3. Лекция 3

3.1. **Алгебраическое замыкание.** В прошлой лекции мы научились строить расширение поля, в котором данный многочлен разлагается на линейные множители. Возникает естественный вопрос: а как построить такое поле, в котором *все* многочлены разлагаются на линейные множители? Это мотивирует следующие определения.

Определение 3.1. Пусть F — поле. $\overline{F}$ называется *алгебраическим замыканием* поля F, если $\overline{F}$ есть алгебраическое расширение F, и каждый многочлен $f(x) \in F[x]$ разлагается над $\overline{F}$ на линейные множители.

Определение 3.2. Поле F *алгебраически замкнуто*, если каждый многочлен с коэффициентами из F разлагается над F на линейные множители.

Несложно доказать, что алгебраическое замыкание поля (если оно вообще существует — а это мы докажем чуть позже) алгебраически замкнуто. Иначе говоря, $\overline{\overline{F}} = \overline{F}$: сколько ни замыкай алгебраически замкнутое поле, ничего нового не получишь.

Предложение 3.3. *Пусть $\overline{F}$ — алгебраическое замыкание F. Тогда $\overline{F}$ алгебраически замкнуто.*

Доказательство. Пусть $f(x)$ — многочлен с коэффициентами из $\overline{F}$, α — корень этого многочлена (в некотором расширении $\overline{F}$. Тогда $\overline{F}(\alpha)$ — алгебраическое расширение $\overline{F}$, а $\overline{F}$ алгебраично над F. Значит, $\overline{F}(\alpha)$ алгебраично над F. В частности, элемент α тоже алгебраичен над F. Поэтому он принадлежит $\overline{F}$, что и требовалось. □

Главный пример алгебраически замкнутого поля — поле $\mathbb{C}$.

Теорема 3.4 (Основная теорема алгебры)**.** *Поле комплексных чисел алгебраически замкнуто.*

Основную теорему алгебры обычно доказывают не алгебраическими средствами, а методами топологии ("Дама с собачкой") или анализа, вещественного или комплексного. Позже мы приведем чисто алгебраическое доказательство этой теоремы, использующее теорию Галуа.

При попытке построить алгебраическое замыкание первая мысль состоит в следующем: нужно добавить к полю одновременно корни всех многочленов. Однако возникает вопрос, в каком именно объемлющем поле это делать. Для этого либо требуется последовательно добавлять их, используя трансфинитную индукцию и ведя аккуратный "бухгалтерский учёт" того, какое поле получается. Мы поступим иначе, применив трюк, принадлежащий, по-видимому,

Эмилю Артину. При этом, впрочем, тоже не обойдётся без трансфинитной индукции — а именно, нам потребуется лемма Цорна. Напомним её.

3.2. **Лемма Цорна.** Пусть A — частично упорядоченное множество, т.е. множество, на котором задано бинарное отношение $\leq$, удовлетворяющее для любых элементов $x, y, z \in A$ следующим аксиомам:

- $x \leq x$ (рефлексивность);
- из $x \leq y$ и $y \leq x$ следует, что $x = y$ (антисимметричность);
- из $x \leq y$ и $y \leq z$ следует, что $x \leq z$ (транзитивность).

Если $x \leq y$ или $y \leq x$, говорят, что x и y *сравнимы*.

Напомним основные определения, связанные с частично упорядоченными множествами. *Цепью*, или *вполне упорядоченным множеством*, называется такое подмножество $B \subset A$, любые два элемента которого сравнимы. *Верхней гранью* подмножества B называется такой элемент $u \in A$, что $b \leq u$ для любого $b \in B$. *Максимальный элемент* множества A — это такой элемент $m \in A$, что если $m \leq x$ для некоторого $x \in A$, то $m = x$. (Отметим, что максимальный элемент не обязан быть *наибольшим* — в частности, он может быть не единственным).

Ключевое утверждение, которое нам понадобится — это

Теорема 3.5 (лемма Цорна)**.** *Пусть A — частично упорядоченное множество, в котором у любой цепи есть верхняя грань. Тогда в A имеется максимальный элемент.*

3.3. **Конструкция алгебраического замыкания.**

Теорема 3.6. *Для всякого поля F существует алгебраически замкнутое поле K, содержащее F.*

Доказательство. Пусть $f = f(x) \in F[x]$ — многочлен со старшим коэффициентом 1. Сопоставим *каждому* такому многочлену свою переменную x_f и рассмотрим кольцо $F[\dots, x_f, \dots]$ многочленов от (огромного числа) всех этих переменных. В каждый из многочленов мы можем подставить "его собственную" переменную; получим многочлен $f(x_f)$, лежащий в этом кольце.

Рассмотрим идеал $I = (f(x_f))$, порожденный всеми такими многочленами.

Лемма 3.7. *Идеал I собственный, т.е. не совпадает со всем кольцом $F[\dots, x_f, \dots]$.*

Доказательство леммы. Пусть это не так. Тогда $1 \in I$. Значит, единица выражается через образующие идеала:

$$1 = g_1 f_1(x_{f_1}) + g_2 f_2(x_{f_2}) + \dots + g_n f_n(x_{f_n}).$$

Положим $x_i = x_{f_i}$ при i от 1 до n и обозначим через $x_{n+1}, \dots, x_m$ все остальные переменные, от которых зависят многочлены g_i (таковых будет конечное число). Получим, что

$$1 = g_1(x_1, \dots, x_m)f_1(x_1) + \dots + g_n(x_1, \dots, x_m)f_n(x_n).$$

Пусть $\widetilde{F}$ — конечное расширение поля F, содержащее корень α_i каждого многочлена $f_i(x)$. Положим $x_i = \alpha_i$ при i от 1 до n, а $x_{n+1}, \dots, x_m$ положим равными нулю; получим, что (в поле $\widetilde{F}$) $0 = 1$. Противоречие; значит, идеал I собственный. □

Согласно лемме Цорна, I содержится в максимальном идеале $\mathfrak{m} \subset F[\dots, x_f, \dots]$. Положим $K_1 = F[\dots, x_f, \dots]/\mathfrak{m}$. Это поле (т.к. идеал $\mathfrak{m}$ максимальный), содержащее копию F. У всех многочленов f в этом поле есть по корню — это образы переменных x_f при факторизации, т.к. $f(x_f) \in I \subset \mathfrak{m}$. Мы получили расширение K_1/F, в котором каждый многочлен из $F[x]$ имеет корень.

Далее применим ту же конструкцию к полю K_1: построим такое его расширение, в котором каждый многочлен с коэффициентами из F имеет корень. Получим последовательность расширений

$$F = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_j \subset K_{j+1} \subset \dots$$

Положим $K = \bigcup_{j \geq 0} K_j$. Это расширение поля F. Ясно, что K алгебраически замкнуто: любой многочлен из $K[x]$ имеет коэффициенты из некоторого K_j, то есть, по построению, имеет корень в K_{j+1}. □

В результате данной конструкции мы не обязательно получили алгебраическое замыкание F. Однако последнее там заведомо содержится.

Предложение 3.8. *Пусть K — алгебраически замкнутое поле, содержащее F. Множество всех алгебраических элементов $\overline{F} \subset K$ есть алгебраическое замыкание F.*

Доказательство. Очевидно. □

Задача 3.9. Докажите, что алгебраическое замыкание поля единственно с точностью до изоморфизма.

3.4. **Сепарабельные расширения.** Над алгебраическим замыканием $\overline{F}$ поля F 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 3.10. 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 3.11. *Производная* многочлена $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ — это многочлен $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1 \in F[x]$.

Замечание 3.12. 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 3.13. Проверьте, что $(f+g)'(x) = f'(x) + g'(x)$ и $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$.

Предложение 3.14. *$f(x)$ 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 3.15. Докажите это.

Пример 3.16. $f = x^n - 1$. 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 3.17. 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 3.18. *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 3.19 (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 3.20. *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 3.21. 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 3.22. *Всякий многочлен над совершенным полем сепарабелен.*

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

Пример 3.23. 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.

3.5. **Конечные поля.** Пусть $n > 0$. Рассмотрим многочлен $x^{p^n} - x \in \mathbb{F}_p[x]$ из примера 3.17. 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 3.24. *Конечное поле порядка p^n существует и единственно с точностью до изоморфизма.*

Упражнение 3.25. Докажите, что для любого конечного поля его мультипликативная группа $\mathbb{F}^\times$ циклическая.