Независимый Московский Университет

Алгебра – II

Второй курс, осенний семестр 1999/2000 г.
Лекция 5

Прежде всего — другое доказательство теоремы 11 из прошлой лекции.

Докажем, что отображения $\varphi_i : \mathbb{F} \to \mathbb{L}$ линейно независимы. Действительно, пусть $\sum_{s=1}^{r} a_s \varphi_{i_s} = 0$ — линейная зависимость с наименьшим числом слагаемых. Отображения φ_i ненулевые, поэтому $r > 1$. Так как вложения φ_i различны, найдется элемент $g \in \mathbb{F}$ такой, что $\varphi_{i_1} \neq \varphi_{i_2}$. Но $\sum_{s=1}^{r} a_s \varphi_{i_s}(g)\varphi_{i_s}(h) = \sum_{s=1}^{r} a_s \varphi_{i_s}(gh) = 0$ для любого $h \in \mathbb{F}$, то есть имеет место линейная зависимость $\sum_{s=1}^{r} a_s \varphi_{i_s}(g)\varphi_{i_s} = 0$, а следовательно, и линейная зависимость $\sum_{s=1}^{r} a_s (\varphi_{i_s}(g) - \varphi_{i_1}(g))\varphi_{i_s} = 0$, число слагаемых в которой меньше r.

Предыдущее рассуждение представляет собой доказательство теоремы Артина о линейной независимости характеров произвольной группы G (то есть мультипликативных гомоморфизмов $G \to \mathbb{L}^*$).

Возвращаясь к нашей теореме, заметим, что в силу доказанной линейной независимости отображений φ_i, образ отображения $\mathbb{L} \otimes_{\mathbb{k}} \mathbb{F} \to \mathbb{L}^n$, продолжающего $\psi : \mathbb{F} \to \mathbb{L}^n$ по $\mathbb{L}$-линейности, совпадает с $\mathbb{L}^n$. Совпадение размерностей гарантирует, что $\mathbb{L} \otimes_{\mathbb{k}} \mathbb{F} \to \mathbb{L}^n$ —изоморфизм.

Утверждение 1. *Пусть R — целозамкнутая область целостности, $\mathbb{k}$ — её поле частных, $\mathbb{F}/\mathbb{k}$ — конечное сепарабельное расширение, A — целое замыкание кольца R в $\mathbb{F}$. Тогда для любого $a \in A$ его характеристический многочлен лежит в $R[x]$. В частности, норма и след a принадлежат R.*

Доказательство. Положим в следствии 10.1 из предыдущей лекции $\mathbb{L} = \bar{\mathbb{k}}$. Ясно, что образ любого элемента $a \in A$ при любом вложении $\mathbb{F} \to \bar{\mathbb{k}}$ является целым над R элементом. Поэтому все коэффициенты характеристического многочлена элемента a являются целыми над R. Поскольку они принадлежат $\mathbb{k}$, то, в силу целозамкнутости R, они принадлежат R. □

Теорема 2. *Пусть R — целозамкнутая область целостности, $\mathbb{k}$ — её поле частных, $\mathbb{F}/\mathbb{k}$ — конечное сепарабельное расширение, A — целое замыкание кольца R в $\mathbb{F}$. Тогда существует такой базис $(e_1, \ldots, e_n)$ поля $\mathbb{F}$ как линейного пространства над $\mathbb{k}$, что $A \subseteq Re_1 + \cdots + Re_n$.*

Доказательство. Пусть $u \in \mathbb{F}$, $f(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0 \in \mathbb{k}[x]$ — минимальный многочлен элемента a. Обозначим через c произведение знаменателей коэффициентов a_i. Тогда, очевидно, элемент cu имеет минимальный многочлен $c^k f(x/c) = x^k + ca_{k-1}x^{k-1} + \cdots + c^k a_0 \in R[x]$, то есть $cu \in A$.

Отсюда следует, что мы можем выбрать базис $(u_1, \ldots, u_n)$ поля $\mathbb{F}$ как линейного пространства над $\mathbb{k}$, состоящий из элементов кольца A. Обозначим через $(e_1, \ldots, e_n)$ двойственный базис относительно билинейной формы $(a, b) = \mathrm{tr}(ab)$

(невырожденной по следствию 11.1 из прошлой лекции). Пусть $a \in A$ и пусть $a = \sum_i a_i e_i$ — его разложение по базису $(e_1, \ldots, e_n)$. Тогда $au_i \in A$ и, следовательно, $\mathrm{tr}(au_i) \in R$ для любого $i = 1, \ldots, n$. Но

$$tr(au_i) = \sum_j \mathrm{tr}(a_j e_j u_i) = \sum_j a_j \,\mathrm{tr}(e_j u_i) = a_i,$$

то есть $a_i \in R$ и $a \in Re_1 + \cdots + Re_n$, что и требовалось получить. □

Следствие 2.1. *В условиях теоремы 2 если кольцо R нётерово, то A — конечное расширение кольца R.*

Следствие 2.2. *В условиях теоремы 2 если R — кольцо главных идеалов, то A является свободным R-модулем, и любой его базис является базисом $\mathbb{F}$ над $\Bbbk$.*

Определение 1. Комплексное число, целое над $\mathbb{Z}$, называется *целым алгебраическим числом.*

Пример 1. Пусть $\mathbb{F}/\mathbb{Q}$ — конечное расширение степени n, A — целое замыкание $\mathbb{Z}$ в $\mathbb{F}$. Рассмотрим всевозможные вложения $\varphi_1, \ldots, \varphi_n$ поля $\mathbb{F}$ в поле $\mathbb{C}$. Пусть $X \subseteq A$ — такое подмножество, что множества $\varphi_1(X), \ldots, \varphi_n(X)$ ограничены (в смысле обычной метрики на поле $\mathbb{C}$). Тогда множество X конечно.

Действительно, пусть $(e_1, \ldots, e_n)$ — базис свободного $\mathbb{Z}$-модуля A. Тогда это также базис $\mathbb{F}$ как векторного пространства над $\Bbbk$. Обозначим через ψ отображение $\mathbb{F} \to \mathbb{C}^n$, переводящее любой элемент $a \in \mathbb{F}$ в $(\varphi_1(a), \ldots, \varphi_n(a))$. По теореме 11 из прошлой лекции элементы $\psi(e_1), \ldots, \psi(e_n)$ образуют базис пространства $\mathbb{C}^n$. Элементы кольца A при отображении ψ переходят в целочисленную решётку, натянутую на этот базис, а множество X — в ограниченное подмножество этой решётки, то есть в некоторое конечное её подмножество. Так как ψ — вложение, то отсюда следует, что X — конечное множество.

Соответствие Галуа.

Определение 2. Расширение $\mathbb{F}/\Bbbk$ называется *нормальным*, если любой неприводимый многочлен из $\Bbbk[x]$, имеющий корень в $\mathbb{F}$, разлагается в $\mathbb{F}[x]$ на линейные множители.

Утверждение 3. *Если $\mathbb{F}/\Bbbk$ — нормальное расширение и $\mathbb{L}$ — некоторое промежуточное поле (то есть $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{F}$), то расширение $\mathbb{F}/\mathbb{L}$ тоже нормально.*

Доказательство. Пусть $f(x) \in \mathbb{L}[x]$ — неприводимый многочлен и $a \in \mathbb{F}$ — его корень. Ясно, что $f(x)$ — минимальный многочлен элемента a над полем $\mathbb{L}$ (почему?). Пусть $g(x) \in \Bbbk[x]$ — минимальный многочлен элемента a над полем $\Bbbk$. Многочлен $g(x)$ неприводим в $\Bbbk[x]$, поэтому он разлагается в $\mathbb{F}[x]$ на линейные множители. С другой стороны, в $\mathbb{L}[x]$ многочлен $g(x)$ делится на $f(x)$ (почему?). Следовательно, и многочлен $f(x)$ разлагается в $\mathbb{F}[x]$ на линейные множители. □

Утверждение 4. *Поле разложения любого многочлена из* $\Bbbk[x]$ *нормально над* $\Bbbk$*.*

Доказательство. Пусть $f(x) \in \Bbbk[x]$ — произвольный многочлен и $\mathbb{F}$ — его поле разложения. Обозначим через $x_1, \ldots, x_n$ все различные корни многочлена $f(x)$.

Пусть $g(x) \in \Bbbk[x]$ — минимальный многочлен некоторого элемента $a \in \mathbb{F}$. Предположим, что он не разлагается на линейные множители в $\mathbb{F}[x]$. Обозначим через $\mathbb{L}$ поле разложения этого многочлена (как многочлена над $\mathbb{F}$). Пусть $b \in \mathbb{L}$ — какой-нибудь корень многочлена $g(x)$, не лежащий в $\mathbb{F}$. По утверждению о продолжении изоморфизма, существует изоморфизм $\varphi : \Bbbk(a) \to \Bbbk(b)$, тождественный на $\Bbbk$.

Пусть $h(x)$ — минимальный многочлен элемента x_1 над $\Bbbk(a)$. Очевидно, что этот многочлен делит $f(x)$. Обозначим через $\tilde{\varphi}$ отображение из кольца многочленов $\Bbbk(a)[x]$ в кольцо многочленов $\Bbbk(b)[x]$, состоящее в замене каждого коэффициента многочлена на его образ при изоморфизме φ. Ясно, что $\tilde{\varphi}$ — изоморфизм колец. Поскольку коэффициенты многочлена $f(x)$ принадлежат полю $\Bbbk$, то $\tilde{\varphi}(f(x)) = f(x)$, поэтому $\tilde{\varphi}(h(x))$ делит $f(x)$. Следовательно, найдется такое $j_1 \in \{1, \ldots, n\}$, что x_{j_1} — корень многочлена $\tilde{\varphi}(h(x))$. По утверждению о продолжении изоморфизма, можно продолжить φ до изоморфизма $\Bbbk(a, x_1) \to \Bbbk(b, x_{j_1})$, переводящего x_1 в x_{j_1}.

Повторив эти рассуждения n раз, мы получим изоморфизм

$$\Bbbk(a, x_1, \ldots, x_n) \to \Bbbk(b, x_{j_1}, \ldots, x_{j_n}).$$

Однако $\Bbbk(a, x_1, \ldots, x_n) = \mathbb{F}$ и $\Bbbk(b, x_{j_1}, \ldots, x_{j_n}) = \mathbb{F}(b)$ (поскольку $(j_1, \ldots, j_n)$ — перестановка последовательности $(1, \ldots, n)$). Отсюда $[\mathbb{F}(b) : \Bbbk] = [\mathbb{F} : \Bbbk]$ и, следовательно, $b \in \mathbb{F}$ в противоречии с нашим предположением. □

Определение 3. Алгебраическое расширение $\mathbb{F}/kk$ называется *расширением Галуа*, если оно нормально и сепарабельно. Группа всех автоморфизмов поля $\mathbb{F}$, тождественных на $\Bbbk$, называется *группой Галуа* расширения $\mathbb{F}/kk$ и обозначается $\mathrm{Gal}(\mathbb{F}/\Bbbk)$.

Для любой группы автоморфизмов H поля $\mathbb{F}$ мы будем обозначать через $\mathbb{F}^H$ множество неподвижных точек этой группы, то есть множество всех $a \in \mathbb{F}$ таких, что $h(a) = a$ для любого $h \in H$.

Упражнение 1. Доказать, что $\mathbb{F}^H$ является подполем поля $\mathbb{F}$.

Теорема 5 (Основная теорема теории Галуа). *Пусть* $\mathbb{F}/kk$ *— конечное расширение Галуа и* $G = \mathrm{Gal}(\mathbb{F}/\Bbbk)$*. Тогда между множеством подполей* $\mathbb{L} \subseteq \mathbb{F}$*, содержащих* $\Bbbk$*, и множеством подгрупп* $H \subseteq G$ *существует биективное соответствие, задаваемое формулами* $\mathbb{L} = \mathbb{F}^H$ *и* $H = \mathrm{Gal}(\mathbb{F}/\mathbb{L})$ *(это соответствие называется соответствием Галуа). Кроме того,* $\mathbb{L}/\Bbbk$ *является расширением Галуа тогда и только тогда, когда соответствующая подгруппа* $H = \mathrm{Gal}(\mathbb{F}/\mathbb{L})$ *нормальна в* G*, и в этом случае имеется естественный изоморфизм* $\mathrm{Gal}(\mathbb{L}/\Bbbk) \cong G/H$*.*

Доказательство. Пусть $\mathbb{L}$ — произвольное промежуточное поле. По утверждению 3 и аналогичному утверждению о сепарабельных расширениях, $\mathbb{F}/\mathbb{L}$ является расширением Галуа. Положим $H = \mathrm{Gal}(\mathbb{F}/\mathbb{L})$. По теореме о числе вложений сепарабельного расширения, число элементов группы H равно $[\mathbb{F}:\mathbb{L}]$. В то же время $\mathbb{L} \subseteq \mathbb{F}^H$ и, как мы знаем, число вложений поля $\mathbb{F}$ в себя над $\mathbb{F}^H$ не превосходит $[\mathbb{F}:\mathbb{F}^H] \leqslant [\mathbb{F}:\mathbb{L}]$. Но все элементы группы H являются, по определению, вложениями $\mathbb{F}$ в себя над $\mathbb{F}^H$. Поэтому $[\mathbb{F}:\mathbb{F}^H] = [\mathbb{F}:\mathbb{L}]$ и, следовательно, $\mathbb{F}^H = \mathbb{L}$.

Пусть, напротив, H — произвольная подгруппа группы G. Положим $\mathbb{L} = \mathbb{F}^H$. Мы должны доказать, что $\mathrm{Gal}(\mathbb{F}/\mathbb{L}) = H$.

Пусть $g \in \mathrm{Gal}(\mathbb{F}/\mathbb{L})$. Докажем, что $g \in H$. Для любого $a \in \mathbb{F}$ составим многочлен

$$f_a(x) = \prod_{h\in H}(x - h(a)).$$

Ясно, что коэффициенты этого многочлена инвариантны относительно действия группы H, то есть $f_a(x) \in \mathbb{L}[x]$. Поэтому g переводит множество корней этого многочлена в себя, в частности, $g(a) = h(a)$ для некоторого $h \in H$ (быть может, зависящего от a). По теореме о примитивном элементе поле $\mathbb{F}$ порождено над $\mathbb{L}$ одним элементом; выбрав этот элемент в качестве a, мы получаем $g = h$ (ибо автоморфизм однозначно определяется своим действием на образующую).

Пусть вновь $\mathbb{L}$ — произвольное промежуточное подполе, и пусть H — соответствующая подгруппа группы Галуа. Для каждого $g \in G$ рассмотрим подполе $g(\mathbb{L})$.

Упражнение 2. Доказать, что расширение $\mathbb{L}/\mathbb{k}$ является нормальным тогда и только тогда, когда $g(\mathbb{L}) = \mathbb{L}$ для любого $g \in G$.

Отметим, что подполю $g(\mathbb{L})$ отвечает подгруппа gHg^{-1} (докажите это!). Отсюда (и из упражнения 2) следует, что $\mathbb{L}/\mathbb{k}$ является расширением Галуа тогда и только тогда, когда соответствующая подгруппа $H = \mathrm{Gal}(\mathbb{F}/\mathbb{L})$ нормальна в G.

Пусть это так. Для каждого элемента $g \in G$ (то есть автоморфизма $\mathbb{F}$ над $\mathbb{k}$) обозначим через $\varphi(g)$ его ограничение на подполе $\mathbb{L}$. Ясно, что φ является гомоморфизмом группы G в группу $\mathrm{Gal}(\mathbb{L}/\mathbb{k})$. Этот гомоморфизм сюръективен (ввиду нормальности расширения $\mathbb{F}/\mathbb{k}$ и утверждения о продолжении изоморфизма). Ядром φ является, по доказанному выше, подгруппа H. По теореме о гомоморфизмах групп, $\mathrm{Gal}(\mathbb{L}/\mathbb{k}) \cong G/H$. $\square$