ можно воспринимать как прямую сумму модулей $Kt^n \simeq K$. Применительно к этому случаю предл. 6.4 утверждает, среди прочего, что каждое K-линейное отображение $f : K[t] \to K$ однозначно задаётся последовательностью K-линейных отображений $f_n = f|_{Kt^n} : Kt^n \to K$ — ограничений отображения f на подмодули $Kt^n \subset K[t]$. Каждое отображение f_n в свою очередь однозначно задаётся

числом $\varphi_n = f_n(t^n) = f(t^n)$ — значением отображения f на базисном мономе t^n. Последовательность чисел $\varphi_n \in K$ может быть любой, и отвечающее такой последовательности K-линейное отображение $f\colon K[t] \to K$ переводит многочлен $a(t) = a_0 + a_1 t + \cdots + a_m t^m$ в число $f(a) = \varphi_0 a_0 + \varphi_1 a_1 + \cdots + \varphi_m a_m$. Таким образом, модуль $\mathrm{Hom}_K(K[t], K)$ изоморфен прямому произведению счётного множества копий модуля K, т. е. модулю формальных степенных рядов $K[\![x]\!]$. Изоморфизм сопоставляет последовательности (φ_n) её *производящую функцию* $\Phi(x) = \sum_{n\geqslant 0} \varphi_n x^n \in K[\![x]\!]$. Например, для любого $\alpha \in K$ *гомоморфизм вычисления*

$$\mathrm{ev}_\alpha\colon K[t] \to K\,, \quad f \mapsto f(\alpha)\,,$$

сопоставляющий многочленам их значения в точке $\alpha \in K$ и действующий на базисные мономы по правилу $t^n \mapsto \alpha^n$, имеет $\varphi_n = \alpha^n$ и задаётся рядом $\sum_{n\geqslant 0} \alpha^n x^n = (1-\alpha x)^{-1} \in K[\![x]\!]$.

6.3. Образующие и соотношения. Говорят, что вектор v из K-модуля M *линейно выражается* над K через векторы $w_1, \ldots, w_m$, если $v = x_1 w_1 + \cdots x_m w_m$ для некоторых $x_1, \ldots, x_m \in K$. Правая часть этой формулы называется *линейной комбинацией* векторов $w_i \in V$ с коэффициентами $x_i \in K$. Линейная комбинация, в которой все коэффициенты $x_i = 0$, называется *тривиальной*.

Мы говорим, что множество $Z \subset M$ *порождает* модуль M, если любой вектор $v \in M$ является линейной комбинацией конечного числа векторов из Z, т. е. $v = x_1 u_1 + \cdots + x_m u_m$ для некоторых $x_i \in K$, $w_i \in G$ и $m \in \mathbb{N}$. Множество векторов $Z \subset M$ называется *линейно зависимым*, если некоторая нетривиальная конечная линейная комбинация векторов из Z обращается в нуль, т. е. существуют такие $k \in \mathbb{N}$, $u_1, \ldots, u_k \in Z$ и $x_1, \ldots, x_k \in K$, что $x_1 u_1 + \cdots + x_k u_k = 0$, но при этом не все x_i равны нулю. Каждая такая такая линейная комбинация называется *линейным соотношением* на векторы из множества Z.

Упражнение 6.16. Покажите, что в модуле без кручения сумма подмодулей $U_1, \ldots, U_m$ прямая[1] если и только если любой набор ненулевых векторов $u_1, \ldots, u_m$, в котором $u_i \in U_i$ при каждом i, линейно независим.

Множество $E \subset M$ называется *базисом* модуля M, если каждый вектор $v \in M$ единственным образом линейно выражается через векторы из E, т. е. $v = \sum_{e\in E} x_e e$, где все $x_e \in K$ и только конечное множество из них отлично от нуля, и равенство $\sum_{e\in E} x_e e = \sum_{e\in E} y_e e$ двух таких сумм с конечным числом ненулевых слагаемых равносильно равенству коэффициентов $x_e = y_e$ при каждом векторе $e \in E$. Коэффициенты x_e единственного линейного выражения вектора v через базисные векторы $e \in E$ называются *координатами* вектора v в базисе E.

Модуль M, обладающий базисом, называется *свободным*. Иначе можно сказать, что свободный модуль с базисом E представляет собою прямую сумму $\bigoplus_{e\in E} Ke$ одинаковых копий $Ke = K$ модуля K, занумерованных элементами $e \in E$. В частности, свободный модуль над целостным кольцом K не имеет кручения[2].

Лемма 6.1
Множество векторов $E \subset M$ тогда и только тогда является базисом K-модуля M, когда оно линейно независимо и порождает M.

Доказательство. Пусть множество векторов E порождает K-модуль M. Если существует линейное соотношение $x_1 e_1 + \cdots + x_n e_n = 0$, в котором $e_i \in E$ и $x_1 \neq 0$, то оно у нулевого вектора

[1] См. n° 6.1.2 на стр. 79.
[2] См. прим. 6.6 на стр. 81.

$0 \in M$ имеется два различных представления в линейной комбинации векторов из E: первое даётся указанным соотношением, второе имеет вид $0 = 0 \cdot e_1$. Наоборот, если множество E линейно независимо и имеется равенство $\sum_{e\in E} x_e e = \sum_{e\in E} y_e e$, в обоих частях которого имеется лишь конечное число ненулевых коэффициентов, то перенося все ненулевые слагаемые в одну часть, получаем конечное линейное соотношение $\sum_{e\in E}(x_e - y_e)\cdot e = 0$, возможное только если все коэффициенты нулевые, т. е. только когда $x_e = y_e$ при всех e. □

Пример 6.10 (примеры несвободных модулей)
Аддитивная группа вычетов $\mathbb{Z}/(m)$, рассматриваемая как $\mathbb{Z}$-модуль в духе прим. 6.8 на стр. 83, не свободна, поскольку в свободном модуле нет кручения. Модуль $\mathbb{Z}/(m)$ порождается над $\mathbb{Z}$ одним вектором $[1]_m$, и этот вектор линейно зависим, поскольку удовлетворяет нетривиальному линейному соотношению $m \cdot [1]_m = 0$.

Упражнение 6.17. Покажите, что класс $[n]_m \in \mathbb{Z}/(m)$ порождает $\mathbb{Z}$-модуль $\mathbb{Z}/(m)$ если и только если $\text{нод}(m, n) = 1$.

Идеал I целостного кольца K, рассматриваемый как K-модуль, свободен если и только если он главный. В самом деле, образующая d главного идеала $I = (d)$ порождает его как K-модуль и линейно независима в силу целостности кольца. Напротив, если идеал $I \subset K$ не является главным, то любой порождающий его набор элементов линейно зависим, поскольку любые два различных элемента $a, b \in K$ линейно зависимы над K, ибо удовлетворяют линейному соотношению $b \cdot a - a \cdot b = 0$. Например, в кольце $K = \mathbb{Q}[x, y]$ многочленов с рациональными коэффициентами идеал $I = (x, y)$, состоящий из многочленов без свободного члена, порождается над $\mathbb{Q}[x, y]$ векторами x и y, которые линейно зависимы над $\mathbb{Q}[x, y]$, ибо $y \cdot x - x \cdot y = 0$, и не может быть порождён одним вектором, поскольку x и y не имеют необратимых общих делителей.

Пример 6.11 (многочлены и ряды, продолжение прим. 6.9 на стр. 84)
Кольцо многочленов $K[t]$ является свободным модулем со счётным базисом из мономов t^n, так как каждый многочлен по определению является конечной K-линейной комбинацией каких мономов, и равенство многочленов означает равенство их коэффициентов при каждом мономе. Иначе говоря, модуль $K[t]$ является прямой суммой модулей $Kt^n \simeq K$. В модуле формальных степенных рядов $K[\![t]\!]$, который является прямым произведением тех же самых модулей Kt^n, мономы t^n базиса уже *не образуют*, поскольку никакой ряд с бесконечным числом ненулевых коэффициентов не является конечной линейной комбинацией мономов.

Упражнение 6.18. Покажите, что при $K \neq 0$ модуль $K[\![t]\!]$ не порождается никаким счётным множеством векторов.

В кольце $\mathbb{R}[\![t]\!]$ несложно предъявить несчётное линейно независимое множество векторов. Например, геометрические прогрессии $(1-\alpha t)^{-1} = 1+\alpha t+\alpha^2 t^2+\ldots$, где α пробегает $\mathbb{R}$, линейно независимы, поскольку равенство $x_1(1-\alpha_1 t)^{-1} + \cdots + x_k(1-\alpha_k t)^{-1} = 0$ в кольце $\mathbb{R}[\![t]\!]$ после приведения к общему знаменателю превращается в равенство

$$x_1 \prod_{\nu\neq 1}(1-\alpha_\nu t) + x_2 \prod_{\nu\neq 2}(1-\alpha_\nu t) + \cdots + x_k \prod_{\nu\neq k}(1-\alpha_\nu t) = 0$$

в кольце $\mathbb{R}[t]$. Последовательно подставляя в него значения $t = 1/\alpha_i$, мы заключаем, что $x_i = 0$ для каждого $i = 1, \ldots, k$.

Пример 6.12 (задание модуля образующими и соотношениями)
Рассмотренный нами в прим. 6.2 на стр. 79 координатный модуль K^n свободен, поскольку каждый вектор $v = (x_1, \dots, x_n)$ единственным образом представляется в виде линейной комбинации $v = x_1 e_1 + \cdots + x_n e_n$ стандартных базисных векторов

$$e_i = (0, \dots, 0, 1, 0, \dots, 0), \tag{6-10}$$

единственной ненулевой координатой которых является единица, стоящая у вектора e_i на i-том месте. Если K-модуль M линейно порождается над K векторами $w_1, \dots, w_m$, то имеется K-линейный эпиморфизм $\pi\colon K^m \twoheadrightarrow M$, $(x_1, \dots, x_n) \mapsto x_1 w_1 + \cdots + x_m w_m$. Его ядро $R = \ker \pi$ называется *модулем соотношений* между образующими w_i, поскольку оно состоит из всех таких строчек чисел $(x_1, \dots, x_n) \in K^m$, которые задают линейное соотношение $x_1 w_1 + \cdots + x_m w_m = 0$ между образующими w_i в модуле M. Таким образом, каждый конечно порождённый K-модуль M имеет вид $M = K^m / R$ для некоторого числа $m \in \mathbb{N}$ и некоторого подмодуля $R \subset K^m$.

6.4. Векторные пространства. В этом разделе собраны необходимые для дальнейшего свойства векторных пространств. Поскольку большинство из них, скорее всего, уже обсуждались в курсе геометрии, обращаться к этому разделу можно лишь по мере необходимости.

Если кольцо скаляров представляет собою поле $\Bbbk$, то наличие $\Bbbk$-линейной зависимости между теми или иными векторами равносильна возможности линейно выразить один этих векторов через остальные. Скажем, если в линейном соотношении $x_1 w_1 + \cdots + x_m w_m = 0$ коэффициент $x_m \neq 0$, то

$$v_m = -\frac{x_1}{x_m}\, v_1 - \cdots - \frac{x_{m-1}}{x_m}\, v_{m-1},$$

и аналогичное линейное выражение можно получить для любого вектора, входящего в линейное соотношение с ненулевым коэффициентом. По этой причине каждое векторное пространство над любым полем свободно, т. е. обладает базисом.

Теорема 6.1 (существование базиса)
В каждом отличном от нуля векторном пространстве V для любого[1] линейно независимого множества векторов A и любого[2] линейно порождающего V множества векторов $B \supset A$ существует базис E, содержащий A и содержащийся в B.

Доказательство. Линейно независимые множества векторов $X \subseteq V$ со свойством $A \subseteq X \subseteq B$ образуют частично упорядоченное отношением включения множество, удовлетворяющее лемме Цорна[3]. А именно, в качестве верхней грани линейно упорядоченной цепи вложенных друг в друга линейно независимых множеств можно взять их объединение. Оно линейно независимо, поскольку все векторы в любой конечной линейной комбинации векторов из такого объединения лежат в одном достаточно большом множестве цепочки, а оно линейно независимо. По лемме Цорна существует такое линейно независимое множество E со свойством $A \subseteq E \subseteq B$, что для любого линейно независимого множества X со свойством $A \subseteq X \subseteq B$ включение $E \subseteq X$ влечёт равенство $E = X$. Покажем, что E линейно порождает V. Для этого достаточно убедиться, что каждый вектор $b \in B \smallsetminus E$ линейно выражается через E. Так как множество $E \cup \{b\}$ строго больше E, оно линейно зависимо. Поскольку само множество E линейно независимо, всякая

[1] В том числе пустого.
[2] В том числе совпадающего со всем V.
[3] См. лем. 1.3 на стр. 18.

линейная зависимость между векторами из $E \cup \{b\}$ содержит с ненулевым коэффициентом вектор b. Тем самым, он линейно выражается через векторы из E. □

Следствие 6.2
Каждое ненулевое векторное пространство имеет базис, и любой базис любого подпространства можно дополнить до базиса во всём пространстве. □

6.4.1. Размерность. Все базисы любого векторного пространства V над полем $\Bbbk$ равномощны. Для векторного пространства V, которое линейно порождается конечным набором векторов, это вытекает из следующей леммы.

Лемма 6.2 (лемма о замене)
Если векторы $w_1, \dots, w_m$ линейно порождают векторное пространство V над полем $\Bbbk$, а векторы $u_1, \dots, u_k \in V$ линейно независимы, то $m \geqslant k$ и векторы w_i можно перенумеровать так, что набор векторов $u_1, \dots, u_k, w_{k+1}, w_{k+2}, \dots, w_m$, полученный заменой первых k векторов w_i векторами u_i, тоже порождает V.

Доказательство. Пусть $u_1 = x_1 w_1 + \dots + x_m w_m$. Так как векторы u_i линейно независимы, $u_1 \neq 0$ и среди коэффициентов x_i есть хоть один ненулевой. Перенумеруем векторы w_i так, чтобы $x_1 \neq 0$. Поскольку вектор w_1 линейно выражается через u_1 и $w_2, \dots, w_m$ как

$$w_1 = \frac{1}{x_1} u_1 - \frac{x_2}{x_1} w_2 - \dots - \frac{x_m}{x_1} w_m ,$$

векторы $u_1, w_2, \dots, w_m$ порождают V. Далее действуем по индукции. Пусть для очередного $i < k$ векторы $u_1, \dots, u_i, w_{i+1}, \dots, w_m$ порождают V. Тогда

$$u_{i+1} = y_1 w_1 + \dots + y_m w_m + x_{i+1} w_{i+1} + \dots + x_m w_m .$$

В силу линейной независимости векторов u_ν вектор u_{i+1} нельзя линейно выразить только через векторы $u_1, \dots, u_k$. Поэтому в предыдущем разложении присутствует с ненулевым коэффициентом хоть один из оставшихся векторов w_j. Следовательно, $m > i$ и мы можем занумеровать оставшиеся w_j так, чтобы $x_{i+1} \neq 0$. Теперь, как и на первом шагу, вектор w_{i+1} линейно выражается через векторы $u_1, \dots, u_{i+1}, w_{i+2}, \dots, w_m$. Тем самым, эти векторы линейно порождают V, что воспроизводит индуктивное предположение. □

Следствие 6.3
Если векторное пространство V обладает базисом из n векторов, то каждый базис пространства V состоит из n векторов, и всякий линейно независимый набор из n векторов, а также всякий порождающий набор из n векторов являются базисами.

Доказательство. Так как каждый базис одновременно линейно независим и порождает[1] V, все базисы состоят из одинакового количества векторов по лем. 6.2. По той же лемме при замене любого базиса любыми n линейно независимыми векторами получится порождающий набор, т. е. тоже базис. По теор. 6.1 любой порождающий набор из n векторов содержит в себе базис. Так как последний тоже состоит из n векторов, он совпадает с исходным набором. □

[1] См. лем. 6.1 на стр. 85.

Определение 6.1
Векторные пространства с конечными базисами называются *конечномерными*. Количество векторов в базисе конечномерного векторного пространства V называется *размерностью* пространства V и обозначается $\dim V$.

Следствие 6.4
В конечномерном пространстве V каждое векторное подпространство $U \subset V$ тоже конечномерно, и $\dim U \leqslant \dim V$, где равенство возможно только при $U = V$. □

Замечание 6.1. (координатные модели конечномерного пространства) Каждое n-мерное векторное пространство V над полем $\Bbbk$ изоморфно координатному пространству $\Bbbk^n$. При этом $\Bbbk$-линейные изоморфизмы $\Bbbk^n \xrightarrow{\sim} V$ взаимно однозначно соответствует базисам в V, поскольку для любого базиса $v_1, \dots, v_n$ в V отображение

$$f : \Bbbk^n \to V\,, \quad (x_1, \dots, x_n) \mapsto x_1 v_1 + \dots + x_n v_n\,, \tag{6-11}$$

линейно и биективно, и наоборот, образы $v_i = f(e_i)$ стандартных базисных векторов[1] $e_i \in \Bbbk^n$ при любом линейном изоморфизме $f : \Bbbk^n \xrightarrow{\sim} V$ составят базис пространства V, причём отображение f действует в этом случае в точности по формуле (6-11).

Упражнение 6.19. Покажите, что векторное пространство бесконечномерно если и только если в нём есть линейно независимый набор из сколь угодно большого числа векторов.

Теорема 6.2 (равномощность базисов)
В каждом векторном пространстве все базисы равномощны.

Доказательство. Пусть базис B строго мощнее базиса E. Так как в конечномерном пространстве это невозможно по сл. 6.3, оба базиса бесконечны. Каждый вектор $e \in E$ является линейной комбинацией конечного множества векторов $B_e \subset B$. Так как множество E бесконечно, объединение $B_E = \bigcup_{e\in E} B_e$ всех множеств B_e равномощно E.

Упражнение 6.20. Убедитесь в этом.

Тем самым, существует вектор $b \in B$, не лежащий в B_e. Линейно выражая b через векторы базиса E, а каждый из входящих в это выражение векторов $e \in E$ — через векторы из B_e, мы получим линейное выражение вектора $b \in B \smallsetminus B_E$ через векторы из B_E. Тем самым, множество B линейно зависимо. □

Следствие 6.5
Всякое более мощное, чем базис, множество векторов линейно зависимо. □

6.4.2. Продолжение линейных отображений. Каждое линейное отображение $f : U \to W$, заданное на каком-либо подпространстве U любого векторного пространства V, может быть продолжено (многими способами) на всё пространство V, т. е. всегда существует такое линейное отображение $g : V \to W$, что $g|_U = f$. Чтобы построить его, выберем произвольный базис B в U, дополним его до базиса $E = B \sqcup C$ в V и рассмотрим любое отображение множеств $g : E \to W$, такое что $g(b) = f(b)$ для всех $b \in B$.

Упражнение 6.21. Убедитесь, что отображение $g : V \to W$, переводящее вектор $v = \sum_{e\in E} x_e e$ в вектор $g(e) = \sum_{e\in E} x_e g(e) \in W$ линейно и совпадает с f на любом векторе $v \in U$.

[1] См. формулу (6-10) на стр. 87.

6.4.3. Размерности конечномерных подпространств и фактор пространств. В этом разделе собраны стандартные факты о размерностях, которые будут повсеместно использоваться в дальнейшем.

Предложение 6.5
Для любых конечномерных подпространств U_1, U_2 в произвольном[1] векторном пространстве V выполняется равенство $\dim(U_1) + \dim(U_2) = \dim(U_1 \cap U_2) + \dim(U_1 + U_2)$.

Доказательство. Выберем какой-нибудь базис $u_1, \dots, u_k$ в $U_1 \cap U_2$ и дополним его векторами $v_1, \dots, v_r$ и $w_1, \dots, w_s$ до базисов в подпространствах U_1 и U_2 соответственно. Достаточно показать, что векторы $u_1, \dots, u_k,\ v_1, \dots, v_r,\ w_1, \dots, w_s$ образуют базис пространства $U_1 + U_2$. Ясно, что они его порождают. Допустим, что они линейно зависимы. Поскольку каждый из наборов $u_1, \dots, u_k, v_1, \dots, v_r$ и $u_1, \dots, u_k, w_1, \dots, w_s$ в отдельности линейно независим, в равенстве

$$x_1u_1 + \dots + x_ku_k + y_1v_1 + \dots + y_rv_r + z_1w_1 + \dots + z_sw_s = 0$$

имеются как векторы v_i, так и векторы w_j. Перенося $w_1, \dots, w_s$ в правую часть, получаем равенство между вектором из U_1 и вектором из U_2, означающее, что этот вектор лежит в пересечении $U_1 \cap U_2$. Но тогда в его разложении по базисам пространств U_1 и U_2 нет векторов v_i и w_j — противоречие. □

Следствие 6.6
Для любых подпространств U_1, U_2 конечномерного векторного пространства V

$$\dim(U_1 \cap U_2) \geqslant \dim(U_1) + \dim(U_2) - \dim(V)\,.$$

В частности, $U_1 \cap U_2 \neq 0$ при $\dim(U_1) + \dim(U_2) > \dim V$.

Доказательство. Это вытекает из предл. 6.5 и неравенства $\dim(U_1 + U_2) \leqslant \dim V$. □

Следствие 6.7 (дополнительные подпространства)
Следующие два свойства векторных подпространств U_1, U_2 в конечномерном векторном пространстве V эквивалентны[2]: (1) $V = U_1 \oplus U_2$ (2) $U_1 \cap U_2 = 0$ и $\dim(U_1) + \dim(U_2) = \dim(V)$.

Доказательство. При $U_1 \cap U_2 = 0$ равенство $\dim(U_1) + \dim(U_2) = \dim(V)$ равносильно равенству $\dim(U_1 + U_2) = \dim V$, означающему, что $U_1 + U_2 = V$. □

Предложение 6.6
Если V конечномерно, то для любого линейного отображения $f : V \to W$

$$\dim \ker f + \dim \operatorname{im} f = \dim V\,. \tag{6-12}$$

Доказательство. Выберем базис $u_1, \dots, u_k \in \ker f$, дополним его векторами $e_1, \dots, e_m$ до базиса в V и покажем, что векторы $f(e_1), \dots, f(e_m)$ образуют базис в $\operatorname{im} f$. Они порождают образ, так как для любого вектора $v = \sum y_iu_i + \sum x_je_j \in V$

$$f(v) = \sum y_i f(u_i) + \sum x_j f(e_j) = \sum x_j f(e_j)\,.$$

[1] Не обязательно конечномерном.

[2] Обладающие этими свойствами подпространства U_1, U_2 называются *дополнительными*.

Они линейно независимы, поскольку равенство $0 = \sum x_i f(e_i) = f(\sum x_i e_i)$ означает, что вектор $\sum x_i e_i$ лежит в $\ker f$, т. е. является линейной комбинацией векторов u_i, что возможно только когда все $x_i = 0$. □

Следствие 6.8
В конечномерном пространстве V для любого подпространства $U \subset V$ выполняется равенство $\dim U + \dim V/U = \dim V$, и если некоторый базис $u_1, \dots, u_n$ подпространства U дополняется до базиса в V векторами $w_1, \dots, w_m$, то их классы $[w_1]_U, \dots, [w_m]_U$ образуют базис в V/U.

Доказательство. Применяем предл. 6.6 и его доказательство к эпиморфизму $V \twoheadrightarrow V/U$. □

Следствие 6.9
Следующие свойства линейного отображения $F : V \to V$ из пространства V в себя эквивалентны друг другу: (1) F изоморфизм (2) $\ker F = 0$ (3) $\operatorname{im} F = V$.

Доказательство. Свойства (2) и (3) равносильны друг другу по предл. 6.6, а их одновременное выполнение равносильно (1), ибо свойство (2) эквивалентно инъективности f. □

Пример 6.13 (интерполяция с кратными узлами)
Зафиксируем несколько различных чисел $a_1, \dots, a_n \in \Bbbk$ и произвольно зададим для каждого числа a_i несколько значений b_{i0}, b_{i1}, … , $b_{im_i} \in \Bbbk$. Пусть общее число заданных значений $(m_1 + 1) + \cdots + (m_n + 1) = m + 1$. Покажем, что существует единственный такой многочлен $g \in \Bbbk[x]$ степени не выше m, что при каждом i сам этот многочлен и первые его m_i производных принимают в точке a_i заданные $m_i + 1$ значений $g(a_i) = b_{i0}$, $g'(a_i) = b_{i1}$, … , $g^{(m_i)}(a_i) = b_{im_i}$, где $g^{(k)}(x) = d^k g(x)/dx^k$ означает k-ю производную от многочлена g. Для этого произвольным образом занумеруем $m + 1$ пар чисел (i, j) с $1 \leqslant i \leqslant n$, $0 \leqslant j \leqslant m_j$ и выпишем их в одну строчку в порядке возрастания номеров. Рассмотрим отображение $F : \Bbbk[x]_{\leqslant m} \to \Bbbk^{m+1}$, переводящее каждый многочлен g степени $\deg g \leqslant m$ в набор значений[1] $g^{(j)}(a_i)$, записанных в строчку согласно зафиксированному только что порядку на множестве индексов (i, j).

Упражнение 6.22. Убедитесь, что отображение F линейно и $\ker F = 0$.

Так как $\dim \operatorname{im} F = \dim \Bbbk[x]_{\leqslant m} = \dim \Bbbk^{m+1}$, мы заключаем, что отображение F биективно, что и требовалось.

6.5. Свободные модули. Свободные модули над произвольным коммутативным кольцом K с единицей имеют много общего с векторными пространствами. Свободный K-модуль F с базисом E является прямой суммой свободных модулей $Ke \simeq K$, порождённых базисными векторами $e \in E$. Каждое K-линейное отображение $f : F \to M$ такого модуля в произвольный K-модуль M однозначно восстанавливается по набору своих значений $w_e = f(e)$ на базисных векторах $e \in E$ и действует на произвольный вектор по правилу[2]

$$f : \sum_{e \in E} x_e e \mapsto \sum_{e \in E} x_e w_e , \tag{6-13}$$

причём формула (6-13) задаёт линейное отображение $f : F \to M$ при любом выборе векторов $w_e \in M$, и это отображение f переводит каждый базисный вектор e в соответствующий вектор w_e. Мы получаем следующий результат, являющийся частным случаем предл. 6.4 на стр. 84.

[1] Где для единообразия обозначений мы полагаем $g^{(0)} \stackrel{\text{def}}{=} g$.

[2] Напомню, что обе суммы в (6-13) имеют лишь конечное число ненулевых коэффициентов x_e.

Теорема 6.3
Для свободного K-модуля F с базисом E и любого K-модуля M сопоставление K-линейному отображению $f : F \to M$ его ограничения на подмножество $E \subset F$ задаёт K-линейный изоморфизм между модулем $\mathrm{Hom}_K(F, M)$ всех K-линейных отображений $F \to M$ и модулем M^E всех отображений[1] множества E в множество M. □

Теорема 6.4
Все базисы свободного модуля M над произвольным коммутативным кольцом K с единицей равномощны.

Доказательство. Рассмотрим произвольный максимальный идеал $\mathfrak{m} \subset K$. Как мы видели в прим. 6.5 на стр. 81, фактор модуль $M/\mathfrak{m}M$ любого K-модуля M по подмодулю $\mathfrak{m}M$, состоящему из всевозможных конечных линейных комбинаций векторв из M с коэффициентами их $\mathfrak{m}$, является векторным пространством над полем $\Bbbk = K/\mathfrak{m}$. Свободный K-модуль F с базисом E является прямой суммой свободных модулей $Ke \simeq K$, порождённых базисными векторами $e \in E$, а его подмодуль $\mathfrak{m}F \subset F$ — прямой суммой их подмодулей $\mathfrak{m}e \subset Ke$. Поэтому[2] фактор $F/\mathfrak{m}F$ является прямой суммой одномерных векторных пространств $(K/\mathfrak{m})[e]$, порождённых классами векторов $e \in E$. Таким образом, мощность множества E совпадает с мощностью базиса векторного пространства $F/\mathfrak{m}F$. Поскольку все базисы векторного пространства равномощны, все базисы в F тоже равномощны. □

Определение 6.2
Свободный модуль F с конечным базисом называется *модулем конечного ранга*, а число элементов в базисе называется *рангом* свободного модуля F и обозначается $\mathrm{rk}\, F$.

Теорема 6.5
Всякий ненулевой подмодуль N свободного модуля M конечного ранга над произвольным кольцом главных идеалов K тоже свободен, и $\mathrm{rk}\, N \leqslant \mathrm{rk}\, M$.

Доказательство. Индукция по $m = \mathrm{rk}\, M$. При $m = 1$ модуль $M \simeq K$ и любой подмодуль $N \subset K$ представляет собою главный идеал $(d) \subset K$, который является свободным K-модулем ранга 1 с базисом d, как мы видели в прим. 6.10 на стр. 86. Пусть теперь $m > 1$. Зафиксируем в M базис $e_1, \ldots, e_m$ и будем записывать векторы из M строчками их координат в этом базисе. Первые координаты всевозможных векторов $v \in N$ образуют идеал $(d) \subset K$. Если $d = 0$, подмодуль N содержится в свободном модуле ранга $m-1$ с базисом $e_2, \ldots, e_m$. По индукции, такой модуль N свободен и $\mathrm{rk}\, N \leqslant (m-1)$. Если $d \neq 0$, обозначим через $v_1 \in N$ какой-нибудь вектор с первой координатой d. Тогда $N = Kv_1 \oplus N'$, где $N' \subset N$ — подмодуль, состоящий из векторов с нулевой первой координатой. Действительно, $Kv_1 \cap N' = 0$, и любой вектор $v \in N$ представляется в виде $xv_1 + w$, где $x = x_1(v)/d \in K$, а $w = v - xv_1 \in N'$. Модуль Kv_1, порождённый вектором v_1, свободен ранга 1, поскольку в объемлющем свободном модуле M нет кручения. Модуль N' содержится в свободном модуле ранга $m-1$ с базисом $e_2, \ldots, e_m$. По индукции N' свободен и $\mathrm{rk}\, N' \leqslant (m-1)$. Поэтому $N = Kv_1 \oplus N'$ тоже свободен и $\mathrm{rk}\, N = 1 + \mathrm{rk}\, N' \leqslant m$. □

[1] См. n° 6.2.1 на стр. 83.
[2] См. упр. 6.7 на стр. 81.

Упр. 6.1. Пусть $0 \cdot v = w$. Тогда $w + v = 0 \cdot v + 1 \cdot v = (0 + 1) \cdot v = 1 \cdot v = v$. Прибавляя к обеим частям этого равенства $-v$, получаем $w = 0$. Из равенства $0 \cdot v = 0$ вытекает, что $x \cdot 0 = x(0 \cdot v) = (x \cdot 0) \cdot v = 0 \cdot v = 0$. Наконец, равенство $(-1) \cdot v + v = (-1) \cdot v + 1 \cdot v = ((-1) + 1) \cdot v = 0 \cdot v = 0$ означает, что $(-1) \cdot v = -v$.

Упр. 6.3. Пусть $A \not\subseteq B$ — две подгруппы в абелевой группе. Выберем $a \in A \smallsetminus B$. Если $A \cup B$ является подгруппой, то $\forall\, b \in B\ a + b \in A \cup B$, но $a + b \notin B$, поскольку $a \notin B$. Следовательно, $a + b \in A$, откуда $b \in A$, т. е. $B \subseteq A$.

Упр. 6.4. Все проверки проводятся дословно также, как для классов вычетов по модулю идеала коммутативного кольца (ср. с упр. 5.7 на стр. 68).

Упр. 6.7. Если $\lambda' = \lambda + x$ и $a' = a + v$, где $x \in I$, $v \in IM$, то $\lambda' a' = \lambda a + (xa + \lambda v + xv)$, где взятая в скобки сумма лежит в IM.

Упр. 6.8. Если $x_1 m_1 = 0$ и $x_2 m_2 = 0$ для ненулевых $x_1, x_2 \in K$, то $x_1 x_2 (m_1 \pm m_2) = 0$ и $x_1 x_2 \neq 0$, так как в K нет делителей нуля. Кроме того, $\forall\, y \in K\ x_1(y m_1) = x_2(y m_2) = 0$.

Упр. 6.10. Ядро и образ любого гомоморфизма абелевых групп являются абелевыми подгруппами согласно n° 2.6 на стр. 27. Если гомоморфизм K-линеен, то обе эти подгруппы выдерживают умножение на элементы из K, поскольку $x\varphi(u) = \varphi(xu)$ и $\varphi(u) = 0 \Rightarrow \varphi(xu) = x\varphi(u) = 0$. Последнее утверждение является переформулировкой того, что $\varphi(v_1) = \varphi(v_2) \iff v_1 - v_2 \in \ker \varphi$. Убедитесь, однако, что отображение $[v] \mapsto \varphi(v)$ K-линейно.

Упр. 6.11. Сопоставьте отображению $\varphi : X \to M$ семейство его значений $\big(\varphi(x)\big)_{x \in X} \in \prod_{x \in X} M_x$.

Упр. 6.13. Прямая проверка: если f и g оба K-линейны, то $fg(xa + yb) = f(xg(a) + yg(b)) = xfg(a) + yfg(b)$ для любых скаляров x, y и векторов a, b.

Упр. 6.15. Если $x \in K \smallsetminus 0$ и $m \in M$ таковы, что $xm = 0$, то $x\varphi(m) = \varphi(mx) = \varphi(0) = 0$.

Упр. 6.16. Если векторы u_i ненулевые, то векторы $x_i u_i$ тоже ненулевые при любых $x_i \neq 0$. Поэтому любое нетривиальное линейное соотношение между векторами u_i является нетривиальным линейным разложением нулевого вектора в сумму векторов из подмодулей U_i.

Упр. 6.18. Множество всевозможных конечных K-линейных комбинаций счётного множества векторов равномощно $K \times \mathbb{N}$, т. е. дизъюнктному объединению счётного множества одинаковых копий множества K, тогда как множество $K[\![t]\!]$ равномощно множеству $K^{\mathbb{N}}$ всевозможных отображений $\mathbb{N} \to K$, которое строго мощнее, чем $K \times \mathbb{N}$ (используйте рассуждение Кантора).

Упр. 6.20. Очевидно, что E вкладывается в B_E, а B_E вкладывается в дизъюнктное объединение

$$\bigsqcup_{n \geqslant 1} \underbrace{E \sqcup \ldots \sqcup E}_{n}$$

счётного множества копий множества E, которое в силу того, что множество E бесконечно, равномощно E. Тем самым, B_E вкладывается в E. Остаётся применить теорему Кантора – Бернштейна.

Упр. 6.22. Линейность F вытекает из того, что отображение дифференцирования

$$d/dx : \Bbbk[x] \to \Bbbk[x], \quad g \mapsto g',$$

и все отображения вычисления $\mathrm{ev}_a : \Bbbk[x] \to \Bbbk$, $g \mapsto g(a)$, где $a \in \Bbbk$, линейны и композиция линейных отображений тоже линейна. Если $g \in \ker F$, то каждое число $a_i \in \Bbbk$ является как

минимум (m_i+1)-кратным корнем многочлена g, и g делится на $\prod_i (x-a_i)^{m_i+1}$, что невозможно при $g \neq 0$, поскольку степень этого произведения равна $m+1 > \deg g$.