АЛГЕБРА, ТРЕТИЙ СЕМЕСТР

Е. Ю. СМИРНОВ

Abstract. Записки лекций 3 семестра, осень 2012/13 учебного года

1. Лекция 1

Пусть F — *поле*, то есть коммутативное кольцо с единицей, в котором у каждого ненулевого элемента есть обратный по умножению.

Пример 1.1. Следующие множества являются полями: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, *конечное поле из* p *элементов* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p — простое число), *поле частных* $\operatorname{Quot} A$ произвольного целостного коммутативного кольца A; *поле рациональных функций* $F(t)$ над произвольным полем F.

Множество обратимых элементов поля образует группу по умножению, которую мы будем обозначать $F^\times$.

1.1. Характеристика поля.

Простейший инвариант поля — это его *характеристика*.

Определение 1.2. *Характеристикой* поля F (обозначение: $\operatorname{char} F$) называется наименьшее положительное число p, для которого $1 + \cdots + 1 = 0$ (p слагаемых). Если такого числа нет, то полагают $\operatorname{char} F = 0$.

Предложение 1.3. $\operatorname{char} F$ — *простое число или нуль. Если* $\operatorname{char} F = p$, *то* $\alpha + \cdots + \alpha = 0$ *для любого* $\alpha \in F$.

Доказательство. Пусть 1_F — единица поля F. Для краткости обозначим $1_F + \cdots + 1_F$ (n раз, $n \in \mathbb{Z}_+$) через $n \cdot 1_F$. Очевидно, что $m \cdot 1_F + n \cdot 1_F = (m+n) \cdot 1_F$ и $(m \cdot 1_F)(n \cdot 1_F) = mn \cdot 1_F$. Отсюда сразу следует первое утверждение предложения. Второе утверждение вытекает из равенства $p \cdot \alpha = p \cdot (1_F \cdot \alpha) = (p \cdot 1_F) \cdot \alpha = 0$. □

Из доказательства предложения следует, что имеется гомоморфизм колец $\varphi\colon \mathbb{Z} \to F$, $\varphi(n) = n \cdot 1_F$. Его ядро — это $\operatorname{Ker} \varphi = (\operatorname{char} F) \cdot \mathbb{Z}$. Значит, имеет место *вложение* либо $\mathbb{Z}$, либо $\mathbb{Z}/p\mathbb{Z}$ в F. Поскольку F — поле (т.е. оно замкнуто относительно взятия отношений), в нём имеется *подполе*, изоморфное либо $\mathbb{Q}$, если

$\operatorname{char} F = 0$, либо $\mathbb{Z}/p\mathbb{Z}$, если $\operatorname{char} F = p$. Ясно, что это *наименьшее* подполе, содержащее 1_F (т.е. подполе, *порожденное* 1_F). Оно называется *простым* подполем (the prime subfield).

Пример 1.4. Простое подполе в $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — это $\mathbb{Q}$; простое поле в $\mathbb{F}_p(t)$ — это $\mathbb{F}_p$.

1.2. Степень расширения.

Определение 1.5. Пусть поле F содержится в поле K. В этом случае говорят, что K является *расширением* поля F. Обозначение: K/F (косая черта здесь не подразумевает никакого факторобразования).

Ясно, что в таком случае K является векторным пространством над полем F. В частности, всякое поле есть векторное пространство над своим простым подполем.

Определение 1.6. Размерность K как векторного пространства над F называется *степенью расширения* K над F. Обозначение: $[K : F]$ или $\deg K/F$. Расширение называется *конечным*, если $[K : F]$ конечна, и *бесконечным* в противном случае.

Упражнение 1.7. Докажите, что: $[\mathbb{C} : \mathbb{R}] = 2$; $[\mathbb{R} : \mathbb{Q}] = \infty$; $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$; $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Важное свойство степени расширений — ее мультипликативность.

Теорема 1.8. *Пусть $F \subset K \subset L$ — башня расширений полей. Тогда*

$$[L : F] = [L : K] \cdot [K : F],$$

либо левая и правая часть одновременно равны бесконечности.

Доказательство. Пусть сначала $[L : K] = m$, $[K : F] = n$, причём обе эти величины конечны. Пусть $\alpha_1, \ldots, \alpha_m$ — базис L над K, а $\beta_1, \ldots, \beta_n$ — базис K над F. Тогда всякий элемент из L представи́м в виде

$$a = a_1\alpha_1 + \cdots + a_m\alpha_m, \qquad a_i \in K.$$

Далее, каждый из a_i раскладывается по базису из β_j:

$$a_i = b_{i1}\beta_1 + \cdots + b_{in}\beta_n, \qquad b_{ij} \in F. \tag{$*$}$$

Значит, $a = \sum_{i,j} b_{ij}\alpha_i\beta_j$. Поэтому элементы $\alpha_i\beta_j$ *порождают* L как векторное пространство над F, т.е. $[L : F] \leq mn$.

Докажем, что они линейно независимы. Пусть $b_{ij}\alpha_i\beta_j = 0$, где $b_{ij} \in F$. Определив $a_i \in K$ по формулам $(*)$, получим, что $a_1\alpha_1 + \cdots + a_m\alpha_m = 0$. Значит, все $a_i = 0$, т.к. α_i — базис L над K. Поэтому при любом i имеется равенство $b_{i1}\beta_1 + \cdots + b_{in}\beta_n = 0$. Теперь воспользуемся тем, что β_i составляют базис K над F и получим, что все b_{ij} равны нулю, что и требовалось. Аналогичное

рассуждение проходит в случае, когда одна из частей бесконечна. □

Следствие 1.9. *Пусть L/F — конечное расширение полей, $K \subset L$ — подполе. Тогда $[L : F]$ делится на $[K : F]$.*

Пример 1.10. $\sqrt{2}$ не содержится в поле $\mathbb{Q}(\alpha)$, где α — вещественный корень многочлена $x^3 - 3x - 1$, т.к. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ (это будет показано ниже), а $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

1.3. **Присоединение корня.** Как получить поле комплексных чисел из поля вещественных чисел? Рассмотрим квадратичное уравнение, неразрешимое над $\mathbb{R}$, например, $x^2 + 1 = 0$. Добавим его решение к полю в качестве формальной переменной, обозначив её через i. При этом i будет удовлетворять соотношению $i^2 + 1 = 0$. Нетрудно доказать, что $\mathbb{R}$-векторное пространство, натянутое на 1 и i, будет полем (квадратичным расширением поля $\mathbb{R}$).

Попробуем обобщить эту конструкцию на случай произвольного поля F и неприводимого многочлена $p(x) \in F[x]$, степень которого выше 1 (т.е. $p(x)$ не имеет корней в F). А именно, построим такое расширение поля F, в котором многочлен $p(x)$ будет иметь корень.

Нам пригодится следующее очевидное

Предложение 1.11. *Пусть $\varphi\colon F \to F'$ — гомоморфизм полей. Тогда либо $\varphi \equiv 0$, либо φ является вложением.*

Теорема 1.12. *Пусть F — поле, $p(x) \in F[x]$ — неприводимый многочлен. Существует такое расширение K поля F, в котором многочлен $p(x)$ имеет корень.*

Доказательство. Рассмотрим главный идеал $(p(x)) \subset F[x]$ в кольце многочленов над F. Поскольку многочлен $p(x)$ неприводим, порождённый им идеал прост. Но в $F[x]$, как в любом кольце главных идеалов, всякий простой идеал является максимальным. Поэтому факторкольцо $K = F[x]/(p(x))$ является *полем*. Рассмотрим гомоморфизм факторизации

$$\pi\colon F[x] \to K = F[x]/(p(x)).$$

Рассмотрим гомоморфизм φ, полученный ограничением гомоморфизма π на множество констант $F \subset F[x]$. $\varphi \not\equiv 0$, поскольку $\varphi(1_F) = \pi(1_F) = 1_K$. Значит, в силу предыдущего предложения, $\varphi(F) \cong F$ — подполе в K, изоморфное F. Поэтому поле K можно считать расширением поля F (отождествив F с его образом при этом изоморфизме).

Далее, пусть $\overline{x} = \pi(x)$. Тогда

$$\pi(\overline{x}) = \overline{p(x)} = p(x) \mod (p(x)) = 0.$$

Значит, $\overline{x} \in K$ — элемент поля K, являющийся корнем многочлена $p(x)$. □

Замечание 1.13. Из нашей конструкции *не* следует, что многочлен $p(x)$ раскладывается над полем K на линейные множители! (Приведите контрпример сами).

Строение полученного поля как векторного пространства над F описывается следующей теоремой.

Теорема 1.14. *Пусть $f(x) \in F[x]$ — неприводимый многочлен степени n над F, и пусть $K = F[x]/(p(x))$. Пусть $\theta = x \mod (p(x)) \in K$. Тогда $1, \theta, \dots, \theta^{n-1}$ — базис K как векторного пространства над F. Иначе говоря,*

$$K = \{a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1} \mid a_0, \dots, a_{n-1} \in F\}.$$

В частности, $[K : F] = n$.

Доказательство. Пусть $a(x) \in F[x]$. Поскольку $F[x]$ — евклидово кольцо, $a(x)$ можно поделить с остатком на $p(x)$:

$$a(x) = p(x)q(x) + r(x), \qquad \text{т.е. } a(x) \equiv r(x) \mod (p(x)).$$

Степень $r(x)$ меньше n, значит, $1, \theta, \dots, \theta^{n-1}$ *порождают* K. Осталось доказать, что они линейно независимы. Действительно, их линейная зависимость означала бы, что при некоторых $b_0, \dots, b_{n-1} \in F$

$$b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1} = 0,$$

т.е. $b(x) = b_0 + b_1 x + \dots + b_{n-1}x^{n-1}$ делится на $p(x)$. Противоречие. Значит, $[K : F] = n$. □

1.4. **Простое расширение.** Пусть F — подполе в K, $\alpha \in K$ — некоторый элемент. Существуют поля, содержащие и F, и α (например, K). Пересечение двух таких полей снова содержит и F, и α. Значит, существует наименьшее поле с этим свойством. Будем обозначать его через $F(\alpha)$.

Определение 1.15. $F(\alpha)$ называется *простым расширением* поля F.

Аналогично для любого набора элементов $\alpha, \beta, \dots \in K$ (даже не обязательно конечного) существует наименьшее подполе в K, содержащее F и все эти элементы. Оно обозначается через $F(\alpha, \beta, \dots)$.

Определение 1.16. Поле $F(\alpha, \beta, \dots)$ называется *полем, порожденным элементами $\alpha, \beta, \dots$ над F.*

Задача 1.17 (Теорема о примитивном элементе)**.** Пусть $F \subset K$ — расширение полей нулевой характеристики. Тогда для любых $\alpha, \beta \in K$ найдётся элемент $\gamma \in K$, для которого $F(\alpha, \beta) = F(\gamma)$ (элемент γ называется *примитивным*).

Теорема 1.18. *Пусть $p(x) \in F(x)$ — неприводимый многочлен. Пусть $F \subset K$, и $\alpha \in K$ — корень многочлена $p(x)$, т.е. $p(\alpha) = 0$. Тогда $F(\alpha) \cong F[x]/((p(x))$.*

Замечание 1.19. Отличие от теоремы из предыдущего пункта состоит в том, что здесь мы уже *предполагаем* наличие корня у данного многочлена в некотором расширении поля F, а не строим такое расширение.

Доказательство. Имеется гомоморфизм $\varphi\colon F[x] \to F(\alpha) \subset K$, $a(x) \mapsto a(\alpha)$. Многочлен $p(x)$ оказывается в ядре этого гомоморфизма. Поэтому φ определен на факторкольце:

$$\varphi\colon F[x]/(p(x)) \to F(\alpha).$$

Но, поскольку многочлен $p(x)$ неприводим, $F[x]/(p(x))$ — поле, причём φ не равен тождественно нулю. Значит, φ — вложение полей. Но $\operatorname{Im}\varphi$ — подполе, содержащее F и α. Значит, в силу минимальности $F(\alpha)$, φ является сюръекцией, т.е. изоморфизмом. □

1.5. **Единственность простого расширения.** Наше определение простого расширения апеллировало к объемлющему полю K. Оказывается, что от него ничего не зависит.

Пусть $\varphi\colon F\tilde{\to}F'$ — изоморфизм полей. Его можно продолжить до изоморфизма колец многочленов над этими полями: $\varphi\colon F[x]\to F'[x]$. Пусть $p(x) \in F[x]$ — неприводимый многочлен. Тогда его образ $p'(x) = \varphi(p(x))$ тоже неприводим (почему?). Ясно, что при этом факторкольца по соответствующим идеалам также изоморфны:$F[x]/(p(x)) \cong F'[x]/(p(x))$. Это позволяет нам доказать теорему о единственности простого расширения.

Теорема 1.20. *Пусть $\varphi\colon F \to F'$ — изоморфизм полей, $p(x)$ — неприводимый многочлен над F, $p'(x)$ — его образ при этом изоморфизме. Пусть α — корень многочлена $p(x)$ в некотором расширении поля F, а β — корень многочлена $p'(x)$ в некотором расширении поля F'. Тогда существует такой изоморфизм $\sigma\colon F(\alpha) \to F'(\beta)$, $\sigma(\alpha) = \beta$, который продолжает изоморфизм φ (т.е. $\sigma\mid_F = \varphi$).*

Доказательство. Как обсуждалось выше, $F[x]/(p(x)) \cong F'[x]/(p(x))$ — изоморфизм полей. А из предыдущей теоремы мы знаем, что $F[x]/(p(x)) \cong F(\alpha)$ и $F'[x]/(p(x)) \cong F'(\beta)$. □

1.6. **Конечно порожденные расширения.**

Определение 1.21. Расширение полей K/F называется *конечно порожденным*, если оно порождено конечным числом элементов, т.е. если существуют такие $\alpha_1, \ldots, \alpha_n$, что $K = F(\alpha_1; \ldots, \alpha_n)$.

Замечание 1.22. Не надо путать конечные и конечно порожденные расширения. Разумеется, каждое конечное расширение является конечно порожденным. А вот обратное неверно: скажем, расширение $\mathbb{Q}(\pi)/\mathbb{Q}$ конечно порожденное (и даже простое), но не конечное.

Конечные расширения можно получать как последовательность простых расширений:

Лемма 1.23. $F(\alpha, \beta) = (F(\alpha))(\beta)$.

Упражнение 1.24. Докажите эту лемму.

1.7. **Алгебраические элементы.** Пусть $F \subset K$, $\alpha \in K$.

Определение 1.25. Элемент $\alpha \in K$ называется *алгебраическим* над F, если α является корнем некоторого многочлена с коэффициентами из F.

Замечание 1.26. Если α алгебраичен над F и $F \subset L$, то α алгебраичен и над L.

Определение 1.27. Расширение полей K/F называется *алгебраическим*, если каждый элемент из K алгебраичен над F.

Предложение 1.28. *Для каждого алгебраического элемента α существует единственный многочлен $m_{\alpha,F}(x) \in F[x]$ минимальной степени со старшим коэффициентом 1, для которого $m_{\alpha,F}(\alpha) = 0$. Многочлен $f(x) \in F[x]$ имеет корень α тогда и только тогда, когда он делится на $m_{\alpha,F}(x)$ в кольце $F[x]$.*

Доказательство. Существование такого многочлена очевидно. Пусть $m(x) = m_{\alpha,F}(x)$ — такой многочлен, и пусть $f(\alpha) = 0$. Разделим f на m с остатком: $f(x) = m(x) \cdot g(x) + r(x)$, где $\deg r(x) < \deg m(x)$. Поскольку $r(\alpha) = 0$, а $m(x)$ имеет минимальную степень, то $r(x) = 0$. Значит, $f(x)$ делится на $m(x)$ без остатка. Отсюда же следует единственность $m(x)$. □

Следствие 1.29. *Если L/F — расширение полей, а элемент α алгебраичен над F, то $m_{\alpha,L}(x) \mid m_{\alpha,F}(x)$ в кольце $L[x]$.*

Определение 1.30. Многочлен $m_{\alpha,F}(x)$ называется *минимальным многочленом* элемента α. Его степень $\deg \alpha := \deg m_{\alpha,F}(x)$ называется *степенью* элемента α.

Предложение 1.31. *Пусть α — алгебраический элемент. Тогда $F(\alpha) = F[x]/(m_{\alpha,F}(x))$. В частности, $[F(\alpha) : F] = \deg \alpha$.*

Доказательство. Это следует из теоремы 1.18. □

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 $1, \alpha, \alpha^2, \ldots, \alpha^n$ 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 $\alpha_1, \ldots, \alpha_k$ степеней $n_1, \ldots, n_k$. В этом случае $[K : F] \leq n_1 \ldots n_k$.*

Доказательство. Часть "тогда" доказана выше. Докажем часть "только тогда". Пусть K/F конечно, $\alpha_1, \ldots, \alpha_n$ — 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 $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots$. 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. □

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, $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F]$. □

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. □

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. □

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

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 $F[\ldots, x_f, \ldots]$ 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 $F[\ldots, x_f, \ldots]$.*

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

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

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

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

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 $x_{n+1}, \ldots, x_m$ положим равными нулю; получим, что (в поле $\widetilde{F}$) $0 = 1$. Противоречие; значит, идеал I собственный. □

Согласно лемме Цорна, I содержится в максимальном идеале $\mathfrak{m} \subset F[\ldots, x_f, \ldots]$. Положим $K_1 = F[\ldots, x_f, \ldots]/\mathfrak{m}$. 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

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

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:

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

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.

4. Лекция 4

4.1. **Автоморфизмы полей.** Пусть K — поле, F — его подполе. *Автоморфизм* поля K — это изоморфизм $\sigma\colon K \to K$. Говорят, что автоморфизм σ оставляет подполе F неподвижным, если $\sigma\alpha = \alpha$ для любого $\alpha \in F$. Группа автоморфизмов поля K обозначается через $\mathrm{Aut}(K)$, подгруппа автоморфизмов, оставляющих неподвижным подполе F — через $\mathrm{Aut}(K/F)$. Поскольку для любого автоморфизма $\sigma(0) = 0$ и $\sigma(1) = 1$, то σ оставляет неподвижным простое подполе $\mathbb{Q}$ или $\mathbb{F}_p$. Значит, если F — простое подполе, то $\mathrm{Aut}(K/F) = \mathrm{Aut}(K)$.

Докажем, что элементы K, алгебраические над F, при любом автоморфизме переходят в алгебраические элементы той же степени.

Предложение 4.1. *Пусть элемент $\alpha \in K$ алгебраичен над F, и $m_\alpha(x)$ — его минимальный многочлен. Тогда для любого $\sigma \in \mathrm{Aut}(K/F)$ элемент $\sigma\alpha$ — тоже корень $m_\alpha(x)$. Более того, если α — корень многочлена $f(x) \in F[x]$, то $\sigma\alpha$ — тоже корень этого многочлена.*

Доказательство. Пусть $f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$. Применим к этому равенству автоморфизм σ. Учитывая, что $\sigma(a_i) = a_i$, получим, что $a_n(\sigma\alpha)^n + \cdots + a_1\sigma\alpha + a_0 = 0$, что и означает, что $f(\sigma\alpha) = 0$. □

Пример 4.2. Пусть $K = \mathbb{Q}(\sqrt{2})$. Рассмотрим элемент $\sqrt{2}$; его минимальный многочлен — $x^2 - 2$. Это значит, что для всякого автоморфизма $\tau \in \mathrm{Aut}\,\mathbb{Q}(\sqrt{2})$ элемент $\tau(\sqrt{2})$ тоже есть корень этого многочлена, то есть $\sqrt{2}$ или $-\sqrt{2}$. Это полностью описывает автоморфизм τ: в первом случае он оказывается тождественным, а во втором — это *сопряжение*: $\tau(a + b\sqrt{2}) = a - b\sqrt{2}$. Поэтому $\mathrm{Aut}\,\mathbb{Q}(\sqrt{2}) = \mathbb{Z}/2\mathbb{Z}$.

Пример 4.3. Пусть $K = \mathbb{Q}(\sqrt[3]{2})$. Тогда минимальный многочлен элемента $\sqrt[3]{2}$ — это $x^3 - 2$. В поле K нет других элементов, удовлетворяющих уравнению $x^3 - 2 = 0$ (остальные два корня этого многочлена не являются вещественными, а значит, не лежат и в $\mathbb{Q}(\sqrt[3]{2})$. Поэтому любой автоморфизм поля $\mathbb{Q}(\sqrt[3]{2})$ оставляет $\sqrt[3]{2}$ на месте, а значит, является тождественным: $\mathrm{Aut}\,\mathbb{Q}(\sqrt[3]{2}) = \{1\}$.

4.2. **Соответствие между подполями и подгруппами в** $\mathrm{Aut}(K/F)$**.** Пусть E — некоторое "промежуточное" подполе в K: $F \subset E \subset K$. Тогда в $\mathrm{Aut}(K/F)$ можно рассмотреть подгруппу $\mathrm{Aut}(K/E)$ автоморфизмов, оставляющих E неподвижным. Обратно, подгруппе H в $\mathrm{Aut}(K/F)$ можно сопоставить подмножество элементов $K^H \subset K$, состоящее из всех неподвижных относительно H элементов.

Предложение 4.4. *Пусть $H \subset \mathrm{Aut}(K/F)$ — подгруппа. Тогда $K^H = \{\alpha \in K \mid \sigma\alpha = \alpha \quad \forall \sigma \in H\}$ — подполе в K.*

Доказательство. По определению гомоморфизма, подмножество K^H будет замкнуто относительно взятия суммы, произведения и обратного. Значит, это подполе. □

Следующее предложение тоже очевидно:

Предложение 4.5. *Такое соответствие между подполями и подгруппами обращает отношение включения: если $F_1 \subset F_2 \subset K$, то $\mathrm{Aut}(K/F_2) \supset \mathrm{Aut}(K/F_1)$. Обратно, если $H_1 \subset H_2 \subset \mathrm{Aut}(K/F)$, то $K^{H_1} \supset K^{H_2}$.*

Пример 4.3 показывает, что это соответствие не всегда биективно: так, подполю $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ и всему полю $\mathbb{Q}(\sqrt[3]{2})$ соответствует одна и та же (тривиальная) подгруппа автоморфизмов. Получается, что автоморфизмов в $\mathrm{Aut}(K/F)$ "слишком мало" для того, чтобы это соответствие было бы биективным.

Приведем ещё один пример:

Пример 4.6. Пусть теперь $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ — поле разложения многочлена $x^3 - 2$ (напомним, что его корни имеют вид $\zeta^j \sqrt[3]{2}$, где $0 \le j \le 2$, а $\zeta = (-1 + \sqrt{-3})/2$ — первообразный корень из 1 степени 3). Это расширение степени 6. Группа $\mathrm{Aut}(K)$ состоит из шести элементов, реализующих все перестановки трёхэлементного множества корней этого многочлена, т.е. $\mathrm{Aut}(K) \cong S_3$. В K имеется одно подполе, являющееся квадратичным расширением $\mathbb{Q}$ — это $\mathbb{Q}(\sqrt{-3})$, и три расширения $\mathbb{Q}$ степени 3: это $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\zeta\sqrt[3]{2})$ и $\mathbb{Q}(\zeta^2\sqrt[3]{2})$. Подгруппы, отвечающие этим подполям в S_3 — это нормальная подгруппа A_3 (она имеет индекс 2) и три подгруппы индекса 3, порождённые транспозициями и не являющиеся нормальными. Видим, что в данном случае описанное соответствие между подгруппами и подполями биективно, причём степень подполя над $\mathbb{Q}$ равняется индексу отвечающей ему подгруппы в $\mathrm{Aut}(K)$.

Такие "хорошие" расширения полей называются *расширениями Галуа*.

4.3. **Расширения Галуа. Формулировка основной теоремы.** В этом разделе мы анонсируем результаты, которые будут доказаны позже.

Теорема 4.7. *Для произвольного конечного расширения имеется неравенство $|\mathrm{Aut}(K/F)| \le [K : F]$.*

Мы видели в предыдущих примерах, что в "хороших" случаях (скажем, для квадратичного расширения, или в примере 4.6) это неравенство обращается в равенство. Сначала дадим "хорошей" ситуации название:

Определение 4.8. Расширение полей K/F называется *расширением Галуа*, если

$$|\operatorname{Aut}(K/F)| = [K : F].$$

Группа автоморфизмов поля K при этом называется его *группой Галуа* и обозначается через $\operatorname{Gal}(K/F)$.

Биекции между подполями в K и подгруппами в $\operatorname{Aut}(K/F)$, которую мы видели в примерах 4.2 и 4.6, суть частные случаи следующей общей теоремы.

Теорема 4.9 (Основная теорема теории Галуа)**.** *Пусть K/F — расширение Галуа. Тогда имеется биекция между подполями в K, содержащими F, и подгруппами в группе $G = \operatorname{Gal}(K/F)$. При этой биекции подполю E соответствует подгруппа $H = \operatorname{Aut}(K/E) \subset G$, а подгруппе $H \subset G$ — её неподвижное подполе $E = K^H$. Эта биекция обладает следующими свойствами:*

(1) *она обращает включения: $E_1 \subset E_2 \Leftrightarrow H_1 \supset H_2$;*
(2) *степень расширения $[K : E]$ равна порядку группы H, а степень расширения $[E : F]$ — индексу подгруппы $[G : H]$;*
(3) *расширение K/E является расширением Галуа, и $\operatorname{Gal}(K/E) = H$;*
(4) *расширение E/F является расширением Галуа тогда и только тогда, когда H нормальна в G; при этом $\operatorname{Gal}(E/F) = G/H$;*
(5) *Пересечению подполей $E_1 \cap E_2$ соответствует группа $\langle H_1, H_2\rangle \subset G$, а композиту полей E_1E_2 — пересечение групп $H_1 \cap H_2$.*

Доказательству теорем из этого раздела будет посвящена оставшаяся часть этой и значительная часть следующей лекции.

4.4. **Характеры.**

Определение 4.10. *(Мультипликативный) характер* группы G со значениями в поле L — это гомоморфизм $\chi\colon G \to L^*$.

Характер можно (и нужно) рассматривать как L-значную функцию на группе G.

Замечание 4.11. В курсе теории представлений мы уже встречались с более общим понятием характера: мы рассматривали следы всевозможных конечномерных (а не только одномерных) представлений. Однако характеры у нас были только комплекснозначные, и работа с ними существенно использовала специфику поля $\mathbb{C}$. Оказывается, что некоторые утверждения — например, теорема о линейной независимости характеров — верны и для произвольного поля.

Теорема 4.12. *Попарно различные характеры $\chi_1, \ldots, \chi_n$ линейно независимы как функции на G.*

Доказательство. Предположим противное: пусть имеется нулевая линейная комбинация характеров, т.е. при всех $g \in G$

$$a_1\chi_1(g) + \cdots + a_n\chi_n(g) = 0.$$

Будем считать, что n минимально (т.е. всякая линейная комбинация $n-1$ характера уже будет нетривиальной).

Поскольку характеры χ_1 и χ_n различны, найдётся такой элемент h, что $\chi_1(h) \neq \chi_n(h)$. Домножим предыдущее равенство на $\chi_n(h)$:

$$a_1\chi_n(h)\chi_1(g) + \cdots + a_n\chi_n(h)\chi_n(g) = 0. \qquad (*)$$

С другой стороны, для любого g

$$a_1\chi_1(hg) + \cdots + a_n\chi_n(hg) = 0,$$

то есть, в силу мультипликативности характеров,

$$a_1\chi_1(h)\chi_1(g) + \cdots + a_n\chi_n(h)\chi_n(g) = 0.$$

Вычтем из этого равенства $(*)$:

$$a_1[\chi_1(h) - \chi_n(h)]\chi_1(g) + \cdots + a_{n-1}[\chi_{n-1}(h) - \chi_n(h)]\chi_{n-1}(g) = 0.$$

Мы получили нетривиальную (т.к. $\chi_1(h) - \chi_n(h) \neq 0$) линейную комбинацию из $n-1$ характера, тождественно равную нулю. Противоречие. □

Пусть $\sigma\colon K \to L$ — гомоморфизм полей (ненулевой, а следовательно, инъективный). Тогда $\sigma\colon K^* \to L^*$ — характер. Обратно, каждый характер однозначно задаёт гомоморфизм: σ нужно доопределить только в нуле, а $\sigma(0) = 0$. Получается

Следствие 4.13. *Пусть $\sigma_1, \ldots, \sigma_n$ — различные вложения $K \to L$. Тогда они линейно независимы как L-значные функции на K.*

4.5. **Порядок группы автоморфизмов поля равен степени расширения поля над ее неподвижным подполем.** В этом разделе мы докажем следующую теорему.

Теорема 4.14. *Пусть $G = \{\sigma_1 = 1, \ldots, \sigma_n\}$ — некоторая группа автоморфизмов поля K, и пусть $F = K^G$ — неподвижное подполе этой группы. Тогда $[K : F] = n = |G|$.*

Доказательство. Сначала покажем, что $n \leq [K : F]$. Предположим противное: $n > [K : F] = m$, и пусть $\omega_1, \ldots, \omega_m$ — базис K как векторного пространства над F. Рассмотрим систему уравнений

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \cdots + \sigma_n(\omega_1)x_n &= 0; \\ &\cdots \\ \sigma_1(\omega_m)x_1 + \cdots + \sigma_n(\omega_m)x_n &= 0. \end{aligned}$$

Это система из m уравнений с $n > m$ неизвестными. Значит, у неё есть нетривиальное решение $\beta_1, \ldots, \beta_n$, где $\beta_i \in K$.

Пусть $a_1, \ldots, a_m$ — произвольные элементы поля F. Тогда $\sigma_i(a_j) = a_j$. Учитывая это, домножим i-е уравнение на a_i и получим:

$$\begin{aligned} \sigma_1(a_1\omega_1)\beta_1 + \cdots + \sigma_n(a_1\omega_1)\beta_n &= 0; \\ &\cdots \\ \sigma_1(a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_m\omega_m)\beta_n &= 0. \end{aligned}$$

Сложив все уравнения, получим, что

$$\sigma_1(a_1\omega_1 + \cdots + a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_1\omega_1 + \cdots + a_m\omega_m)\beta_n = 0.$$

Линейная комбинация в скобках может при подходящем выборе a_i равняться любому элементу из K, т.к. ω_i — базис. Значит, для любого $\alpha \in K$

$$\sigma_1(\alpha)\beta_1 + \cdots + \sigma_n(\alpha)\beta_n = 0.$$

Получаем, что σ_i линейно зависимы, что противоречит следствию 4.13.

Теперь докажем неравенство в обратную сторону: $n \geq [K : F]$. Заметим, что мы пока не пользовались тем фактом, что G — это группа, а не произвольный набор автоморфизмов.

Итак, допустим, что $n < [K : F]$. Поэтому в K можно выбрать $n+1$ линейно независимый над F элемент $\alpha_1, \ldots, \alpha_{n+1} \in K$. Снова составим систему:

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0; \\ &\cdots \\ \sigma_n(\alpha_1)x_1 + \cdots + \sigma_n(\alpha n + 1)x_{n+1} &= 0. \end{aligned}$$

Она имеет нетривиальное решение $\beta_1, \ldots, \beta_{n+1} \in K$. Среди всех нетривиальных решений системы выберем такое, у которого количество отличных от нуля компонент (обозначим его через r) минимально.

Заметим, что среди β_i есть элементы не из F: действительно, поскольку $\sigma_1 = 1$, то $\sigma_1\alpha_i = \alpha_i$, и если бы все β_i были из F, то из первого уравнения следовала бы линейная зависимость α_i над F. Будем считать, что $\beta_1 \neq F$. Далее, будем считать, что первые r чисел $\beta_1, \ldots, \beta_r$ отличны от 0. Кроме того, домножив их все на подходящее число, можно сделать $\beta_r = 1$. Тогда система примет вид

$$\begin{aligned} \sigma_1(\alpha_1)\beta_1 + \cdots + \sigma_1(\alpha_{r-1})\beta_{r-1} + \sigma_1(\alpha_r) &= 0; \\ &\cdots \\ \sigma_n(\alpha_1)\beta_1 + \cdots + \sigma_n(\alpha_{r-1})\beta_{r-1} + \sigma_n(\alpha_r) &= 0, \end{aligned}$$

или, что то же самое,

$$\sigma_i(\alpha_1)\beta_1 + \cdots + \sigma_i(\alpha_{r-1})\beta_{r-1} + \sigma_i(\alpha_r) = 0. \qquad (**)$$

Существует такой автоморфизм $\tilde{\sigma}$, что $\tilde{\sigma}\beta_1 \neq \beta_1$. Применив $\tilde{\sigma}$ к $(**)$, получим систему уравнений вида

$$\tilde{\sigma}\sigma_i(\alpha_1)\tilde{\sigma}(\beta_1) + \cdots + \tilde{\sigma}\sigma_i(\alpha_{r-1})\tilde{\sigma}(\beta_{r-1}) + \tilde{\sigma}\sigma_i(\alpha_r) = 0.$$

Мы подействовали на G левым сдвигом на $\tilde{\sigma}$. Поэтому множества $\{\sigma_1, \ldots, \sigma_n\}$ и $\{\tilde{\sigma}\sigma_1, \ldots, \tilde{\sigma}\sigma_n\}$ совпадают. Значит, последнюю систему уравнений можно переписать (поменяв порядок уравнений) как

$$\sigma_i(\alpha_1)\tilde{\sigma}(\beta_1) + \cdots + \sigma_i(\alpha_{r-1})\tilde{\sigma}(\beta_{r-1}) + \sigma_i(\alpha_r) = 0.$$

Вычтя из неё $(**)$, получим систему

$$\sigma_i(\alpha_1)[\tilde{\sigma}(\beta_1) - \beta_1] + \cdots + \sigma_i(\alpha_{r-1})[\tilde{\sigma}(\beta_{r-1}) - \beta_{r-1}] = 0.$$

Мы получили нетривиальное решение исходной системы (поскольку $\tilde{\sigma}(\beta_1) \neq \beta_1$), у которого имеется не более $r-1$ ненулевой компоненты. Это противоречит минимальности r.

Значит, $|G| = [K : F]$. Теорема доказана.

□

5. Лекция 5

В этой лекции мы докажем основную теорему теории Галуа. Для этого сначала выведем несколько следствий из теоремы 4.14.

5.1. Три следствия из теоремы 4.14.

Следствие 5.1. *Пусть K/F — конечное расширение. Тогда $|\operatorname{Aut}(K/F)| \leq [K:F]$.*

Доказательство. Пусть F_1 — неподвижное поле группы $\operatorname{Aut}(K/F)$. Тогда $F_1 \supset F$. По теореме 4.14 $|\operatorname{Aut}(K/F)| = [K:F_1] = [K:F]/[F_1:F] \leq [K:F]$. □

Следствие 5.2. *Пусть G — конечная группа автоморфизмов поля K, и $F = K^G$. Тогда всякий автоморфизм поля K, оставляющий F на месте, содержится в G, т.е. $\operatorname{Aut}(K/F) = G$. В частности, отсюда вытекает, что K/F — расширение Галуа.*

Доказательство. По условию, подполе F неподвижно относительно G, то есть $G \subset \operatorname{Aut}(K/F)$, следовательно, $|G| \leq |\operatorname{Aut}(K/F)|$. Но по теореме 4.14 имеем равенство $|G| = [K:F]$, а по предыдущему следствию $|\operatorname{Aut}(K/F)| \leq [K:F]$. Получаем цепочку неравенств:

$$[K:F] = |G| \leq |\operatorname{Aut}(K/F)| \leq [K:F].$$

Значит, они все являются равенствами, откуда и следует требуемое утверждение. □

Следствие 5.3. *Пусть $G_1, G_2 \subset \operatorname{Aut}(K)$. Если $G_1 \neq G_2$, то $K^{G_1} \neq K^{G_2}$.*

Доказательство. Пусть $F_1 = K^{G_1}$, $F_2 = K^{G_2}$. Если $F_1 = F_2$, то поле F_1 неподвижно относительно G_2, и поэтому $G_2 \subset G_1$. Аналогично получаем, что $G_1 \subset G_2$. Поэтому $G_1 = G_2$. □

5.2. Нормальные сепарабельные расширения.

Предложение 5.4. *Пусть $f(x) \in F[x]$ — многочлен без кратных сомножителей, E — его поле разложения. Тогда E является расширением Галуа тогда и только тогда, когда $f(x)$ сепарабелен.*

Доказательство. Напомним (это теорема 2.15), что для любого изоморфизма $\varphi\colon F \to F'$ существует продолжающий его изоморфизм полей разложения многочленов f и $\varphi(f)$, обозначавшийся через $\sigma\colon E \to E'$.

Покажем по индукции по степени расширения $[E:F]$, что таких гомоморфизмов σ, продолжающих φ, не более чем $[E:F]$, причем равенство достигается тогда и только тогда, когда $f(x)$ сепарабелен.

База индукции очевидна: если $[E:F] = 1$, то $E = F$, и $\sigma = \varphi$.

Если $[E : F] > 1$, то у $f(x)$ существует неприводимый сомножитель $p(x)$. Пусть α — корень $p(x)$. Если σ — продолжение φ, то пусть $\tau = \sigma|_{F(\alpha)} \colon F(\alpha) \to E'$. Гомоморфизм τ однозначно задаётся своим действием на α. Ясно, что $\beta = \tau\alpha$ — корень многочлена $p'(x) = \varphi(p(x))$. Поэтому число способов продолжить φ до $\tau \colon F(\alpha) \to F'(\beta)$ не превосходит $\deg p(x) = [F(\alpha) : F]$, причем равняется ему, если $p(x)$ сепарабелен. Теперь можно применить предположение индукции к продолжению гомоморфизма $\tau \colon F(\alpha) \to F'(\beta)$ до гомоморфизма $\sigma \colon E \to E'$. Число этих продолжений, согласно предположению индукции, не превосходит $[E : F(\alpha)]$.

Для завершения доказательства осталось заметить, что $[E : F] = [E : F(\alpha)][F(\alpha) : F]$. Поэтому число продолжений φ до σ, т.е. элементов $\mathrm{Aut}(E/F)$, равняется $[E : F]$ в точности тогда, когда $f(x)$ сепарабелен. □

Следствие 5.5. *Нормальное сепарабельное расширение является расширением Галуа.*

Оказывается, верно и обратное утверждение. Удобно сформулировать его вместе с предыдущим предложением, в форме “тогда и только тогда”.

Теорема 5.6. *Расширение K/F является расширением Галуа тогда и только тогда, когда K является полем разложения некоторого сепарабельного многочлена над F. Более того, каждый неприводимый многочлен с коэффициентами из F, имеющий корни в K, сепарабелен, и все его корни лежат в K.*

Доказательство. Часть “тогда” – это предложение 5.4.

Докажем часть “только тогда”. Сначала покажем, что если K/F — расширение Галуа, то каждый неприводимый многочлен $p(x) \in F[x]$ с корнем в K раскладывается над K на линейные множители. Пусть $G = \mathrm{Gal}(K/F)$

Пускай $\alpha \in K$ — корень $p(x)$; рассмотрим орбиту этого корня под действием группы Галуа: $G\alpha = \{\alpha_1, \ldots, \alpha_r\}$ (все элементы последнего множества различны). Ясно, что каждый элемент $\tau \in G$ как-то переставляет эти элементы. У многочлена $f(x) = (x - \alpha_1) \ldots (x - \alpha_r)$ коэффициенты (элементарные симметрические многочлены от $\alpha_1, \ldots, \alpha_r$) инвариантны относительно G, поэтому они принадлежат полю F.

Поскольку $p(x)$ неприводим и имеет α корнем, то $p(x)$ — минимальный многочлен для α над полем F. Но α также является корнем многочлена $f(x) \in F[x]$. Поэтому $p(x)|f(x)$ в $F[x]$. Но, с другой стороны, все числа $\alpha_1, \ldots, \alpha_r$ — корни $p(x)$, поэтому $f(x)|p(x)$. Значит, $p(x) = f(x)$. Поэтому $p(x)$ сепарабелен, и все его корни лежат в K.

Далее, пусть K/F — расширение Галуа, и $\omega_1, \ldots, \omega_n$ — базис поля K над F. Пусть $p_i(x)$ — минимальный многочлен элемента ω_i. По доказанному выше, он сепарабелен, и все его корни лежат в K. Возьмём произведение этих многочленов: $f(x) = p_1(x) \ldots p_n(x)$. Пусть многочлен $g(x)$ получается из $f(x)$ вычёркиванием всех кратных множителей (т.е. это делитель $f(x)$ максимальной степени, свободный от квадратов). Многочлен $g(x)$ сепарабелен, его поле разложения содержит $\omega_1, \ldots, \omega_n$, то есть содержит K. С другой стороны, все корни этого многочлена лежат в K. Поэтому K и есть его поле разложения. □

Определение 5.7. Пусть K/F — расширение Галуа, $\sigma \in \mathrm{Gal}(K/F)$, $\alpha \in K$. Элементы α и $\sigma\alpha$ называют *сопряжёнными*. Если $E \subset K$, то $\sigma(E)$ — *сопряжённое к* E *подполе*.

В доказательстве предыдущей теоремы мы показали, что в расширении Галуа все корни неприводимого многочлена являются сопряжёнными (т.е. группа Галуа действует на корнях транзитивно).

Итак, у нас имеются четыре равносильных описания расширения Галуа. Расширение Галуа K/F — это:

(1) поле разложения сепарабельного многочлена с коэффициентами в F;
(2) расширение, в котором $K^{\mathrm{Aut}(K/F)}$ есть в точности F (т.е. не больше);
(3) расширение, для которого $|\mathrm{Aut}(K/F) = [K : F]$ (исходное определение);
(4) нормальное сепарабельное расширение.

5.3. **Доказательство основной теоремы теории Галуа.** Напомним формулировку основной теоремы (мы её уже приводили в предыдущей лекции):

Теорема 5.8 (Основная теорема теории Галуа)**.** *Пусть K/F — расширение Галуа. Тогда имеется биекция между подполями в K, содержащими F, и подгруппами в группе $G = \mathrm{Gal}(K/F)$. При этой биекции подполю E соответствует подгруппа $H = \mathrm{Aut}(K/E) \subset G$, а подгруппе $H \subset G$ — её неподвижное подполе $E = K^H$. Эта биекция обладает следующими свойствами:*

(1) *она обращает включения: $E_1 \subset E_2 \Leftrightarrow H_1 \supset H_2$;*
(2) *степень расширения $[K : E]$ равна порядку группы H, а степень расширения $[E : F]$ — индексу подгруппы $[G : H]$;*
(3) *расширение K/E является расширением Галуа, и $\mathrm{Gal}(K/E) = H$;*
(4) *расширение E/F является расширением Галуа тогда и только тогда, когда H нормальна в G; при этом $\mathrm{Gal}(E/F) = G/H$;*
(5) *Пересечению подполей $E_1 \cap E_2$ соответствует группа $\langle H_1, H_2 \rangle \subset G$, а композиту полей E_1E_2 — пересечение групп $H_1 \cap H_2$.*

Доказательство. Во-первых, по каждой подгруппе $H \subset G = \mathrm{Gal}(K/F)$ можно построить подполе $E = K^H \subset K$. Согласно следствию 5.3, это соответствие инъективно: разным группам отвечают разные подполя.

Далее, если K — поле разложения сепарабельного многочлена $f(x) \in F[x]$, то $f(x)$ можно рассматривать как элемент кольца $E[x]$ для любого поля $E \supset F$. Поэтому K также будет полем разложения многочлена $f(x)$ как многочлена с коэффициентами в E. Поэтому K/E всегда будет расширением Галуа (описание (1) из предыдущего пункта). Стало быть, E есть неподвижное поле группы $\mathrm{Aut}(K/E) \subset G$. Поэтому *любое* подполе в K, содержащее F, есть неподвижное поле для некоторой подгруппы $H \subset G$. Значит, соответствие Галуа — биекция.

Обращение включений (часть (1) теоремы) очевидно.

Далее, если $E = K^H$ — неподвижное поле подгруппы H, то $[K : E] = |H|$ (т.к. K/E — расширение Галуа), а $[K : F] = |G|$ (по той же причине), поэтому $[E : F] = [G : H]$. Отсюда получается (2).

(3) получается из следствия 5.2.

Пусть $E = K^H$ — неподвижное поле подгруппы H. Всякий автоморфизм $\sigma \in G$, ограниченный на E, определяет вложение $\sigma|_E \colon E \to \sigma(E) \subset K$. Обратно, пусть $\tau \colon E \tilde{\to} \tau E \subset \overline{F}$ — вложение E в алгебраическое замыкание поля F, содержащее K. Тогда $\tau(E) \subset K$. Действительно, если $\alpha \in E$ отвечает минимальный многочлен $m_{\alpha,F}(x) \in F[x]$, то элемент $\tau\alpha$ тоже является корнем этого многочлена, и по теореме 5.6 поле K содержит все эти корни. Поэтому K является полем разложения некоторого многочлена $f(x)$ над E, а также полем разложения многочлена $\tau f(x) = f(x)$. Согласно теореме о продолжении гомоморфизма, существует такой автоморфизм $\sigma \colon K \to K$ поля K, который продолжает изоморфизм $\tau \colon E \to \tau(E)$.

Если ограничения автоморфизмов σ и σ' на одно и то же вложение E совпадают, это значит, что $\sigma^{-1}\sigma' = 1$. Поэтому $\sigma^{-1}\sigma' \in H$, или, что то же самое, $\sigma' \in \sigma H$. Поэтому различные автоморфизмы поля K, оставляющие E неподвижным, взаимно однозначно отвечают смежным классам σH. Поэтому

$$|\,\mathrm{Emb}(E/F)| = [G : H] = [E : F],$$

где $\mathrm{Emb}(E/F)$ — множество *вложений* E в K, оставляющих F неподвижным.

Расширение E/F является расширением Галуа тогда и только тогда, когда $|\,\mathrm{Aut}(E/F) = [E : F]$. Это значит, что всякое вложение E в K есть *автоморфизм* поля E, то есть $\sigma(E) = E$ для любого $\sigma \in G$.

Если $\sigma \in G$, то подгруппа в G, оставляющая на месте подполе $\sigma(E)$, есть $\sigma H \sigma^{-1}$, то есть $\sigma(E) = K^{\sigma H \sigma^{-1}}$. Наоборот, если

$\sigma H \sigma^{-1} = H$, то $\sigma(E) = E$. Поэтому H нормальна тогда и только тогда, когда E/F есть расширение Галуа, и в этом случае $\mathrm{Gal}(E/F) = G/H$.

Упражнение 5.9. Докажите самостоятельно часть (5) теоремы.

□

6. Лекция 6

6.1. Композит расширений. Простые расширения.

Предложение 6.1 (о подъёме расширений Галуа)**.** *Пусть K/F — расширение Галуа, F'/F — произвольное расширение. Тогда KF'/F' — снова расширение Галуа, причем* $\mathrm{Gal}(K/K\cap F')\cong\mathrm{Gal}(KF'/F')$.

Доказательство. Пусть K/F — расширение Галуа. Тогда K является полем разложения некоторого многочлена $f(x)\in F[x]$. Этот же многочлен можно рассмотреть как многочлен с коэффициентами в F', и тогда его поле разложения над F' будет композитом KF' (т.к. оно содержит и K, и F'). Поэтому KF'/F' — расширение Галуа.

Поскольку K/F — расширение Галуа, всякое вложение K в поле KF', оставляющее на месте поле F, есть автоморфизм K. Поэтому корректно определен гомоморфизм ограничения $\varphi\colon\ \mathrm{Gal}(KF'/F')\to\mathrm{Gal}(K/F)$, переводящий σ в $\sigma|_K$. Ядро этого гомоморфизма тривиально: гомоморфизм из ядра оставляет на месте, с одной стороны, поле K, а с другой — F', т.к. он принадлежит $\mathrm{Gal}(KF'/F')$, а значит, и композит KF'. Значит, φ — вложение.

Обозначим его образ через $H\subset\mathrm{Gal}(K/F)$. Пусть K^H — отвечающее этой подгруппе поле. Докажем, что $K^H=K\cap F'$. Одно включение очевидно: каждый элемент из H оставляет F' неподвижным, поэтому $K^H\subset K\cap F'$.

С другой стороны, поле $K^H\cdot F'$ неподвижно относительно группы $\mathrm{Gal}(KF'/F')$, т.к. всякий автоморфизм $\sigma\in\mathrm{Gal}(KF'/F')$ оставляет на месте F' и действует на K^H ограничением $\sigma|_K\in H$. По основной теореме теории Галуа, $K^H\cdot F'=F'$, так что $K^H\subset F'$, откуда получается, что $K^H\cdot K\subset F'$. Значит, $K^H=K\cap F'$, поэтому $H=\mathrm{Gal}(K/K\cap F')$. □

Следствие 6.2. *Пусть K/F — расширение Галуа, F'/F — произвольное расширение. Тогда*

$$[KF':F]=\frac{[K:F]\cdot[F':F]}{[K\cap F':F]}.$$

Доказательство. Это напрямую следует из равенства $[KF':F']=[K:K\cap F']$ и предыдущего предложения. □

Упражнение 6.3. Приведите пример, показывающий, что предыдущее предложение может не иметь место, если K/F — не расширение Галуа.

7. Лекция 7

8. Лекция 8

Рассмотрим n-мерное аффинное пространство $\mathbb{A}^n = \mathbb{A}^n_K$ над полем K, которое мы определим как множество наборов $(x_1, \ldots, x_n)$, где $x_i \in K$. Мы будем изучать *аффинные алгебраические множества* — подмножества в $\mathbb{A}^n$, получаемые как множества решений систем полиномиальных уравнений $f_\alpha(x_1, x_2, \ldots, x_n) = 0$.

Пример 8.1. Окружность на плоскости является аффинным алгебраическим множеством (это множество решений уравнения $x^2 + y^2 - 1 = 0$), а график синусоиды таковым не является (почему, будет ясно чуть позже).

Вообще говоря, системам уравнений разрешается быть бесконечными. Однако оказывается, что всякая бесконечная система полиномиальных уравнений эквивалентна некоторой конечной системе. Это следует из *теоремы Гильберта о базисе.*

8.1. Нётеровы кольца, теорема Гильберта о базисе.

Напомним определение нётерова кольца:

Определение 8.2. Коммутативное кольцо A с 1 называется *нётеровым*, если выполнено любое из двух эквивалентных условий:

(1) всякий идеал в A порождается конечным числом элементов;
(2) В A не бывает бесконечно возрастающей цепочки вложенных идеалов $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n \subsetneq \ldots$. Иначе говоря, всякая возрастающая цепочка идеалов стабилизируется[1].

Упражнение 8.3. Докажите эквивалентность этих условий.

Пример 8.4. Всякое кольцо главных идеалов нётерово (в нём любой идеал порождён *одним* элементом).

Теорема 8.5 (Теорема Гильберта о базисе, Basissatz)**.** *Пусть A — нетерово кольцо. Тогда кольцо многочленов $A[x]$ тоже нетерово.*

Доказательство. Будем пользоваться первым определением нетеровости. Пусть $I \subset A[x]$ — идеал в кольце многочленов. Докажем, что он конечно порождён.

Рассмотрим множество всевозможных многочленов из I. Их старшие коэффициенты образуют идеал в A (почему?), который мы обозначим через L. Идеал L конечно порождён; выберем в нем какую-нибудь систему образующих $L = (a_1, \ldots, a_r)$. Для каждой из этих образующих возьмём многочлен $f_i = a_i x^{d_i} + \cdots \in I$ со старшим членом a_i. Пусть d_i — степень этого многочлена.

Выберем максимум этих степеней: $N = \max(d_i)$. Для каждого числа $d < N$ рассмотрим множество I_d всех многочленов из I степени не выше d. Их старшие коэффициенты снова образуют идеал

[1] По-английски это условие называется accending chain condition, сокращенно ACC.

в A, который мы обозначим через L_d. Обозначим его образующие через $b_{1,d}, \ldots, b_{r_d,d}$ и для каждой из этих образующих выберем в I_d многочлен с соответствующим старшим коэффициентом: $g_{i,d} = b_{i,d}x^d + \ldots$. Мы получим конечное множество многочленов $g_{i,d}$, где $d < N$.

По построению, все многочлены f_i и $g_{i,d}$ лежат в идеале I. Породим ими идеал $I' \subset I$. Докажем, что это включение на самом деле является равенством. Преположим противное и возьмём многочлен $h \in I \setminus I'$ минимальной степени. Пусть $h = ax^m + \ldots$.

Возможны два случая, в зависимости от степени h. Первый случай: пусть $\deg h \geq N$. Старший коэффициент a многочлена h лежит в L по построению, и при этом $\deg h$ не меньше степеней всех образующих f_i. Тогда найдётся такой многочлен $f \in I'$ такой же степени и с таким же старшим коэффициентом, как h. Поэтому их разность $h - f$ будет лежать в I, но не в I', и будет иметь меньшую степень. Противоречие.

Если же $\deg h < N$, то $h \in I_d$ для некоторого d, а значит, найдётся такой многочлен g, являющийся линейной комбинацией $g_{i,d}$ (т.е. лежащий в I'), который имеет ту же степень и тот же старший член, что h. Снова получаем противоречие с минимальностью степени многочлена h. □

Следствие 8.6. *Кольцо многочленов от конечного числа переменных нетерово.*

Следствие 8.7. *Всякая бесконечная система алгебраических уравнений эквивалентна некоторой конечной системе.*

Доказательство. Породим уравнениями первой системы идеал и выберем в нём конечный базис. □

Замечание 8.8. Теорема Гильберта о базисе утверждает, что базис идеала существует, но не даёт никакого способа его найти. Явное алгоритмическое нахождение такого базиса является предметом теории базисов Грёбнера.

8.2. **Топология Зарисского.** Введём в пространстве $\mathbb{A}^n$ топологию, определив замкнутые подмножества.

Определение 8.9. Множество общих нулей $X \subset \mathbb{A}^n$ системы полиномиальных уравнений $f_i(x_1, \ldots, x_n) = 0$ называется *замкнутым в топологии Зарисского.*

По определению, открытые множества — это дополнения до замкнутых.

Пример 8.10. Замкнутые по Зарисскому подмножества прямой $\mathbb{A}^1$ — это пустое множество, вся прямая и всевозможные *конечные* наборы точек.

Убедимся, что это действительно определяет топологию. В самом деле, справедливо следующее

Предложение 8.11. *Объединение конечного числа замкнутых множеств замкнуто; пересечение любого числа замкнутых множеств замкнуто.*

Доказательство. Пересечение замкнутых множеств соответствует объединению систем уравнений, определяющих эти множества. С объединением дело обстоит немногим сложнее: если X задаётся системой уравнений $\{f_\alpha = 0\}$, а Y — системой $\{g_\beta = 0\}$, то их объединение есть множество нулей системы $\{f_\alpha g_\beta = 0\}$. □

8.3. **Теорема Гильберта о нулях, слабая форма.** Пусть у нас имеется некоторая система уравнений $\{f_\alpha = 0\}$. Когда она вообще имеет решение? И, наоборот, когда решений нет? Сразу можно указать ответ на второй вопрос: когда идеал (f_α) содержит единицу, т.е. если при помощи алгебраических комбинаций уравнений системы можно получить уравнение $1 = 0$, то система, очевидно, неразрешима. Теорема Гильберта о нулях (вернее, её слабая форма) утверждает, что если основное поле алгебраически замкнуто, то это необходимое условие является также и достаточным.

Теорема 8.12 (Теорема Гильберта о нулях, слабая форма)**.** *Пусть поле K алгебраически замкнуто. Система полиномиальных уравнений $\{f_\alpha(x_1, \dots, x_n) = 0\}$ не имеет общих решений тогда и только тогда, когда идеал $(f_alpha) \subset K[x_1, \dots, x_n]$ совпадает со всем кольцом, или, что то же самое, найдутся такие $f_1, \dots, f_m$ из системы уравнений и такие многочлены $g_1, \dots, g_m \in K[x_1, \dots, x_n]$, что*

$$f_1 g_1 + \dots + f_m g_m = 1.$$

Доказательство этой теоремы будет приведено в следующей лекции.

Замечание 8.13. Над алгебраически незамкнутым полем теорема, очевидно, неверна: так, идеал $(x^2 + 1) \subset \mathbb{R}[x]$ не совпадает со всем кольцом, но соответствующее уравнение не имеет корней.

Пусть $\xi = (\xi_1, \dots, \xi_n) \in \mathbb{A}^n$ — произвольная точка. Рассмотрим идеал функций, обращающихся в ней в нуль. Тогда $\mathfrak{m}_\xi = (x_1 - \xi_1, \dots, x_n - \xi_n)$ Очевидно, этот идеал максимален: $K[x_1, \dots, x_n]/\mathfrak{m}_\xi \cong K$, причём изоморфизм задаётся вычислением полинома в данной точке (его ядро — это те полиномы, которые в ней равны нулю). Оказывается, других максимальных идеалов нет.

Предложение 8.14. *Всякий максимальный идеал в кольце многочленов над алгебраически замкнутым полем имеет вид $\mathfrak{m}_\xi$ для некоторой точки ξ.*

Доказательство. Рассмотрим произвольный максимальный идеал $\mathfrak{m} \subset K[x_1, \dots, x_n]$. Он отличен от всего кольца, т.е. не содержит единицу. Поэтому, согласно теореме Гильберта о нулях, существуют такие точки, где все многочлены из этого идеала обращаются в нуль. Поскольку идеал максимален, то такая точка только одна (иначе бы $\mathfrak{m}$ содержался бы собственным образом в идеале $\mathfrak{m}_\xi$ для каждой из этих точек, что противоречит максимальности). $\square$

8.4. **Соответствие между идеалами и их множествами нулей.** Пусть $X \subset \mathbb{A}^n$ — замкнутое по Зарисскому множество. Ему можно сопоставить идеал функций $I(X) \subset K[x_1, \dots, x_n]$, обращающихся в нуль на X.

Обратно, если у нас имеется идеал $I \subset K[x_1, \dots, x_n]$, ему соответствует замкнутое по Зарисскому множество точек $V(I) \subset \mathbb{A}^n$, где все функции из этого идеала обращаются в нуль. По слабой теореме Гильберта о нулях, для собственного идеала это множество будет непустым.

Таким образом, имеются два отображения: из идеалов в замкнутые множества и обратно. У этих отображений существует две композиции (в разном порядке). Рассмотрим их подробнее.

Что получится, если начать с множества X, сопоставить ему идеал $I(X)$, а потом по нему построить множество $V(I(X))$? Оказывается, получится само X. Это тавтология: идеал $I(X)$ состоит из функций, равных нулю на X, а множество точек, где все эти функции равны нулю, есть $V(I(X))$.

Теперь рассмотрим отображение из идеалов в идеалы, задаваемое композицией этих двух отображений в другом порядке: т.е. идеалу I сопоставляется идеал $I(V(I))$. С одной стороны, ясно, что $I \subset I(V(I))$. Однако несложно построить пример, когда это включение строгое.

Пример 8.15. Пусть $I = (x^n) \subset K[x]$. Тогда $V(I) = \{0\}$, и $I(V(I)) = (x)$.

То есть соответствия $I \mapsto V(I)$ и $X \to I(X)$ не биективны. (Вернее, первое из них не инъективно, а второе не сюръективно). Оказывается, их можно сделать биекциями, сузив множество рассматриваемых идеалов.

Определение 8.16. *Радикал* идеала $I \subset A$ в кольце A — это идеал $r(I) = \{f \in A \mid f^n \in I\}$, состоящий из всех элементов, некоторая степень которых содержится в I. Идеал называется *радикальным*, если $r(I) = I$.

Упражнение 8.17. Проверьте, что $r(I)$ действительно является идеалом, а при каноническом эпиморфизме $A \to A/I$ идеал $r(I)$ переходит в нильрадикал кольца A/I (т.е. в идеал всех нильпотентных элементов этого кольца). Соответственно, идеал I радикален тогда и только тогда, когда A/I не содержит нильпотентов.

Упражнение 8.18. Проверьте, что $r(r(I)) = r(I)$.

Сильная форма теоремы Гильберта о нулях утверждает, что соответствие между замкнутыми по Зарисскому подмножествами в $\mathbb{A}^n$ и *радикальными* идеалами в кольце $K[x_1, \ldots, x_n]$ является биекцией.

Теорема 8.19 (Теорема Гильберта о нулях, сильная форма)**.** *Если $I \subset K[x_1, \ldots, x_n]$ — идеал, то $I(V(I)) = r(I)$. Более подробно, если многочлен f обращается в нуль на множестве общих нулей системы $h_1 = \cdots = h_m = 0$, то найдётся такое натуральное число k и многочлены $g_1, \ldots, g_m$, что*

$$g_1 h_1 + \cdots + g_m h_m = f^k.$$

Эту теорему мы также докажем (вернее, выведем из слабой теоремы Гильберта о нулях) в следующей лекции.