2. Лекция 2

2.1. Алгебраические элементы и конечные расширения.

Предложение 2.1. *Элемент α алгебраичен над F тогда и только тогда, когда расширение $F(\alpha)/F$ конечно.*

Доказательство. Если α алгебраичен над F, то $[F(\alpha):F] = \deg m_{\alpha,F}(x)$. Значит, если α удовлетворяет уравнению степени n, то $[F(\alpha):F] \leq n$.

Обратно, пусть α — элемент расширения степени n. Значит, $n+1$ элемент $1, \alpha, \alpha^2, \dots, \alpha^n$ линейно зависимы над F, то есть α обращает в нуль многочлен степени n. □

Следствие 2.2. *Если расширение K/F конечно, то оно алгебраично.*

Упражнение 2.3. Докажите, что утверждение, буквально обратное к этому, неверно: придумайте алгебраическое расширение бесконечной степени.

Верное обратное утверждение звучит так.

Теорема 2.4. *Расширение K/F конечно тогда и только тогда, когда K порождается над F конечным числом алгебраических элементов $\alpha_1, \dots, \alpha_k$ степеней $n_1, \dots, n_k$. В этом случае $[K:F] \leq n_1 \dots n_k$.*

Доказательство. Часть “тогда” доказана выше. Докажем часть “только тогда”. Пусть K/F конечно, $\alpha_1, \dots, \alpha_n$ — базис K над F. Для каждого из элементов α_i степень расширения $[F(\alpha):F]$ делит число $n = [K:F]$. Поэтому она конечна, следовательно, все элементы α_i алгебраичны. Второе утверждение следует из мультипликативности степени. □

Следствие 2.5. *Пусть α, β алгебраичны над F. Тогда элементы $\alpha+\beta$, $\alpha\beta$, α/β также алгебраичны над F.*

Доказательство. Эти элементы лежат в расширении $F(\alpha, \beta)$. Оно конечно, поэтому все его элементы алгебраичны. □

Задача 2.6. Попробуйте доказать это непосредственно (указание: используйте основную теорему о симметрических многочленах).

Следствие 2.7. *Пусть L/F — расширение полей. Тогда множество элементов из L, алгебраичных над F, образует подполе в L.*

Пример 2.8. Пусть $\overline{\mathbb{Q}}$ — множество всех чисел из $\mathbb{C}$, алгебраических над $\mathbb{Q}$. Во-первых, $[\overline{\mathbb{Q}}:\mathbb{Q}] = \infty$, поскольку $\overline{\mathbb{Q}}$ содержит $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots$. Во-вторых, $\mathbb{Q}$ не совпадает с $\mathbb{C}$, так как эти множества имеют разную мощность (счётную и континуум соответственно). Поэтому существуют *трансцендентные* (т.е. не алгебраические) числа.

Доказать про какое-нибудь число, что оно не алгебраично, обычно бывает весьма сложной задачей. Приведем без доказательства следующую теорему, из которой следуют трансцендентность e и π.

Теорема 2.9 (Эрмит–Линдеман, 1882)**.** *Если α — ненулевое алгебраическое число, то e^α трансцендентно.*

Теорема 2.10. *Пусть L/K и K/F — алгебраические расширения. Тогда расширение L/F тоже алгебраическое.*

Доказательство. Пусть $\alpha \in L$ — произвольный элемент. Значит, α удовлетворяет полиномиальному уравнению

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0, \qquad a_i \in K.$$

Рассмотрим поле $F(\alpha, a_0, \ldots, a_n) \subset L$. Поскольку расширение K/F алгебраично, все элементы $a_0, \ldots, a_n$ также алгебраические. Значит, расширение $F(a_0, \ldots, a_n)$ — конечное алгебраческое расширение F, поэтому оно конечно. Но $F(\alpha, a_0, \ldots, a_n)$ — конечное расширение этого поля, причём его степень не превосходит n. Значит,

$$[F(\alpha, a_0, \ldots, a_n) : F] = [F(\alpha, a_0, \ldots, a_n) : F(a_0, \ldots, a_n)]\cdot[F(a_0, \ldots, a_n) : F]$$

конечное расширение. Поэтому элемент α алгебраичен над F, значит, расширение L тоже алгебраично. $\square$

2.2. **Композит полей.** Пусть $K_1, K_2 \subset K$ — два подполя. *Композит* полей K_1 и K_2 (обозначение: K_1K_2) — это наименьшее подполе в K, содержащее как K_1, так и K_2. Иначе говоря, это пересечение всех подполей в K, содержащих оба этих поля.

Пример 2.11. $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}(\sqrt[6]{2})$; $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Предложение 2.12. *Пусть K_1/F и K_2/F — конечные расширения F, лежащие в некотором поле K. Тогда $[K_1K_2 : F] \leq [K_1 : F] \cdot [K_2 : F]$, причем равенство достигается тогда и только тогда, когда F-базис поля K_1 остается линейно независимым и над другим полем. Если $\alpha_1, \ldots, \alpha_m$ и $\beta_1, \ldots, \beta_n$ — базисы K_1 и K_2 над F, то элементы $\alpha_i\beta_j$ порождают поле K_1K_2 над F.*

Доказательство. $K_1K_2 = F(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n) = K_1(\beta_1, \ldots, \beta_n)$. Значит, $\beta_1, \ldots, \beta_n$ порождают K_1K_2 над K_1. Поэтому $[K_1K_2 : K_1] \leq n = [K_2 : F]$, где равенство достигается в том и только в том случае, когда эти элементы линейно независимы над K_1. Но, в силу мультипликативности степени, $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F]$. $\square$

Следствие 2.13. *Пусть $[K_1 : F] = m$, $[K_2 : F] = n$, причем n и m взаимно просты. Тогда $[K_1K_2 : F] = mn$.*

Доказательство. $[K_1K_2 : F]$ делится и на m, и на n, а значит, делится и на их наименьшее общее кратное. $\square$

2.3. **Поле разложения многочлена.** Мы уже выяснили, что для всякого многочлена $f(x) \in F[x]$ существует такое расширение K/F, в котором у многочлена $f(x)$ есть корень. То есть найдётся такое $\alpha \in K$, что $f(\alpha) = 0$. Это эквивалентно тому, что $f(x)$ делится на двучлен $x - \alpha$ над полем K. Теперь выясним, можно ли найти такое поле, над которым $f(x)$ будет не просто иметь корень, а раскладываться на линейные множители.

Определение 2.14. Поле $K \supset F$ называется *полем разложения* многочлена $f(x)$, если над полем K многочлен $f(x)$ раскладывается на линейные множители, и при этом он не раскладывается на линейные множители ни над каким собственным подполем поля K, содержащим F.

Теорема 2.15. *Для всякого поля F и многочлена $f(x) \in F[x]$ существует расширение K/F, являющееся полем разложения для $f(x)$.*

Доказательство. Сначала докажем, что существует такое поле, в котором $f(x)$ раскладывается на линейные множители. Основная идея здесь проста: надо по очереди присоединить к полю все корни многочлена $f(x)$. Проведём индукцию по $\deg f(x)$. База очевидна: при $\deg f(x) = 1$ многочлен линеен, и доказывать нечего.

Пусть теперь $n > 1$. Если все неприводимые сомножители $f(x)$ линейны, то всё доказано. Если нет, то существует такой неприводимый многочлен $p(x) \mid f(x)$ степени не ниже 2. Тогда найдётся расширение E_1/F, содержащее корень α многочлена $p(x)$. Значит, $(x - \alpha) \mid f(x)$ над E_1. Разделив $f(x)$ на $x - \alpha$, получим многочлен меньшей степени над полем E_1, для которого всё уже доказано по предположению индукции.

Расширение полей получается как пересечение всех полей, каждое из которых содержит все корни многочлена $f(x)$. □

Определение 2.16. Если K — алгебраическое расширение поля F, являющееся полем разложения над F некоторого набора многочленов, то K называется *нормальным расширением* поля F.

Пример 2.17.
(1) Поле разложения многочлена $x^2 - 2$ над $\mathbb{Q}$ — это $\mathbb{Q}(\sqrt{2})$.
(2) Поле разложения многочлена $(x^2 - 2)(x^2 - 3)$ над $\mathbb{Q}$ — это $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
(3) Поле разложения многочлена $x^3 - 2$ над $\mathbb{Q}$ — это не $\mathbb{Q}(\sqrt[3]{2})$ (как можно было бы подумать), а $\mathbb{Q}(\sqrt[3]{2}, \zeta)$, где ζ есть первообразный кубический корень из 1. Это поле также можно представить как $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. В качестве упражнения читатель может доказать, что это расширение $\mathbb{Q}$ шестой степени.

(4) Поле разложения многочлена x^4+4 над $\mathbb{Q}$ — это не что иное, как $\mathbb{Q}(i)$, то есть расширение $\mathbb{Q}$ степени 2. Это связано с тем, что $x^4+4=(x^2+2x+2)(x^2-2x+2)=\prod(x\pm 1\pm i)$.

Из доказательства теоремы 2.15 с лёгкостью следует

Предложение 2.18. *Степень поля разложения многочлена степени n не превосходит $n!$.*

2.4. **Единственность поля разложения.** Теорема, которую мы сейчас докажем, является аналогом теоремы 1.20.

Теорема 2.19. *Пусть $\varphi\colon F\to F'$ — изоморфизм полей, $f(x)$ — многочлен над F, $f'(x)$ — его образ при этом изоморфизме. Пусть $E\supset F$ и $E'\supset F'$ — поля разложения многочленов f и f' соответственно. Тогда существует такой изоморфизм $\sigma\colon E\to E'$, который продолжает изоморфизм φ (т.е. $\sigma\,|_F=\varphi$).*

Доказательство. Если $f(x)$ раскладывается над F на линейные множители, то доказывать нечего: $E=F$, $E'=F'$, $\sigma=\varphi$. Это база индукции. Предположим, что требуемое утверждение доказано для многочленов, степень которых не превосходит n.

Пусть $p(x)$ — неприводимый сомножитель в $f(x)$, степень которого не меньше 2, и $p'(x)=\varphi(f(x))$. Присоединим к полю F корень многочлена $p(x)$: пусть $\alpha\in E$ — корень многочлена $p(x)$, $\beta\in E'$ — корень многочлена $p'(x)$. Согласно теореме 1.20, существует изоморфизм $\sigma'\colon F(\alpha)\to F'(\beta)$, продолжающий изоморфизм $\varphi'\colon F\to F'$.

Пусть теперь $F_1=F(\alpha)$, $F_1'=F'(\beta)$, $\sigma'\colon F_1\to F_1'$ — построенный нами изоморфизм. По предположению индукции, он может быть продолжен до изоморфизма $\sigma\colon E\to E'$. Теорема доказана. $\square$

Следствие 2.20. *Любые два поля разложения многочлена $f(x)$ изоморфны.*