3. Третья лекция, 25 сентября 2017 г.

3.1. **Поле разложения многочлена.** В первой лекции 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 3.1. 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 3.2. *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 3.3. Если K — алгебраическое расширение поля F, являющееся полем разложения над F некоторого набора многочленов, то K называется *нормальным расширением* поля F.

Пример 3.4.
(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 3.2 с лёгкостью следует

Предложение 3.5. *Степень поля разложения многочлена степени n не превосходит $n!$.*

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

Теорема 3.6. *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 $p'(x)=\varphi(p(x))$. 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. □

Следствие 3.7. *Любые два поля разложения многочлена $f(x)$ изоморфны.*

3.3. **Сепарабельные расширения.** В прошлом году обсуждалась конструкция алгебраического замыкания данного поля. Это такое расширение $\overline{F}$ поля F, над которым каждый многочлен $f(x)\in F[x]$ раскладывается на линейные множители:

$$f(x)=(x-\alpha_1)^{n_1}\dots(x-\alpha_k)^{n_k}.$$

Элемент α_i называется *кратным корнем* $f(x)$, если $n_i>1$.

Определение 3.8. Многочлен $f(x)\in F[x]$ называется *сепарабельным*, если он не имеет кратных корней в $\overline{F}$ (или, что то же самое, ни в каком расширении поля F).

Как выяснить, есть ли у многочлена кратные корни?

Определение 3.9. *Производная* многочлена $f(x)=a_nx^n+\dots+a_1x+a_0\in F[x]$ — это многочлен $f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\dots+2a_2x+a_1\in F[x]$.

Замечание 3.10. Отметим, что определение производной дается в чисто алгебраических терминах и не использует никаких эпсилонов, дельт и прочих предельных переходов. Поэтому оно имеет смысл над любым полем (в т.ч. положительной характеристики). Однако привычные свойства у него сохраняются.

Упражнение 3.11. Проверьте, что $(f+g)'(x) = f'(x) + g'(x)$ и $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$.

Предложение 3.12. *$f(x)$ имеет кратный корень α (над каким-либо расширением поля F) тогда и только тогда, когда α также является и корнем $f'(x)$. В частности, f сепарабелен тогда и только тогда, когда $(f, f') = 1$.*

Упражнение 3.13. Докажите это.

Пример 3.14. $f = x^n - 1$. Его производная $f'(x) = nx^{n-1}$ имеет единственный корень, равный 0, поэтому она взаимно проста с $f(x)$. Поэтому над любым полем имеются n *различных* корней n-й степени из единицы.

Пример 3.15. Пусть $\mathbb{F}_p$ — поле из p элементов, где p — простое число. Рассмотрим многочлен $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Его производная тождественно равна единице, поэтому он сепарабелен: имеет над алгебраическим замыканием $\overline{\mathbb{F}}_p$ ровно p^n различных корней.

Предложение 3.16. *Всякий неприводимый многочлен над полем нулевой характеристики сепарабелен.*

Доказательство. Пусть $f(x)$ неприводим, и $\deg f(x) = n$. Единственные его делители — это он сам и 1. Но производная $f'(x)$ имеет степень $n-1$. Поэтому она не может иметь общих делителей с $f(x)$. □

Особенность поля характеристики p состоит в том, что над ним степень производной многочлена может быть не $n-1$, а меньше (как мы видели). В частности, существуют отличные от констант многочлены, производная которых равна 0: это многочлены от x^p (т.е. те, в которые входят мономы 1, x^p, x^{2p} и т.д.).

Предложение 3.17 (Мечта первокурсника)**.** *Пусть* $\operatorname{char} F = p$. *Тогда для любых $a, b \in F$ верно, что $(a+b)^p = a^p + b^p$ и $(ab)^p = a^p b^p$.*

Доказательство. Второе равенство имеет место всегда. Первое равенство получается из бинома Ньютона с учётом того факта, что при $k \neq 0, p$ биномиальный коэффициент $\binom{p}{k}$ делится на p, то есть равен 0 в поле характеристики p. □

Из этого предложения следует, что отображение $\varphi\colon F \to F, \varphi(a) = a^p$ является инъективным эндоморфизмом поля F. Он называется *эндоморфизмом Фробениуса*. Если F конечно, то φ — *автоморфизм* (почему?).

Предложение 3.18. *Всякий неприводимый многочлен над конечным полем F сепарабелен.*

Доказательство. Пусть $\operatorname{char} F = p$. Допустим, что $f(x)$ несепарабелен. Тогда $f'(x) = 0$. Это значит, что $f(x) = q(x^p)$. Далее, поскольку φ — изоморфизм, из каждого элемента поля F извлекается корень p-й степени: для любого $x \in F$ существует такой $y \in F$, что $y^p = x$. Поэтому

$$f(x) = q(x^p) = \sum a_k x^{kp} = \sum (b_k)^p x^{kp} = \Big(\sum b_k x^k\Big)^p.$$

А это противоречит неприводимости многочлена $f(x)$. □

Здесь мы использовали то, что из каждого элемента поля F извлекается корень p-й степени. Такие поля называются *совершенными*.

Определение 3.19. Пусть $\operatorname{char} F = p$. Поле F называется *совершенным*, если для любого $x \in F$ найдётся $y \in F$, для которого $y^p = x$.

Следующее предложение доказывается дословно так же, как и предыдущее.

Предложение 3.20. *Всякий многочлен над совершенным полем сепарабелен.*

Чтобы читателю жизнь не казалась медом, приведем пример неприводимого, но несепарабельного многочлена.

Пример 3.21. Рассмотрим поле $\mathbb{F}_2(t)$ рациональных функций от одной переменной над $\mathbb{F}_2$. Из элемента t в этом поле не извлекается квадратный корень. (Контрольный вопрос: что является образом эндоморфизма Фробениуса?)

Многочлен $x^2 - t \in (\mathbb{F}_2(t))[x]$ *неприводим* над $\mathbb{F}_2(t)$. Над его алгебраическим замыканием он раскладывается на линейные множители: $x^2 - t = (x - \sqrt{t})(x + \sqrt{t})$. Однако эти два корня совпадают, поскольку $\sqrt{t} = -\sqrt{t}$! Поэтому этот многочлен несепарабелен.

3.4. **Конечные поля.** Пусть $n > 0$. Рассмотрим многочлен $x^{p^n} - x \in \mathbb{F}_p[x]$ из примера 3.15. Мы видели, что над $\overline{\mathbb{F}}_p$ он имеет p^n различных корней. Обозначим их множество через $\mathbb{F}$.

Пусть α и β — корни этого многочлена. Тогда $(\alpha\beta)^{p^n} = \alpha\beta$, $(\alpha^{-1})^{p^n} = \alpha^{-1}$ и $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$. Поэтому множество $\mathbb{F}$ замкнуто относительно взятия суммы, произведения и обратного, т.е. образует *поле*. Поскольку оно содержит все корни многочлена $x^{p^n} - x$ и не содержит ничего более, оно является полем разложения этого многочлена. В нем p^n элементов, поэтому $[\mathbb{F} : \mathbb{F}_p] = n$.

Далее, пусть $\mathbb{F}$ — произвольное конечное поле характеристики p. В нём p^n элементов. Мультипликативная группа $\mathbb{F}^\times$ имеет порядок

$p^n - 1$, поэтому каждый элемент $\alpha \in \mathbb{F}^\times$ в степени $p^n - 1$ равен единице. Значит, он удовлетворяет уравнению $x^{p^n} - x = 0$. Поэтому $\mathbb{F}$ является полем разложения многочлена $x^{p^n} - x$. Мы доказали следующее

Предложение 3.22. *Конечное поле порядка p^n существует и единственно с точностью до изоморфизма.*

Упражнение 3.23. Докажите, что для любого конечного поля его мультипликативная группа $\mathbb{F}^\times$ циклическая.

E-mail address: esmirnov@hse.ru