АЛГЕБРА, ТРЕТИЙ СЕМЕСТР

ЛЕКЦИЯ 1

Расширения полей

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 $\alpha_1, \dots, \alpha_m$ — базис L над K, а $\beta_1, \dots, \beta_n$ — базис K над F. Тогда всякий элемент из L представи́м в виде

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

Далее, каждый из a_i раскладывается по базису из β_j:

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

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. $[L : F] \le mn$.

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 $a_1\alpha_1 + \dots + a_m\alpha_m = 0$. Значит, все $a_i = 0$, т.к. α_i — базис L над K. Поэтому при любом i имеется равенство $b_{i1}\beta_1 + \dots + b_{in}\beta_n = 0$. 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 $p(x)$. $\square$

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. $\sigma|_F = \varphi$).*

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 $\alpha_1, \dots, \alpha_n$, что $K = F(\alpha_1; \dots, \alpha_n)$.

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.

Конечно порожденные 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. □