МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

ДОПОЛНИТЕЛЬНЫЕ ГЛАВЫ АЛГЕБРЫ. ЧАСТЬ 2

КАНУННИКОВ
АНДРЕЙ ЛЕОНИДОВИЧ

МЕХМАТ МГУ

Содержание

Лекция 2

Пусть $f(x) = x^5 - 4x + 2 = 0$. Существует ли такая цепочка расширений полей:

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots K_m \ni \underbrace{x_1, \dots, x_5}_{\text{корни } f},$$

где каждое поле получается из предыдущего присоединением некоторого радикала:

$$K_i = K_{i-1}(r_i), \quad r_i^n \in K_{i-1}.$$

То есть мы множество $K_{i-1} \bigcup \{r_i\}$ замыкаем относительно четырех арифметических действий: «+», «−», «×», «/». Теорема Галуа гласит, что такой «башни полей» не существует.

Примеры числовых полей: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Поле вычетов: $\mathbb{Z}_p$, p — простое.

Если есть поле K, то можно построить кольцо многочленов $K[x]$ и поле частных этого кольца — поле формальных дробей $K(x)$ ($K[x] \subseteq K(x)$).

Также известно, что если поле K бесконечно, то многочлены можно отождествлять с функциями, а дроби — с рациональными функциями.

В случае конечных полей это не так: $Z_2[x]$, $x^2 \neq x$.

Предположим, что есть расширение поля $K \subseteq L \ni \alpha$. Тогда можно построить кольцо и поле, порожденные этим элементом:

$$K[\alpha] = \{f(\alpha) \mid f \in K[x]\},$$
$$K(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} \mid f, g \in K[\alpha], g(\alpha) \neq 0\}.$$

Легко понять, что $K[\alpha]$ — это наименьшее подкольцо в L, которое содержит K и α, а $K(\alpha)$ — это наименьшее подполе в L, содержащее K и α. Иногда они совпадают.

Пример 1. Пусть в качестве поля K — поле $\mathbb{Q}$, $\alpha = \sqrt{2}$. Так как

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2},$$

то $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$.

Определение 1. Пусть $K \subseteq L \ni \alpha$. Элемент α называется *алгебраическим* над K $\iff \exists\ f \in K[x]$, $f \neq 0$: $f(\alpha) = 0$.

Если K — это $\mathbb{Q}$, а L — поле $\mathbb{C}$, то множество таких α называется полем алгебраических чисел:

$$\mathbb{A} = \{\alpha \in \mathbb{C} \mid \alpha \text{ — алгебр. над } \mathbb{Q}\}.$$

Можно ли в общем случае избавиться от иррациональности в знаменателе?

Пример 2. Пусть $\alpha = \sqrt[3]{2}$ ($u(x) \in \mathbb{Q}[x]$).

$$\frac{1}{\sqrt[3]{4} + \sqrt[3]{2} + 3} = u(\alpha) \iff u(x)(x^2 + x + 3) - 1 \vdots x^3 - 2 = \mu_\alpha(x) \tag{1}$$

Определение 2. $\mu_\alpha(x)$ — многочлен над K с корнем α, старшим коэффициентом 1 и минимальной степени.

Теорема 1. *1)* $\mu_\alpha(x)$ *неприводим над полем* K.

2) Если $\exists\ f(x) \in K[x]$, $f(\alpha) = 0$, *то* $\mu_\alpha(x) \mid f$.

3) Пусть $f(x) \in K[x]$, $f(\alpha) = 0$, f *неприводим. Следовательно,* $f \sim \mu_\alpha(x)$, *то есть* f *ассоциирован с* $\mu_\alpha(x)$ *(т.е. в точности* $\mu_\alpha(x)$ *с точностью до множителя).*

Доказательство.

1) Если бы $\mu_\alpha(x)$ был приводим, то мы разложили бы его на множители меньшей степени: $f(x)g(x)$, и α был бы корнем одного из множителей — противоречие с минимальностью

2) Разделим с остатком:

$$f(x) = q(x)\mu_\alpha(x) + r(x),$$
$$\deg r(x) < \deg \mu_\alpha(x) \text{ или } r(x) = 0.$$

Однако неравенство со степенями не выполняется, если подставить α (иначе было бы противоречие с минимальностью). Следовательно, $r(x) = 0$.

□

Вернемся к (**??**). Получим, что

$$u(x)(x^2 + x + 3) + v(x)(x^3 - 2) = 1$$

Это «соотношение Безу» или представление наибольшего общего делителя целых чисел в виде их линейной комбинации с целыми коэффициентами.

Одно из приложений этой операции — это избавление от иррациональности в знаменателе. Многочлены $u(x)$, $v(x)$ можно найти методом неопределенных коэффициентов, а стандартный способ для любы евклидовых колец — это обратный ход алгоритма Евклида.

$$(2x^2 + x - 7)(x^2 + x + 3) - (2x + 3)(x^3 - 2) = -15$$

Следовательно,

$$\frac{2\sqrt[3]{4} + \sqrt[3]{2} - 7}{15}.$$

Неалгебраические элементы называются *трансцендентными.*

Если α трансцендентно, то он не удовлетворяет никакому алгебраическому соотношению, поэтому его можно отождествлять с формальной переменной. «Формальной» — значит имеет место изоморфизм $K(\alpha) \cong K(x)$, где x — формальное переменная, α — трансцендентный над K элемент:

$$x \longmapsto \alpha,$$
$$f(x) \longmapsto f(\alpha),$$
$$f(\alpha) = 0 \Longleftrightarrow f(x) = 0.$$

Например, $\mathbb{Q}(x) \cong \mathbb{Q}(\pi)$.

Пример 3. 1882 — $\pi \notin \mathbb{A}$ (Линдеман),
1873 — $e \notin \mathbb{A}$ (Эрмит),
$\pi + e \notin \mathbb{Q}$ — не доказано,
1844 — $\sum\limits_{n=0}^{\infty} 2^{-n!} \notin \mathbb{A}$ (Лиувилль).

Доказать существование трансцендентных чисел можно из соображений мощности. Алгебраические числа — это корни многочленов над $\mathbb{Q}$, многочленов над $\mathbb{Q}$ счетное множество, у каждого многочлена конечное число корней. Следовательно, всего алгебраических чисел счетное множество, а $\mathbb{C}$ — континуально, поэтому трансцендентные числа существуют.

Теорема 2. *Следующие условия эквивалентны:*

1) α *алгебраично над* K*,*

2) $K(\alpha) = K[\alpha]$*,*

3) $[K(\alpha) : K] = \dim_K K(\alpha) < \infty$*.*

**) При выполнении этих условий* $[K(\alpha) : K] = \deg \mu_\alpha = \deg \alpha$*.*

Доказательство.

$\boxed{1 \Rightarrow 2}$ $\frac{1}{f(\alpha)} \in K(\alpha)$, $f \in K[x]$, $f(\alpha) \neq 0 \Longrightarrow (f, \mu_\alpha) = 1 = uf + v\mu_\alpha$. Следовательно, $\frac{1}{f(\alpha)} = u(\alpha)$.

$\boxed{2 \Rightarrow 1}$ По условию $\frac{1}{\alpha} \in K[\alpha]$, $(\alpha \neq 0)$. $1/\alpha = f(\alpha) \Longrightarrow$

$$\alpha f(\alpha) - 1 = 0,$$
$$xf(x) - 1|_{x=\alpha} = 0.$$

Следовательно, α — алгебраическое.

$\boxed{1 \Rightarrow 3, *}$ Пусть $\mu_\alpha(x) = x^n + \ldots$.

Тогда $K[\alpha] = \{b_0 + b_1\alpha + b_2\alpha^2 + \ldots + b_{n-1}\alpha^{n-1} \mid b_0, \ldots, b_{n-1} \in K\}$ — с базисом $1, \alpha, \ldots, \alpha^{n-1}$.

$\boxed{3 \Rightarrow 1}$ Существует $k \in \mathbb{N}$: $1, \alpha, \ldots, \alpha^k$ линейно зависимы $\Longrightarrow$ α алгебраично над K.

□

Пример 4.

1) $\sqrt[n]{2} \in \mathbb{A}$. $\deg \sqrt[n]{2} \underbrace{=}_{?} n \Longleftrightarrow \mu_{\sqrt[n]{2}} = x^n - 2 \Longleftrightarrow x^n - 2$ неприводим над $\mathbb{Q}$.

Признак Эйзенштейна. Многочлен $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ неприводим над $\mathbb{Z}(\mathbb{Q})$, если $\exists\, p$ — простое: $p \nmid a_n$, $p \mid a_{n-1}, \ldots, a_1, a_0$, $p^2 \nmid a_0$.

2) $\alpha = \sqrt{3} + \sqrt{2} \Longrightarrow \alpha^2 = 5 + 2\sqrt{6} \Longrightarrow (\alpha^2 - 5)^2 = 24$, т.е. $x^4 - 10x^2 + 1|_{x=\alpha} = 0$. Верно ли, что $\mu_\alpha(x) = x^4 - 10x^2 + 1$? Все корни этого многочлена: $\pm\sqrt{3} \pm \sqrt{2}$.

   Если мы можем разложить $x^4 - 10x^2 + 1$ в произведение двух квадратных трехчленов. Но как бы мы не разбили четыре числа из $\pm\sqrt{3} \pm \sqrt{2}$ на две пары, то их произведение будет иррациональным, т.е. получатся многочлены с иррациональными коэффициентами.

   Поэтому $\deg \alpha = 4$.

3) $\cos \frac{2\pi}{5} = c$.

$$1 + 2c + 2(2c^2 - 1) = 0,$$
$$4c^2 + 2c - 1 = 0, \quad 0 < c = \frac{-1 + \sqrt{5}}{4}.$$

4) $\cos \frac{2\pi}{9} = c$.

$$4c^3 - 3c = -\frac{1}{2},$$
$$8x^3 - 6x + 1 = 8\mu_{\cos \frac{2\pi}{9}}(x) \text{ — неприводим над } \mathbb{Q}.$$

Упражнение 1. $\deg \cos \frac{2\pi}{n} = ?$

Упражнение 2. при каких $a \in \mathbb{Q}$ $\deg \sqrt[n]{a} = n$, то есть $x^n - a$ неприводим над $\mathbb{Q}$.

- $a > 0$ или n нечетно
- $a < 0$, $n = 4$, $x^4 + |a|$
- $a < 0$, $n = 2^s$,
- общий случай

Определение 3. Расширение L/K называется конечным $\Longleftrightarrow [L : K] < \infty$.

Определение 4. Расширение L/K называется алгебраическим $\Longleftrightarrow \forall \alpha \in L$ α — алгебраическое над K.

Факт. Конечное $\Longrightarrow$ алгебраическое.

А именно, возьмем любое $\alpha \in L$ и его степени: $1, \alpha, \ldots, \alpha^n$, где $n = [L : K]$. Тогда они линейно зависимы, поэтому α алгебраично.

Обратное, вообще говоря, неверно (например, $\mathbb{A}$ над $\mathbb{Q}$).

Лемма 1 (о башне)**.** *Пусть есть башня расширений*

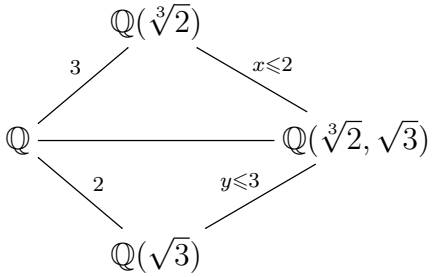
$$K \overset{m}{\text{—}} K \overset{n}{\text{—}} P,$$

где $[L : K] = m$, $[P : L] = n$. *Следовательно,* $[P : K] = mn$.

Доказательство. Если $e_1, \dots, e_m$ — базис в L/K, $f_1, \dots, f_n$ — базис в P/L. Следовательно, $(e_i, f_j)_{i,j}$ — базис в P/K. Во–первых, $P \ni p = \sum a_j f_j$, $a_j = \sum b_{ij} e_i$). Теперь надо доказать линейную независимость. Если $\sum a_j f_j = 0$, то все $a_j = 0$, так как f_j — базис. В свою очередь, и $\sum b_{ij} e_i = 0$, а так как e_i образуют базис, то все $b_{ij} = 0$. □

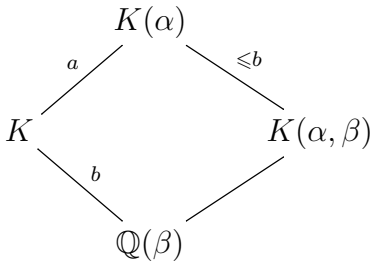
Пример 5. Покажем, что $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}] = 6$.

Видно, что



По лемме о башне $3x = 2y$, $x \leqslant 2$, $y \leqslant 3$. Следовательно, $x = 2$, $y = 3$.

Обобщение:



Теорема 3. *Пусть L/K — любое расширение. Множество всех элементов в L, алгебраичных над K является подполем в L. В частности, $\mathbb{A}$ — поле.*

Доказательство. Пусть $\alpha, \beta \in L$ — алгебраичны над K. Рассмотрим такую башню:

$$K \underbrace{\overset{<\infty(1)}{\longrightarrow} K(\alpha) \overset{<\infty(2)}{\longrightarrow} K(\alpha, \beta)}_{<\infty(3)},$$

Так как при присоединении алгебраического элемента, степень расширения конечна (расширения «1», «2»), и по лемме о башне расширение «3» конечно, то расширение «3» алгебраично (всякое конечное расширение алгебраично). Что, в свою очередь, означает, что каждый элемент алгебраичен. Теорема доказана. □

В расширении $\mathbb{C}/\mathbb{R}$ числа $a \pm bi$ называются сопряженными (у числа i сопряженные $\pm i$). Аналогично в $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ числа $a \pm b\sqrt{2}$ — сопряженные (у числа $\sqrt{2}$ сопряженные $\pm\sqrt{2}$).

Рассмотрим расширение $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Здесь у числа $\sqrt[3]{2}$ сопряженные $\varepsilon^k \sqrt[3]{2}$, где $\sqrt[3]{1} = \{1, \varepsilon, \varepsilon^2\}$ (корни $x^3 - 2$).

Определение 5. Пусть $\mu_\alpha^K(x) = (x - \alpha_1) \dots (x - \alpha_n) \in K[\alpha]$, $\alpha_1, \dots, \alpha_n \in L$.

Все корни $\alpha_1, \dots, \alpha_n$ называются *сопряженными с α над K*.

Например, у $\cos\frac{2\pi}{9}$ сопряженные: $\cos\frac{2\pi}{9}$, $\cos\frac{4\pi}{9}$, $\cos\frac{8\pi}{9}$.

Упражнение 3. Найти сопряженные над $\mathbb{Q}$ для чисел:

$$\sqrt[3]{1+\sqrt{2}}+\sqrt[3]{1-\sqrt{2}},$$
$$\sqrt[3]{7+5\sqrt{2}}+\sqrt[3]{7-5\sqrt{2}}.$$

Понятие сопряженности зависит от того, над каким полем мы рассматриваем сопряженные. Например, у числа i над полем $\mathbb{R}$ сопряженные — $\pm i$, а над $\mathbb{C}$ — i ($i \in \mathbb{C}$, его минимальный многочлен $x-i$). И вообще говоря, минимальный многочлен при увеличении поля не увеличивается.

Рассмотрим многочлен x^4-2. Он неприводим над $\mathbb{Q}$ по признаку Эйзенштейна. У него 4 корня: $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-i\sqrt[4]{2}$. Они образуют его класс сопряженности над $\mathbb{Q}$.

Если присоединить к полю $\mathbb{Q}$ $\sqrt{2}$ — $\mathbb{Q}(\sqrt{2})$, то в нем разложение на неприводимые исходного многочлена выглядит так: $(x^2-\sqrt{2})(x^2+\sqrt{2})$. Тогда классы эквивалентности будут такими: $(\sqrt[4]{2}, -\sqrt[4]{2})$, $(i\sqrt[4]{2}, -i\sqrt[4]{2})$.

Теперь рассмотрим $\mathbb{Q}(\sqrt[4]{2})$. Здесь $(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x^2+\sqrt{2})$, классы эквивалентности будут такими: $(\sqrt[4]{2})$, $(-\sqrt[4]{2})$, $(i\sqrt[4]{2}, -i\sqrt[4]{2})$. Если мы теперь присоединим i, то все четыре корня будут в различных классах сопряженности.

Пусть α, β — алгебраические над K.

$$\alpha_1 = \alpha, \ldots, \alpha_m \text{ — сопряженные с } \alpha,$$
$$\beta = \beta, \ldots, \beta_n \text{ — сопряженные с } \beta.$$

Какие сопряженные у $\alpha+\beta$?

Рассмотрим $\prod\limits_{i=1}^{m}\prod\limits_{j=1}^{n}(x-\alpha_i-\beta_j) \in K[x]$.

Лемма 2. *Рассмотрим многочлен $(x-\alpha_1)\ldots(x-\alpha_n) \in K[x]$. Если есть многочлен $f(y, x_1, \ldots, x_n) \in K[y, x_1, \ldots, x_n]$ — симметричный по $x_1, \ldots, x_n$, то $f(y, \alpha_1, \ldots, \alpha_n) \in K[y]$.*

Доказательство. Доказательство следует из теоремы Виета и основной теоремы о симметрических многочленах □

Применим лемму. Рассмотрим $\prod\limits_{i=1}^{m}\prod\limits_{j=1}^{n}(x-x_i-y_j)$. По x_i этот многочлен симметрический $\Longrightarrow \prod\limits_{i=1}^{m}\prod\limits_{j=1}^{n}(x-\alpha_i-y_j) \in K[x, y_1, \ldots, y_n]$. Теперь так как получившийся многочлен является симметрическим по y_j, применяем лемму второй раз: $\prod\limits_{i=1}^{m}\prod\limits_{j=1}^{n}(x-\alpha_i-\beta_j) \in K[x]$. Таким образом, получили альтернативное доказательство того, что алгебраические числа образуют поле, потому что помимо доказательства алгебраичности $\alpha+\beta$, мы нашли все элементы, среди которых содержатся его сопряженные (потому что, вообще говоря, полученный многочлен может не быть минимальным, но всегда делится на него).

Таким образом, $\alpha * \beta$ **содержатся** среди $\alpha_i * \beta_j$, где $* \in \{+, -, \times, /\}$.

Теорема 4. *Пусть α — алгебраическое над K, $\alpha_1, \dots, \alpha_n$ — все сопряженные с α. Тогда сопряженные с $f(\alpha)$, где $f \in K[x]$, это* ***в точности*** *$f(\alpha_1), \dots, f(\alpha_n)$ (среди $f(\alpha_i)$ могут быть повторы).*

Доказательство. Во–первых, докажем, что числа $f(\alpha_1), \dots, f(\alpha_n)$ действительно являются сопряженными:

Рассмотрим $\mu_{f(\alpha)}$. Он алгебраичен, потому что он лежит в $K(\alpha)$. Вообще говоря, любой элемент поля $K(\alpha)$ имеет вид $f(\alpha)$. Теперь возьмем композицию двух многочленов: $\mu_{f(\alpha)}(f(x)) \in K[x]$.

Так как α — корень этого многочлена, то $\mu_\alpha(x) \mid \mu_{f(\alpha)}(f(x))$. Все корни делителя являются корнями делимого. Но все корни делителя — это в точности все сопряженные с α. Значит, все сопряженные будут корнями $\mu_{f(\alpha)}(f(x))$. Следовательно, все $f(\alpha_i)$ сопряжены с $f(\alpha)$ для любого i.

Теперь докажем, почему других сопряженных нет:

Рассмотрим многочлен: $g = (x - f(\alpha_1)) \dots (x - f(\alpha_n)) \in K[x]$. (так как он симметричен по α_i, а дальше по лемме). Следовательно, $\mu_{f(\alpha)}(x) \mid g$. Теорема доказана. □

Рассмотрим минимальный многочлен

$$\mu_\alpha(x) = (x - \alpha_1) \dots (x - \alpha_n).$$

Верно ли, что $\#\{\alpha_1, \dots, \alpha_n\} = n = \deg \alpha$? То есть могут ли быть у минимального многочлена кратные корни?

Вопрос:

Может ли неприводимый над K многочлен иметь кратные корни в некотором расширении поля K?

Ответ: Пусть $\operatorname{char} K = 0$.

«Кратный корень f» = «общий корень f и f'» = «корень (f, f')». Знаем, что $\deg f' = \deg f - 1$. Так как f неприводим, то

$$(f, f') = \left[\begin{array}{l} 1, \\ f. \end{array} \right.$$

Но из того, что $\deg(f, f') \leqslant \deg f' = \deg f - 1$, получаем: $(f, f') = 1$.

Корни $\frac{f}{(f,f')}$ те же, что у f, но все простые (кратности 1).

Итак, если $\operatorname{char} K = 0$, то **ответ — да**.

Лекция 3

Пусть R — ассоциативное кольцо с единицей.

Определение 6. Множество M называется R–модулем, если на нем введены две операции: сложения $+: M \times M \to M$ и умножения на элемент кольца $\cdot : R \times M \to M$ такие, что выполнены аксиомы:

1) $(M, +)$ — абелева группа;

2) $(a + b)m = am + bm$;

3) $a(m_1 + m_2) = am_1 + am_2$;

4) $(ab)m = a(bm)$;

5) $1 \cdot m = m$.

Если R — поле, то мы получаем определение векторного пространства.

Если $S \subseteq R$ — подкольцо, то любой R–модуль является S–модулем.

Пример 6. Любое кольцо R можно рассмотреть как R–модуль.

Пример 7. Если $S \subseteq R$ — подкольцо, то R можно рассматривать как S–модуль.

Пример 8. Если $I \subseteq R$ — левый идеал, то I является R–модулем.

Пример 9. Любая абелева группа является $\mathbb{Z}$–модулем.

Пример 10. Пусть V — векторное пространство над полем K, и пусть $\varphi : V \to V$ — линейный оператор. Тогда V можно наделить структурой $K[x]$–модуля, задав умножение по формуле

$$f(x) \cdot v = f(\varphi)(v).$$

Пример 11. Пусть K — поле. Множество R называется K–алгеброй, если на R заданы три операции: сложения, умножения и умножения на элемент поля K такие, что

1) R с операциями сложения и умножения — кольцо;

2) R с операциями сложения и умножения на число — векторное пространство;

3) $c(xy) = (cx)y$, $c \in K$, $x, y \in R$.

Пусть R — это K–алгебра с единицей, тогда K вкладывается в R как подкольцо $\langle 1 \rangle$. Мы будем рассматривать только ассоциативные алгебры с единицей, если не оговорено противное.

Если M — это R–модуль, а R — это K–алгебра, то M является K–векторным пространством.

Определение 7. Пусть R — кольцо, M и N — два R–модуля. Отображение $f : M \longrightarrow N$ называется R–линейным, если

1) $f(m_1 + m_2) = f(m_1) + f(m_2)$ для любых $m_1, m_2 \in M$;

2) $f(am) = af(m)$ для любых $a \in R$, $m \in M$.

Множество R–линейных отображений из M в N мы будем обозначать $Hom_R(M, N)$. На множестве $Hom_R(M, N)$ можно ввести операцию сложения по формуле

$$(f + g)(m) = f(m) + g(m).$$

Легко видеть, что $Hom_R(M, N)$ с этой операцией является абелевой группой.

Введем операцию умножения на элемент R на множестве $Hom_R(M, N)$ по формуле

$$(a \cdot f)(m) = f(am).$$

Однако в общем случае эта операция не делает R–модулем множество $Hom_R(M, N)$. Дело в том, что

$$((ab) \cdot f)(m) = f(abm), \text{ но } (a \cdot (b \cdot f))(m) = b \cdot f(am) = f(bam).$$

Однако видно, что для коммутативного кольца $Hom_R(M, N)$ является R–модулем.

Следствием из предыдущего является утверждение, что если R — это K–алгебра, то $Hom_R(M, N)$ является K–векторным пространством (так как K коммутативно).

Теорема 5. *Пусть R — ассоциативное кольцо с единицей и пусть M — R–модуль. Тогда имеет место изоморфизм абелевых групп*

$$Hom_R(M, N) \simeq M.$$

Более того, если R — это K–алгебра, то этот изоморфизм является изоморфизмом векторных пространств над K.

Доказательство. Определим отображение $\Phi : Hom_R(M, N) \to M$ по формуле

$$\Phi(f) = f(1).$$

Легко видеть, что Φ — гомоморфизм абелевых групп, так как

$$\Phi(f_1 + f_2) = (f_1 + f_2)(1) = f_1(1) + f_2(1) = \Phi(f_1) + \Phi(f_2).$$

Также, поскольку для $c \in K$ выполнено $\Phi(cf) = cf(1) = c\Phi(f)$.

Осталось доказать биективность Φ. Докажем сперва инъективность. Пусть $\Phi(f) = \Phi(g)$. Тогда $f(1) = g(1)$. Но тогда

$$f(r) = f(r \cdot 1) = rf(1) = rg(1) = g(r \cdot 1) = g(r)$$

для всех $r \in R$. То есть $f = g$.

Теперь докажем сюръективность Φ. Возьмем $m \in M$ и определим $f_m : R \to M$ по формуле $f_m(r) = rm$. Отображение f_m задает R–линейное отображение из R в M такое, что $f_m(1) = m$. □

Определение 8. Пусть M и N — R–модули. Прямой суммой $M \oplus N$ этих модулей называется прямая сумма абелевых групп M и N с операцией умножения на элемент r, определенной по правилу

$$r \cdot (m, n) = (rm, rn).$$

Можно проверить, что получится R–модуль.

Аналогично определяется прямая сумма большего количества слагаемых. Пусть $M = M_1 \oplus \ldots \oplus M_k$. Естественные проекции $\pi_i : M \to M_i$, $\pi_i(m_1, \ldots, m_k) = m_i$ являются R–линейными отображениями.

Теорема 6. *Пусть M и N — R–модули. И пусть модуль M раскладывается в прямую сумму модулей $M_1 \oplus \ldots \oplus M_k$. Тогда существует изоморфизм абелевых групп*

$$Hom_R(M, N) \simeq Hom_R(M_1, N) \oplus \ldots \oplus Hom_R(M_k, N).$$

Более того, в случае, когда R является K–алгеброй, это изоморфизм векторных пространств над K.

Доказательство. Рассмотрим следующее отображение

$$\Psi : Hom_R(M_1, N) \oplus \ldots \oplus Hom_R(M_k, N) \longrightarrow Hom_R(M_1 \oplus \ldots \oplus M_k, N),$$

$$\Psi(f_1, \ldots, f_k)(m_1, \ldots, m_k) = f_1(m_1) + \ldots + f_k(m_k).$$

Легко видеть, что Ψ — гомоморфизм абелевых групп и, если R является K–алгеброй, это Ψ — K–линейное отображение.

Если $\Psi(f_1, \ldots, f_k) = \Psi(g_1, \ldots, g_k)$, применим его к $(0, \ldots, 0, m_i, 0, \ldots, 0)$. Получим $f_i(m_i) = g_i(m_i)$. Следовательно, Ψ — инъекция.

Пусть теперь задано R–линейное отображение

$$f : \bigoplus_{i=1}^{k} M_i \longrightarrow N.$$

Определим $f_i : M_i \to N_i$ по формуле

$$f_i(m_i) = f(0, \ldots, 0, m_i, 0, \ldots, 0).$$

Тогда

$$\Psi(f_1, \ldots, f_k)(m_1, \ldots, m_k) = \sum f_i(m_i) = \sum f(0, \ldots, 0, m_i, 0, \ldots, 0) = f(\sum(0, \ldots, 0, m_i, 0, \ldots, 0))f($$

Отсюда следует, что Ψ сюръективно. □

Определение 9. Подмножество N модуля M над кольцом R называется подмодулем, если оно является модулем с теми же операциями.

Заметим, что если R — это K–алгебра, то подмодуль в R–модуле является его подпространством над K.

Определение 10. Модуль M называется простым, если он не имеет подмодулей, кроме $\{0\}$ и M.

Если задано R–линейное отображение R–модулей $\varphi : M \to N$, то $\operatorname{Ker}\varphi$ и $Im\varphi$ являются подмодулями. Сюръективность φ равносильна $Im\varphi = N$. Стандартная лемма для абелевых групп утверждает, что инъективность φ равносильна $\operatorname{Ker}\varphi = \{0\}$.

Лемма 3 (Шур)**.** *Пусть M и N — два простых R–модуля. Тогда любое R–линейное отображение $\varphi : M \to N$ — это либо изоморфизм, либо нулевое отображение. Если же $M = N$ и R является $\mathbb{C}$–алгеброй, то $\varphi = \lambda \operatorname{id}$ для некоторого $\lambda \in \mathbb{C}$.*

Доказательство. Ядро отображения φ — это подмодуль в M. Значит, либо $\operatorname{Ker}\varphi = M$ и тогда φ — нулевое отображение, либо $\operatorname{Ker}\varphi = \{0\}$, что означает, что φ — инъекция. Образ φ — подмодуль в N. Так как N простой, либо $Im\varphi = \{0\}$ и тогда φ — нулевое отображение, либо $Im\varphi = N$, то есть φ — сюръекция. Итак, мы доказали, что если $\varphi \neq 0$, то это биекция, и следовательно, изоморфизм модулей.

Пусть теперь R является $\mathbb{C}$–алгеброй. Тогда $M = N$ — это комплексное векторное пространство и φ — линейный оператор на нем. Тогда у φ существует собственное значение $\lambda \in \mathbb{C}$. Оператор $\varphi - \lambda \operatorname{id}$ вырожденный, следовательно это не изморфизм векторных пространств, а следовательно, не изморфизм модулей.

С другой стороны,

$$(\varphi - \lambda \operatorname{id})(rm) = \varphi(rm) - rm = r\varphi(m) - rm = r(\varphi - \lambda \operatorname{id})(m).$$

Это показывает, что $\varphi - \lambda \operatorname{id}$ — это R–линейное отображение. Что означает, что $\varphi - \lambda \operatorname{id} = 0$, то есть $\varphi = \lambda \operatorname{id}$. □

Пример 12. Пусть K — поле, G — группа. Рассмотрим групповую алгебру $R = KG$ группы G над полем K. Это K–векторное пространство с базисом $\{e_g \mid g \in G\}$, в котором определено умножение базисных элементов по формуле $e_g \cdot e_h = e_{gh}$. Произведение не базисных элементов определяется по дистрибутивности, то есть

$$\Big(\sum_g \lambda_g e_g\Big) \cdot \Big(\sum_h \mu_h e_h\Big) = \sum_{g,h} \lambda_g m u_h e_{gh}.$$

Легко видеть, что KG — это ассоциативная K–алгебра с единицей e_e.

Любое линейное представление ρ группы G в пространстве V над полем K задает структуру KG–модуля на V. В самом деле, можно определить

$$\Big(\sum_g \lambda_g e_g\Big) \cdot v = \sum_g \lambda_g \rho(g)(v).$$

Напротив, если задан KG–модуль M, то M является K–векторным пространством и можно определить соответствующее линейное представление $\rho : G \to GL(M_K)$ по формуле $\rho(g)(m) = e_g m$.

Рутинные проверки убеждают нас в том, что данные отображения корректны и взаимно обратны. Таким образом, у нас есть соответствие между K–представлениями G и KG–модулями.

Более того, инвариантные подпространства в V соответствуют подмодулям в KG–модуле V. Таким образом, неприводимые представления соответствуют простым модулям.

Прямая сумма представлений соответствует прямой сумме модулей.

Теорема 7 (Машке)**.** *Пусть G — конечная группа и K — поле, такое что* $\operatorname{char} K \nmid |G|$*. Тогда любой KG–модуль, являющийся конечномерным векторным пространством, есть прямая сумма простых.*

Применим эту теорему к KG–модулю KG. Получим разложение

$$KG = (V_1^1 \oplus \ldots \oplus V_{n_1}^1) \oplus \ldots \oplus (V_1^r \oplus \ldots \oplus V_{n_r}^r),$$

где $V_a^i \simeq V_b^j \iff i = j$.

Теорема 8. *1) В условиях теоремы Машке любой KG–модуль изоморфен некоторому слагаемому V_a^i.*

2) Пусть $K = \mathbb{C}$ и V — простой KG–модуль. Тогда в любом разложении $\mathbb{C}G$ в прямую сумму простых модулей модули, изоморфные V встречаются $\dim_{\mathbb{C}} V$ *раз.*

Доказательство. 1) Рассмотрим простой KG–модуль V. По доказанной ранее теореме имеем изоморфизм некоторых полей над K:

$$V \simeq Hom_{KG}(KG, V).$$

С другой стороны, по второй доказанной теореме,

$$Hom_{KG}(KG, V) \simeq Hom_{KG}(\oplus V_a^i, V) \simeq \oplus Hom_{KG}(V_a^i, V).$$

Таким образом,

$$V \simeq \oplus Hom_{KG}(V_a^i, V).$$

Это значит, что не все слагаемые нулевые. А следовательно, существует V_a^i, изоморфный V (иначе по лемме Шура $Hom_{KG}(V_a^i, V) = \{0\}$.

2)

$$\dim_{\mathbb{C}} V = \sum_{j,b} \dim_{\mathbb{C}} Hom_{KG}(V_b^j, V) = \#\{(j,b) \mid V_b^j \simeq V\} = n_i.$$

Предпоследнее равенство основано на том, что если два простых модуля V и V_b^j не изоморфны, то $Hom_{KG}(V_b^j, V) = 0$, а если изоморфны, то $Hom_{KG}(V_b^j, V) = \{\lambda \operatorname{id}\} \simeq CC$.

□

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in

ЛЕКЦИИ УЧЕНЫХ МГУ