Независимый Московский Университет

Алгебра – II

Второй курс, осенний семестр 1999/2000 г.
Лекции 6,7

Ещё одно доказательство теоремы Гильберта о нулях.

Теорема 1 (Лемма Нётера о нормализации). *Пусть B — ненулевая конечнопорождённая алгебра над полем $\Bbbk$. Существуют такие алгебраически независимые над $\Bbbk$ элементы $a_1, \dots, a_k \in B$, что B является целым расширением кольца $A = \Bbbk[a_1, \dots, a_k]$.*

Доказательство. Воспользуемся индукцией по числу образующих алгебры B. Если число образующих равно нулю (то есть $B = \Bbbk$), то доказывать нечего. Пусть $B = \Bbbk[b_1, \dots, b_n]$ и для $n-1$ образующей результат верен. Мы можем считать, что $\{b_1, \dots, b_k\}$ — максимальное алгебраически независимое множество образующих. Если $k = n$, то доказывать опять нечего. В противном случае существует такой ненулевой многочлен $f \in \Bbbk[x_1, \dots, x_n]$, что $f(b_1, \dots, b_n) = 0$. Пусть

$$f(x_1, \dots, x_n) = \sum_{\lambda \in \mathbb{Z}_+^n} c_\lambda x^\lambda,$$

где $x^\lambda = x_1^{\lambda_1} \dots x_n^{\lambda_n}$.

Для каждого набора неотрицательных чисел вида $\mu = (\mu_1, \mu_2, \dots, \mu_{n-1}, 1)$ рассмотрим $g(x) = f(x_1 + x_n^{\mu_1}, x_2 + x_n^{\mu_2}, \dots, x_{n-1} + x_n^{\mu_{n-1}}, x_n)$ как многочлен от x_n. Мы имеем

$$g(x) = \sum_{\lambda \in \mathbb{Z}_+^n} c_\lambda x_n^{(\lambda, \mu)} + r(x),$$

где $r(x)$ — многочлен, не содержащий мономов вида x_n^k. Если $d = (\deg f) + 1$, то положив $\mu = (d^{n-1}, d^{n-2}, \dots, d, 1)$, мы получим, что все мономы вида $x_n^{(\lambda,\mu)}$, для которых $c_\lambda \neq 0$, имеют разные степени. Пусть m — максимальная из них. Тогда легко видеть, что степень $r(x)$ по переменной x_n меньше m. Таким образом, $g(b_1 - b_n^{d^{n-1}}, \dots, b_{n-1} - b_n^d, b_n) = 0$ представляет собой уравнение целой зависимости для b_n над подкольцом $\Bbbk[b_1 - b_n^{d^{n-1}}, \dots, b_{n-1} - b_n^d]$. Остаётся применить предположение индукции к этому подкольцу. □

Теорема 2. *Пусть $\Bbbk \subseteq \mathbb{L}$ — расширение полей, причём $\mathbb{L}$ — конечнопорождённая $\Bbbk$-алгебра. Тогда $\mathbb{L}$ является алгебраическим расширением поля $\Bbbk$.*

Доказательство. Пусть $\mathbb{L} = \Bbbk[a_1, \dots, a_n]$. По лемме Нетера, мы можем считать, что $a_1, \dots, a_k$ алгебраически независимы над $\Bbbk$, а $\mathbb{L}$ является целым над

$\mathbb{k}[a_1,\ldots,a_k]$. Пусть $k>0$. Напишем уравнение целой зависимости для a_1^{-1} над $\mathbb{k}[a_1,\ldots,a_k]$. Мы имеем

$$a_1^{-d}+\sum_{s=0}^{d-1} f_s(a_1,\ldots,a_k)a_1^{-s}=0.$$

Умножая на a_1^d, получаем

$$\sum_{s=0}^{d-1} f_s(a_1,\ldots,a_k)a_1^{d-s}+1=0,$$

что противоречит алгебраической независимости $a_1,\ldots,a_k$. Полученное противоречие доказывает, что $k=0$, то есть $\mathbb{L}/\mathbb{k}$ — алгебраическое расширение. $\square$

Следствие 2.1 (Теорема Гильберта о нулях). *Пусть $\mathbb{k}$ — алгебраически замкнутое поле, $I\subseteq\mathbb{k}[x_1,\ldots,x_n]$ — неединичный идеал. Тогда множество $V(I)\subseteq\mathbb{k}^n$ нулей идеала I непусто.*

Доказательство. Можем считать I максимальным идеалом. Тогда $\mathbb{L}=\mathbb{k}[x_1,\ldots,x_n]/I$ — поле, являющееся конечнопорождённой $\mathbb{k}$-алгеброй. По доказанной теореме это алгебраическое расширение поля $\mathbb{k}$. Так как поле $\mathbb{k}$ алгебраически замкнуто, то $\mathbb{L}=\mathbb{k}$. Образы $x_1,\ldots,x_n$ при канонической проекции $\mathbb{k}[x_1,\ldots,x_n]\to\mathbb{k}[x_1,\ldots,x_n]/I$ дают координаты точки из $V(I)$. $\square$

Круговые многочлены. Главной целью Галуа при разработке основ теории, названной впоследствии его именем, было исследование разрешимости алгебраических уравнений в радикалах. Не уточняя, что такое разрешимость в радикалах, я ограничусь следующей формулировкой.

Теорема 3. *Пусть $f(x)$ — сепарабельный неприводимый многочлен над полем $\mathbb{k}$. Уравнение $f(x)=0$ разрешимо в радикалах в том и только том случае, если группа Галуа поля разложения многочлена $f(x)$ над $\mathbb{k}$ разрешима.*

А сейчас мы разберем другое приложение теории Галуа.

Определение 1. *Примитивным (первообразным) корнем* степени n из 1 называется комплексное число ζ, имеющее в группе всех корней n-ой степени из 1 порядок n.

Положим $\Phi_n(x)=\prod\limits_{\zeta\text{ – примитивный }\sqrt[n]{1}}(x-\zeta)$. Многочлен $\Phi_n(x)$ называется *n-м круговым многочленом.*

Утверждение 4. $x^n-1=\prod\limits_{d|n}\Phi_d(x)$.

Следствие 4.1. $\Phi_n(x)\in\mathbb{Z}[x]$.

Теорема 5. *Многочлен $\Phi_n(x)$ неприводим.*

Доказательство. Предположим, это не так. Пусть ζ — первообразный корень. Пусть $f(x)$ — неприводимый делитель Φ_n, такой что $f(\zeta) = 0$.

Предположим, нашлось простое p, такое что $(n,p) = 1$ и ζ^p не является корнем f. Пусть $g(x)$ — неприводимый делитель Φ_n, такой что $g(\zeta^p) = 0$. Тогда $\Phi_n(x) = f(x)g(x)R(x)$, а так как ζ — корень $g(x^p)$, то $g(x^p) \vdots f(x)$. Приведем все по модулю p.

$$\overline{g}(x^p) = [\overline{g}(x)]^p \vdots \overline{f}(x)$$

Пусть $\overline{h}(x)$ — какой-нибудь простой делитель $\overline{f}(x)$. Тогда

$$\overline{g}(x) \vdots \overline{f}(x)$$

$$\overline{\Phi}_n(x) \vdots \overline{h}^2(x)$$

$$x^n - 1 \vdots \overline{h}^2(x)$$

$$(x^n - 1)' \vdots \overline{h}(x)$$

Противоречие — по предположению $(p,n) = 1$ и $(x^n - \overline{1})' = \overline{n}x^n$ не имеет общих делителей с $x^n - 1$.

Итак, если $(p,n) = 1$, а ζ — первообразный корень, то ζ^p — тоже первообразный корень — является корнем того же минимального многочлена, что и ζ. Если η — произвольный первообразный корень, то $\eta = \zeta^{p_1 \cdots p_k}$, где все простые p_i не делят n. Применяя предыдущее заключение k раз, получаем, что и η является корнем того же минимального многочлена $f(x)$, что и ζ. Таким образом, $f(x) = \Phi_n(x)$. □

Построения циркулем и линейкой. Перед началом построений на плоскости отмечены только точки с координатами $(0,0)$ и $(1,0)$. Рассмотрим некоторую конечную последовательность построений и рассмотрим поле, порожденное координатами всех построенных точек.

Назовем поле $\mathbb{k}$ *поликвадратичным*, если существует последовательность вложенных расширений $\mathbb{Q} \subset \mathbb{k}_1 \subset \ldots \subset \mathbb{k}_n \subset \mathbb{k}$, каждое из которых квадратично.

Теорема 6. *Поля, получающиеся посредством построений циркулем и линейкой, поликвадратичны.*

Доказательство. Воспользуемся индукцией по числу построений. После каждого построения к полю добавляются координаты всех новых точек пересечения. Возможны два случая:

1) Добавляется точка пересечения двух прямых. Ее координаты получаются решением системы линейных уравнений, поле не меняется.
2) Добавляются точки пересечения двух окружностей или точки пересечения прямой и окружности. Ее координаты получаются решением квадратного уравнения, поэтому поле либо не меняется, либо получается присоединением корней квадратного уравнения.

Поэтому поле, полученное после очередного построения, поликвадратично над предыдущим. Доказательство окончено. □

Следствие 6.1. *Правильный p-угольник (p — простое) можно построить циркулем и линейкой только для $p = 2^n + 1$, $n \in \mathbb{N}$.*

Доказательство. Предположим, что правильный p-угольник можно построить. Добавляя к соответствующему вещественному поликвадратичному расширению $i = \sqrt{-1}$, получаем, как легко убедиться, поле, содержащее поле разложения кругового многочлена $\Phi_p = x^{p-1} + \cdots + 1$. Степень поликвадратичного расширения может быть только степенью двойки, поэтому $p = 2^n + 1$, $n \in \mathbb{N}$.

С другой стороны, пусть $p = 2^n + 1$, $n \in \mathbb{N}$. Поле разложения кругового многочлена $\Phi_p = x^{p-1} + \cdots + 1$ (круговое поле) является расширением Галуа поля $\mathbb{Q}$ с группой Галуа порядка 2^n. Любая такая группа имеет нормальный ряд, все факторы которого изоморфны $\mathbb{Z}_2$. Соответственно, круговое поле можно получить последовательностью квадратичных расширений. Каждое квадратичное расширение получается присоединением комплексного числа, являющегося корнем квадратного уравнения. Поэтому его вещественную и мнимую части можно построить циркулем и линейкой, исходя из отрезков, длины которых являются вещественными и мнимыми частями элементов исходного поля (проверьте это!). Следовательно, вещественная и мнимая части примитивного корня из 1 степени p допускают построение циркулем и линейкой, то есть правильный p-угольник можно построить. □

Линейные представления и модули.

Определение 2. Пусть G — группа. *Линейным представлением* группы G в пространстве V называется такое отображение $\rho : G \to \operatorname{End}_{\Bbbk} V$, что $\rho(e) = \mathrm{id}_V$ и $\rho(gh) = \rho(g)\rho(h)$ для любых $g, h \in G$. Другими словами, линейное представление группы G в пространстве V — это гомоморфизм ее в группу $GL(V)$ обратимых линейных операторов в пространстве V.

Определение 3. Пусть A — ассоциативная алгебра с единицей. *Линейным представлением* алгебры A в пространстве V называется такое отображение $\rho : A \to \operatorname{End}_{\Bbbk} V$, что $\rho(1) = \mathrm{id}_V$, $\rho(xa) = x\rho(a)$, $\rho(a + b) = \rho(a) + \rho(b)$ и $\rho(ab) = \rho(a)\rho(b)$ для любого $x \in \Bbbk$ и для любых $a, b \in A$. Другими словами, линейное представление ассоциативной алгебры с единицей A в пространстве V — это гомоморфизм ее в ассоциативную алгебру с единицей $\operatorname{End}_{\Bbbk} V$ всех линейных операторов в пространстве V (под гомоморфизмом алгебр с единицей мы понимаем гомоморфизм алгебр, переводящий единицу в единицу).

Вместо слов «линейное представление» мы будем обычно говорить просто «представление», другие (не линейные) представления нам не встретятся.

Определение 4. Пусть A — ассоциативная алгебра с единицей над полем $\Bbbk$. *Левым A-модулем* называется векторное пространство V над полем $\Bbbk$, снабженное операцией *левого умножения* на элементы алгебры A, причем требуется выполнение следующих условий:

1) $1v = v$ для любого $v \in V$;
2) отображение $A \times V \to V$, переводящее всякую пару (a, v) в av, билинейно;
3) $(ab)v = a(bv)$ для любых $a, b \in A$, $v \in V$.

Аналогично определяется понятие *правого A-модуля*.

Ясно, что понятия левого A-модуля и представления алгебры A тесно связаны: если задано представление $\rho : A \to \operatorname{End}_{\Bbbk} V$, то V получает естественную структуру левого A-модуля (произведение av определяется как $\rho(a)v$); наоборот, если векторное пространство V является левым A-модулем, то тем самым задается представление алгебры A в пространстве V (по определению полагаем $\rho(a)v = av$).

Основные свойства представлений одни и те же для групп и ассоциативных алгебр; мы разберем их для алгебр. В основном я буду пользоваться языком модулей, отмечая, как переводятся те или другие утверждения на язык представлений.

Далее буква A обозначает ассоциативную алгебру с единицей над полем $\Bbbk$. Всё сказанное о левых A-модулях буквально переносится на правые A-модули.

Все векторные пространства (в том числе алгебры и модули над ними) будут предполагаться конечномерными (если не оговорено противное).

Определение 5. Пусть V — левый A-модуль. *Подмодулем* модуля V называется любое подпространство $U \subseteq V$, замкнутое относительно умножения на все элементы алгебры A. Если U — подмодуль левого A-модуля V, то факторпространство V/U наделяется естественной структурой левого A-модуля (полагаем $a(v + U) = av + U$ для любого $a \in A$ и любого смежного класса $a + U \in V/U$; корректность этого определения следует из замкнутости U относительно умножения на элементы кольца A). Модуль V/U называется *фактормодулем* модуля V по подмодулю U.

На языке представлений подмодуль называется *инвариантным подпространством*, представление в инвариантном подпространстве называется *подпредставлением*, а представление в факторпространстве называется *факторпредставлением* исходного представления.

Определение 6. Пусть V, W — левые A-модули. *Гомоморфизмом* модуля V в модуль W называется любое линейное отображение $F : V \to W$, удовлетворяющее условию $F(av) = aF(v)$ для любых $a \in A$ и $v \in V$. *Изоморфизмом* называется обратимый гомоморфизм. Если существует изоморфизм $F : V \to W$, то модули V и W называются *изоморфными*.

На языке представлений гомоморфизмы модулей называются *морфизмами представлений* или *сплетающими операторами*, а представления в изоморфных модулях тоже называются изоморфными или *эквивалентными*.

Понятия внешней прямой суммы и внутренней прямой суммы автоматически переносятся с векторных пространств на модули (и на представления).

Определение 7. Левый A-модуль V называется *простым*, если он ненулевой и у него нет нетривиальных подмодулей (то есть подмодулей, отличных от 0 и V). Левый A-модуль V называется *полупростым*, если всякий подмодуль $U \subseteq V$ является прямым слагаемым (то есть существует подмодуль $W \subseteq V$ такой, что $V = U \oplus W$).

Представления, отвечающие простым модулям, называются *неприводимыми*, а представления, отвечающие полупростым модулям, называются *вполне приводимыми*.

Ясно, что любой простой модуль является также и полупростым.

Теорема 7. *Если модуль V полупрост, то его можно разложить в прямую сумму прострых подмодулей.*

Доказательство. Воспользуемся индукцией по размерности V.

Если $\dim V = 0$, то есть если модуль V нулевой, то он является прямой суммой пустого семейства подмодулей.

Пусть $\dim V > 0$ и для всех модулей меньшей размерности утверждение теоремы выполнено. Выберем в V минимальный по включению ненулевой подмодуль U. Ясно, что это простой подмодуль. Поскольку модуль V полупрост, мы можем найти подмодуль $W \subseteq V$ такой, что $V = U \oplus W$. Докажем, что модуль W полупрост.

Пусть $U' \subseteq W$ — подмодуль. Поскольку модуль V полупрост, существует подмодуль $W' \subseteq V$ такой, что $V = U' \oplus W'$. Тогда $W'' = W' \cap W$ — подмодуль модуля W, и $W = U' \oplus W''$.

Так как $\dim W < \dim V$, то W разлагается в прямую сумму простых подмодулей. Следовательно, это верно и для V. □

Теорема 8. *Если модуль V можно разложить в сумму (не обязательно прямую) прострых подмодулей, то он полупрост.*

Доказательство. Пусть $V = V_1 + \cdots + V_k$, где V_i — простые подмодули, и пусть $U \subseteq V$ — некоторый подмодуль. Найдем некоторое максимальное по включению множество индексов $I \subseteq \{1, \ldots, k\}$, удовлетворяющее условию $U \cap \sum\limits_{i \in I} V_i = 0$. Положим $W = \sum\limits_{i \in I} V_i$. Докажем, что $V = U \oplus W$.

Пусть V_j — один из простых модулей, входящих в разложение $V = V_1 + \cdots + V_k$. Предположим, что $V_j \nsubseteq (U + W)$. Тогда $j \notin I$ и $V_j \cap (U + W) = 0$ (поскольку модуль V_j прост). Но тогда $U \cap (W + V_j) = 0$, в противоречии с выбором I. Следовательно, все V_j лежат в $U + W$, так что $V = U + W$. Поскольку $U \cap W = 0$, эта сумма прямая. □

Упражнение 1. Пусть $V = V_1 + \dots + V_k$, где V_i — простые подмодули. Доказать, что найдется такое подмножество $I \subseteq \{1, \dots, k\}$, что $V = \bigoplus\limits_{i\in I} V_i$.

Определение 8. Гомоморфизм модуля в себя называется *эндоморфизмом*. Множество всех эндоморфизмов A-модуля V обозначается через $\operatorname{End}_A V$. Эндоморфизмы левого A-модуля V мы будем записывать *справа* от элементов V, то есть мы считаем V *правым* $(\operatorname{End}_A V)$-модулем. Аналогично, эндоморфизмы правого модуля действуют на него слева.

Упражнение 2. Доказать, что $\operatorname{End}_A V$ является подалгеброй алгебры $\operatorname{End}_{\Bbbk} V$ всех линейных операторов в пространстве V.

Теорема 9. *Если U и V — простые модули, то любой ненулевой гомоморфизм $F : U \to V$ является изоморфизмом.*

Доказательство. Ядро и образ гомоморфизма являются подмодулями. Если $F \neq 0$, то $\operatorname{Ker} F = 0$, $\operatorname{Im} F = V$ (так как модули U и V просты). Поэтому гомоморфизм F обратим, то есть является изоморфизмом. □

Следствие 9.1. *Алгебра эндоморфизмов простого A-модуля V является телом.*

Следствие 9.2 (Лемма Шура). *Если поле $\Bbbk$ алгебраически замкнуто, то любой эндоморфизм простого A-модуля V скалярен.*

Доказательство. Пусть $F : V \to V$ — эндоморфизм, λ — его собственное значение. Эндоморфизм $F - \lambda E$ необратим, поэтому он нулевой. □

Пример 1. Пусть поле $\Bbbk$ алгебраически замкнуто, U — простой левый A-модуль и

$$V = \underbrace{U \oplus \dots \oplus U}_{n} \simeq U \otimes \Bbbk^n.$$

Рассмотрим произвольный A-эндоморфизм $F : V \to V$. Применим его к элементу вида

$$v_i(u) = (0, \dots, 0, u, 0, \dots, 0),$$

где u стоит на i-м месте. Получим $v_i(u)F = (uF_{i1}, \dots, uF_{in})$, где, очевидно, $F_{ij} \in \operatorname{End}_A U$. По лемме Шура F_{ij} — умножение на некоторую константу $\lambda_{ij} \in \Bbbk$. Тогда применение эндоморфизма F к строке $(u_1, \dots, u_n)$ — это умножение ее справа на матрицу (λ_{ij}). Таким образом, $\operatorname{End}_A V = M_n(\Bbbk)$.

Теорема 10 (о двойном централизаторе). *Пусть A — некоторая подалгебра алгебры $\operatorname{End}_{\Bbbk} V$, действующая в V слева, причем известно, что левый A-модуль V полупрост. Положим $B = \operatorname{End}_A V$. Тогда $\operatorname{End}_B V = A$.*

Доказательство. Докажем сперва одно вспомогательное утверждение.

Лемма 10.1. *Для любого $v \in V$ и любого $\varphi \in \operatorname{End}_B V$ найдется такой элемент $a \in A$, что $av = \varphi v$.*

Доказательство. Рассмотрим подмодуль $Av \subseteq V$. Так как A-модуль V полупрост, то имеет место разложение в прямую сумму $V = Av \oplus U$ для некоторого A-подмодуля $U \subseteq V$. Проекция $\pi : V \to Av$ вдоль U является эндоморфизмом A-модуля V, то есть $\pi \in B$. Следовательно, $\varphi v = \varphi(v\pi) = (\varphi v)\pi$, то есть $\varphi v \in Av$, что и требовалось доказать. □

Перейдем теперь к доказательству теоремы. Пусть φ — произвольный элемент алгебры $\operatorname{End}_B V$. Докажем, что $\varphi \in A$.

Рассмотрим A-модуль
$$W = \underbrace{V \oplus \cdots \oplus V}_{n},$$
где $n = \dim V$. Так же, как и в примере 1, проверяем, что $\operatorname{End}_A W = M_n(B)$. Ясно, что $\varphi^{(n)} = \varphi \oplus \cdots \oplus \varphi : W \to W$ является эндоморфизмом $M_n(B)$-модуля W. Положим $w = (v_1, \ldots, v_n)$, где векторы $v_1, \ldots, v_n$ составляют базис V как векторного пространства над $\Bbbk$. По лемме 10.1 найдется такой элемент $a \in A$, что $aw = \varphi^{(n)} w$, то есть $av_i = \varphi v_i$ для всех $i = 1, \ldots, n$. Но это означает, что $a = \varphi$. □

Следствие 10.1. *Пусть поле $\Bbbk$ алгебраически замкнуто, A — некоторая подалгебра алгебры $\operatorname{End}_{\Bbbk} V$, действующая в V слева, причем левый A-модуль V прост. Тогда $A = \operatorname{End}_{\Bbbk} V$.*

Доказательство. По лемме Шура $\operatorname{End}_A V = \Bbbk$, откуда, по теореме о двойном централизаторе, получаем $\operatorname{End}_{\Bbbk} V = A$. □