Георгий Потошин, 2024

Алгебра I, листочек 7

1. **Постройте базисы над полем $\Bbbk$ в алгебрах: матриц $\mathcal{Mat}_n(\Bbbk)$; верхнетреугльных матриц; многочленов с коэффициентами в $\Bbbk$. Запишите законы умножения в этих базисах.**

   Очевидно, что на матрицы можно смотреть как на наборы чисел, а значит и как на элементы свободного модуля. Тогда матричные единицы $\{e_{i,j}\}$, в которых на одном месте стоит единица, а на остальных нули, образуют базис алгебры, более того часто матрицы строят как свободная алгебра на матричных единицах. Умножение матричных единиц происходит по следующему правилу $e_{i,j}e_{k,l} = \delta_{j,k}e_{i,l}$.

   Базис верхнетреугольных матриц состоит из матричных единиц $e_{i,j}$, для которых $i \leq j$. Умножение остается таким же, проверим замкнутость по нему: пусть $i \leq j$ и $k \leq l$, если произведение $e_{i,j}e_{k,l}$ не нулевое, то $j = k$, тогда по транзитивности $\leq$ мы получим $i \leq l$, а значит результат произведения также врехнетреугольный.

   Так как полиномы имеют моном максимальной степени, то каждый полином раскладывается в линейную комбинацию x^n. Тогда $\{x^n\}$ – базис алгебры. Это нельзя формализовать из наивного определения полиномов, но если из рассматривать как элементы группового (наверно правильнее говорить моноидального, так как $\mathbb{N}$ не группа) кольца $K[\mathbb{N}]$, то это утверждение верно по определению. Произведение ведёт себя следующим образом, $x^n x^m = x^{n+m}$.

2. **Постройте канонические изоморфизмы**

   (a) $U + W \cong U \bigoplus W/(U \cap W)$ **для подпространств** $U, W \leq V$

   Если прочитать это соотношение как $U+W \cong U \bigoplus (W/(U\cap W))$, то изоморфизм нельзя канонически построить, так как придётся выбирать базис, и поэтому мы пойдём по иному пути, который верен в более общем случае для модулей.

   $U + W \cong (U \bigoplus W)/(U \cap W)$. Построим точную последовательность

   $$0 \to U \cap W \to U \bigoplus W \to U + W \to 0$$

   где нетривиальные стрелки $i = a \mapsto (a, -a)$ и $\pi = (a, b) \mapsto a + b$ в том порядке, в котором они появляются в последовательности. Её точность тривиальна, а тогда согласованно с ней искомое соотношение, которое следует для теоремы об изоморфизме для π, то есть $U + W = \mathrm{Im}(\pi) \cong U \bigoplus W/\mathrm{Ker}(\pi) = U \bigoplus W/\mathrm{Im}(i) \cong U \bigoplus W/U \cap W$, так как $i : U \cap W \to U \bigoplus W$ – вложение и факторизация происходит по нему. Сопутствующий изоморфизм будет следующим:

   $$[(a, b)] \in U \bigoplus W/U \cap W \mapsto a + b$$

   (b) **[Теорема Нетер об изоморфизме]** $(U+W)/U \cong W/(U\cap W)$ **для подмодулей** $U, W \leq V$

   Построим сюръективный морфизм $\phi = a \in W \mapsto a + U \in (U + W)/U$, ядро которого $W \cap U$. Применим теорему о гомоморфизме и получим нужное соотношение $W/(U \cap W) \cong (U + W)/U$. Сопутствующий изомрфизм $w + U \cap W \in W/(U \cap W) \mapsto w + U \in (U + W)/U$.

   (c) $V/(U + W) \cong (V/U)/(W/(U \cap W))$ **для подмодулей** $U, W \leq V$

   Здесь правый фактор не происходит по стандартному вложению, так как одно не подмножество другого, поэтому это соотношение образовано из точной последовательности:

   $$0 \to W/(U \cap W) \to V/U \to V/(U + W) \to 0$$

   где нетривиальные стрелки следующие $i = w + U \cap W \mapsto w + U$ и $\pi = v + U \mapsto v + U + W$. Первая инъективна так как для $w \in W$, $w + U = U$ означает, что $w \in U$, а тогда $w \in U \cap W$ и $w + U \cap W = U \cap W$. Вторая стрелка инъективна, так как для $v + U + W$ можно найти прообраз $v + U$. Последовательность точна, так как с одной стороны для $w \in W$ $w + U + W = U + W$, а значит $\mathrm{Im}(i) \subseteq \mathrm{Ker}(\pi)$, с другой стороны, если $v + U + W = U + W$, то $v \in U + W$, тогда $v = u + w$ для некоторых $u \in U$ и $w \in W$. Тогда прообраз равен $v+U = w+u+U = w+U \in \mathrm{Im}(i)$ и мы получили второе включение. Осталось использовать теорему о гомеоморфизме $V/(U+W) = \mathrm{Im}(\pi) \cong (V/U)/\mathrm{Ker}(\pi) = (V/U)/\mathrm{Im}(i) \cong (V/U)/(W/(U \cap W))$. Сопутствующий изоморфизм следующий $[v+U] \in (V/U)/(W/(U \cap W)) \mapsto v + U + W$.

(d) $V/U \cong (V/W)/(U/W)$ **для подмодулей** $W \leq U \leq V$ Построим точную последовательность

$$0 \to U/W \to V/W \to V/U \to 0$$

где нетривиальные морфизмы $i = u+W \mapsto u+W$ и $\pi = v+W \mapsto U$. Единственная вещь достойная проверки – это точность посередине. С одной стороны для $u \in U$ $\pi(u+W) = U$, а значит $\mathrm{Im}(i) \leq \mathrm{Ker}(\pi)$, в другую сторону проверка также очевидна. Тогда согласно этой последовательности построим изоморфизм $V/U = \mathrm{Im}(\pi) \cong (V/W)/\mathrm{Ker}(\pi) = (V/W)/\mathrm{Im}(i) \cong (V/W)/(U/W)$, сопутствующий изоморфизм $[v+W] \mapsto v + U$.

Здесь во всех случаях корректность изоморфизма гарантирована теоремой о гомоморфизме.

3. **Постройте канонический изоморфизм** $V \cong U \oplus V/U$**, где** $U \leq V$**.**

Я не рассматриваю в доказуемое соотношение правую часть как сумму пространства и фактор пространства, так как тогда изоморфизм не будет каноническим, так как придется выбирать базисы. С другой стороны разложение на компоненты

Этот случай совпадает с первым пунктом прошлого задания, а тогда я вкратце повторю шаги. Построим точную последовательность

$$0 \to U \to U \oplus V \to V$$

где нетривиальные стрелки $i = u \mapsto (u, -u)$ и $\pi = (u,v) \mapsto u + v$. Точность гарантирует соотношение и индуцирует изоморфизм $[(u,v)] \mapsto u + v$.

4. **Докажите, что**

Здесь я изменю порядок пунктов, чтобы решение одних основывалось на предыдущих результатах.

(a) $\dim(U \oplus W) = \dim(U) + \dim(W)$ **для пространств** U, W

Выберем базис $\{u_i\}_{i\in I}$ в U и базис $\{w_j\}_{j\in J}$ в W, тогда базисом $U \oplus W$ будет $\{(u_i, 0)\}_{i\in I} \sqcup \{(0, w_j)\}_{j\in J}$, так как очевидно порождает $U \oplus W$ и линейно независим, если $\sum(u_i, 0)k_i + \sum(0, w_j)l_j = (0,0) = (\sum u_i k_i, \sum w_j l_j)$, то в каждой координате линейная комбинация занулить, так как там нулевые линейные комбинация элементов базисов компонент суммы. Дизъюнктивная сумма по определению складывает кардиналы базисов, а значит формула суммы верна.

(b) $\dim(V) = \dim(U) + \dim(V/U)$ **для подпространства** $U \leq V$

Для этого построим не канонический изоморфизм, выберем базис $\{u_i\}$ в U и дополним его элементами $\{v_i\}$ до базиса V. Тогда элемент $x = \sum u_i x_i + \sum v_j x_j$ мы отправим в $(\sum u_i x_i, \sum v_j x_j + U)$. Как нетрудно заметить, мы получим сюрьективный морфизм векторных пространств. Осталось проверить, его инъективность, она верна, так как если $(\sum u_i x_i, \sum v_j x_j + U) = (0,0)$, то по свойству базиса все координаты при u_i занулятся, но и так как тогда $\sum v_j x_j \in U$, то $\sum v_j x_j = \sum u_j k_j$, но по свойству базиса все координаты должны занулится, а поэтому координаты при v_j нулевые, ядро тривиально, морфизм инъективен, а значит теперь мы показали, что он изоморфизм.

Тогда по прошлому пункту из $V \cong U \oplus V/U$ заключаем, что $\dim(V) = \dim(U) + \dim(V/U)$.

(c) $\dim(U+W) = \dim(U) + \dim(W) - \dim(U \cap W)$ **для подпространств** $U, W \leq V$

По прошлому заданию мы знаем, что $U+W \cong (U \oplus W)/(U \cap W)$, а тогда $\dim(U+W) = \dim(U \oplus W) - \dim(U \cap W) = \dim(U) + \dim(W) - \dim(U \cap W)$

(d) $\dim(V) - \dim(U) = \dim(V/(\mathrm{Im}(f))) - \dim(\mathrm{Ker}(f))$ **для гомоморфизма** $f : U \to V$

Мы знаем, что $\mathrm{Im}(f) \cong U/\mathrm{Ker}(f)$, а значит $\dim(U) = \dim(\mathrm{Im}(f)) + \dim(\mathrm{Ker}(f))$. С другой стороны $\dim(V/\mathrm{Im}(f)) = \dim(V) - \dim(\mathrm{Im}(f)) = \dim(V) - (\dim(U) - \dim(\mathrm{Ker}(f))$, откуда мы и получаем искомое тождество.

5. **Докажите, что целочисленными элементарными преобразованиями строк и столбцов любую целочисленную матрицу можно привести к диагональному виду с числами** $d_1, \ldots, d_k$ **на диагонали, так что** $d_1 | \ldots | d_k$**.**

Мы постараемся показать, что любую матрицу $A_0 \in \mathcal{M}at_{n\times m}(\mathbb{Z})$ можно привести к виду

$$\begin{pmatrix} a_1 & 0 \dots 0 \\ 0 & \\ \vdots & A_1 \\ 0 & \end{pmatrix}$$

где a_1 делит все коэффициенты в A_1. Так как тогда можно продолжить алгоритм для матричного нижнего блока и так как целочисленные преобразования сохраняют наибольший общий делитель, то приведенный вида подматрицы A_1 на блоки a_2 и A_2 будет удовлетворять условию $a_1|a_2$.

Этап 1. Для начала, если матрица ненулевая, то можно перестановками строк и столбцов добиться того, чтобы в верхнем левом угле стоял не нуль. В $\mathbb{Z}$ у каждого числа есть только конечный набор делителей, и мы будем этим активно пользоваться.

Этап 2. Дальше мы добьёмся того, чтобы число a в верхнем левом угле делило все числа в первой строке и в первом столбце. Мы этого добьёмся следующей процедурой, если некоторое число b в первой строке или столбце не делится на a, то мы воспользуемся соотношением Безу и найдем целые числа α, β, что $a\alpha + b\beta = \gcd(a, b) = d$. Заменим $a' = a/d$ и $b' = b/d$. Тогда у нас будет $a'\alpha + b'\beta = 1$. Этому соотношению будет соответствовать матрица с детерминантом 1.

$$P_0 = \begin{pmatrix} \alpha & \beta \\ -b' & a' \end{pmatrix}$$

Покажем, что эта матрица образована произведением элементарных матриц, соответствующих элементарным преобразованиям. Для этого обозначим $a = (1, 0)$ и $b = (0, 1)$, что можно записать в матричном виде

$$\left(\begin{array}{cc|c} 1 & 0 & a' \\ 0 & 1 & b' \end{array}\right)$$

Применим алгоритм евклида по строкам, в котором каждое действие соответствует элементарному преобразованию по окончанию алгоритма мы получим

$$\left(\begin{array}{cc|c} x & y & 1 \\ z & w & 0 \end{array}\right)$$

где матрица имеет детерминант 1. Это означает, что $xa' + yb' = 1$ и $za' + wb' = 0$. Так как $\mathrm{gdc}(a', b') = 1$ и $\mathrm{gdc}(z, w) = 1$, иначе детерминант не был бы 1, то нетрудно видеть, решив это диофантовое уравнение, что $z = -b'$ и $w = a'$. Тогда матрица слева это в точности матрица P_0. Она раскладывается в произведение элементарных.

Теперь если b лежит в первом столбце в строке i, то мы строим матрицу P по матрице из единичной матрицы I_m, занулив в ней 1 и i строки и поместив в $(1, 1)$ $(P_0)_{1,1}$, в $(i, 1)$ $(P_0)_{2,1}$, в $(1, i)$ $(P_0)_{1,2}$ и в (i, i) $(P_0)_{i,i}$. Очевидно, что эта матрица также получена теми же элементарными преобразованиями, что и P_0, но на иных строках 1 и i. Теперь если b

Домножение на P, как нетрудно убедится запишет в $(1, 1)$ $\gcd(a, b)$. Мы будем продолжать этот процесс, пока верхний левый коэфициент не будет делить все числа в первом столбце и в первой строке. Количество итераций ограничено количеством простых делителей верхнего левого коэффициента, так как каждая уменьшает их количество, а значит вычислимая ситуация наступит за конечное время.

Дальше мы вычтим первую строку и первый столбец необходимое число раз, чтобы занулить все коэффициенты в первой строке и в первом столбце, кроме верхнего левого коэффициента, после этого, если наш верхний левый коэффициент не делит какой-нибудь коэффициент из нижней блочной матрицы, то мы добавим строку с этим коэффициентом в первую и начнем заново процедуру этапа 2. Это имеет смысл, так как такое добавление не изменит наш верхний левый коэффициент, потому как в первом столбце под первой строчкой везде нули, и это действие перенесет неделящийся коэффициент наверх, относительно которого вновь можно считать нод. По той же причине, что и в прошлый раз вычисления закончатся за конечное время.

Теперь у нас будет нужный вид и когда вычисления закончатся у нас будет диагональная матрицаБ

6. **Докажите, что подгруппа свободной? конечно порожденной абелевой группы свободна? и конечно порождена. Докажите, что любая свободная? конечно порожденная абелева группа изоморфна**

$$\mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_k\mathbb{Z}$$

для некоторых $d1, \ldots, dk$, так что $d_1 | \ldots | d_k$. Единственно ли такое разложеие?

(Решения пока нет)

7. **Верно ли, что подмодуль свободного модуля свободен?** Это конечно же не верно, так как в свободном $\mathbb{Z}/4\mathbb{Z}$-модуле $\mathbb{Z}/4\mathbb{Z}$ есть подмодуль $2\mathbb{Z}/4\mathbb{Z}$ и он конечно же не свободен, так как его порядок 2, что не является степенью порядка кольца $\mathbb{Z}/4\mathbb{Z}$, то есть не степень 4.