

ЛЕКЦИЯ 13

Теорема 1. Пусть F – поле. Кольцо $F[x]/(f)$ является полем тогда и только тогда, когда многочлен f неприводим.

Доказательство. Ясно, что $F[x]/(f)$ – коммутативное ассоциативное кольцо с единицей.

Если $f(x) = g(x)h(x)$, где $g(x)$ и $h(x)$ меньшей степени, то $g + (f) \neq 0 + (f)$, $h + (f) \neq 0 + (f)$, но $(g + (f)) \cdot (h + (f)) = 0 + (f)$. То есть в факторкольце есть делители нуля. Значит, это не поле.

Пусть теперь f неприводим и $g(x)$ не делится на $f(x)$, что эквивалентно тому, что $g(x) + (f(x)) \neq 0$. Найдем обратный к элементу $g + (f)$. Заметим, что $\text{НОД}(f, g) = 1$. Следовательно, существуют $u(x)$ и $v(x)$ такие, что $u(x)f(x) + v(x)g(x) = 1$. В факторкольце имеем $(u + (f))(f + (f)) + (v + (f))(g + (f)) = 1 + (f)$. Но $f + (f) = 0 + (f)$. Отсюда $(v + (f))(g + (f)) = 1 + (f)$. \square

Заметим, что $F[x]/(f)$ – алгебра над F .

Лемма 1. Базис этой алгебры $\{1 + (f), x + (f), \dots, x^{n-1} + (f)\}$, где $n = \deg f$.

Доказательство. Пусть $g(x) \in F[x]$. Поделим g на f с остатком: $g(x) = q(x)f(x) + r(x)$. Тогда $g + (f) = r + (f)$. Но $\deg r(x) \leq n-1$. Значит, $r(x)$ является линейной комбинацией $1, x, \dots, x^{n-1}$. Мы доказали, что $\{1 + (f), x + (f), \dots, x^{n-1} + (f)\}$ – полная система.

Докажем линейную независимость. Пусть $\sum_{i=0}^{n-1} \alpha_i(x^i + (f)) = 0$. Положим $h(x) = \sum_{i=0}^{n-1} \alpha_i x^i$. Тогда $h + (f) = 0 + (f)$. Это значит, что $h \in (f)$, то есть h делится на f , чего не может быть, так как $\deg h(x) < \deg f(x)$. \square

Замечание 1. Если мы имеем алгебру A размерности n над полем \mathbb{Z}_p , то $|A| = p^n$. В самом деле, пусть $\{e_1, \dots, e_n\}$ – базис A . Тогда $A = \{\lambda_1 e_1 + \dots + \lambda_n e_n \mid \lambda_i \in \mathbb{Z}_p\}$. Каждый коэффициент λ_i принимает p значений. Значит, всего p^n вариантов.

Пример 1. Рассмотрим многочлен $f(x) = x^2 + x + 1$ в кольце $\mathbb{Z}_2[x]$. Проверим, что у $f(x)$ нет корней в \mathbb{Z}_2 . Действительно, $f(0) = 1$, $f(1) = 1$. Так как f – многочлен второй степени и у него нет корней, он неприводим. Значит, кольцо $\mathbb{Z}_2[x]/(x^2 + x + 1)$ является полем из 4 элементов. Построим таблицы сложения и умножения.

+	0	1	x	x+1	·	0	1	x	x+1
0	0	1	x	x+1	0	0	0	0	0
1	1	0	x+1	x	1	0	1	x	x+1
x	x	x+1	0	1	x	0	x	x+1	1
x+1	x+1	x	1	0	x+1	0	x+1	1	x

Например, $(x + (f)) \cdot (x + (f)) = x^2 + (f) = x + 1 + (f)$.

Определение 1. Пусть F – поле. Характеристика поля F – это минимальное натуральное n такое, что сумма n единиц равна нулю $1 + 1 + \dots + 1 = 0$. Если такого n не существует, характеристика поля равна нулю. Обозначается характеристика через $\text{char } F$.

Пример 2. 1) $\text{char } \mathbb{R} = \text{char } \mathbb{C} = \text{char } \mathbb{Q} = 0$.

2) $\text{char } \mathbb{Z}_p = p$.

3) $\text{char } \mathbb{Z}_p[x]/(f) = p$.

Лемма 2. Характеристика поля – либо ноль, либо простое число.

Доказательство. Допустим, что характеристика поля F равна lm .

$$0 = \underbrace{1 + 1 + \dots + 1}_{lm \text{ раз}} = \underbrace{(1 + \dots + 1)}_{l \text{ раз}} \underbrace{(1 + \dots + 1)}_{m \text{ раз}}.$$

Так как в поле нет делителей нуля, одна из скобок равна 0. \square

Определение 2. Простое поле – это поле, в котором нет собственных подполей. (Мы считаем, что в поле $0 \neq 1$, а значит, $\{0\}$ – не подполе.)

Предложение 1. В каждом поле F есть простое подполе. Если $\text{char } F = 0$, то оно изоморфно \mathbb{Q} . Если же $\text{char } F = p$, то оно изоморфно \mathbb{Z}_p .

Доказательство. 1) Пусть $\text{char } F = p$, рассмотрим

$$K = \{0, 1, 1 + 1, 1 + 1 + 1, \dots, \underbrace{1 + 1 + \dots + 1}_{(p-1) \text{ раз}}\}$$

Тогда K – подполе в F , изоморфное \mathbb{Z}_p .

2) Пусть $\text{char } F = 0$. Рассмотрим $L = \{0, 1, -1, 1 + 1, -(1 + 1), \dots\}$. Тогда L – подкольцо в F , изоморфное \mathbb{Z} . Рассмотрим отношения всех элементов из L , такие, что знаменатель не ноль. Получим подполе K , изоморфное \mathbb{Q} . \square

Следствие 1. Количество элементов в конечном поле является степенью простого числа (равного характеристике данного поля).

Доказательство. Если поле F конечно, то его характеристика не равна нулю. Значит, в нем содержится простое подполе $E \cong \mathbb{Z}_p$. Тогда F – векторное пространство над E . Так как $|F| < \infty$, то и $\dim_E F < \infty$. Пусть $\dim_E F = n$. Тогда $|F| = p^n$. \square

Пусть $\text{char } F = p$. Рассмотрим следующее отображение $\varphi: F \rightarrow F$, $\varphi(x) = x^p$.

Предложение 2. Отображение φ является инъективным гомоморфизмом.

Доказательство. Очевидно, что $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$. Проверим сохранение сложения: $\varphi(a + b) = (a + b)^p = \sum_{i=0}^p C_p^i a^i b^{p-i}$. Так как число p простое, биномиальный коэффициент $C_p^i = \frac{p!}{i!(p-i)!}$ делится на p при $i \notin \{0, p\}$. Так как характеристика поля F равна p , в поле F коэффициент C_p^i равен 0. Значит, в F выполнено $(a + b)^p = a^p + b^p$.

Итак, φ – гомоморфизм. При этом $\text{Ker } \varphi = \{0\}$, поскольку из $a^p = 0$ следует $a = 0$. (В поле нет делителей нуля.) \square

Определение 3. При $|F| < \infty$, φ – автоморфизм. В самом деле, в случае $|F| < \infty$ из того, что φ – инъекция следует, что φ – сюръекция. Этот автоморфизм называется *автоморфизмом Фробениуса*. Если $|F| = \infty$, то φ может быть не сюръективен.

Заметим, что гомоморфизм из поля в какое-либо кольцо либо нулевой, либо вложение (так как в поле нет нетривиальных идеалов). Значит, изучение гомоморфизмов между полями сводится к изучению вложений.

Определение 4. Пусть E – подполе поля F . Тогда поле F называется *расширением* поля E .

Определение 5. Элемент $a \in F$ называется *алгебраическим* над E , если существует ненулевой многочлен $h(x)$ с коэффициентами из E такой, что $h(a) = 0$.

Иначе элемент a называется *трансцендентным* над E .

Определение 6. Расширение полей $E \subset F$ называется *алгебраическим*, если любой элемент $a \in F$ является алгебраическим над E .

Расширение полей $E \subset F$ конечным, если $\dim_E F < \infty$.

Предложение 3. Конечное расширение алгебраическое.

Доказательство. Пусть $a \in F$ и $\dim_E F = n$. Тогда элементы $1, a, a^2, \dots, a^n$ линейно зависимы над E . Значит, существуют $c_0, c_1, \dots, c_n \in E$ такие, что $c_0 + c_1 a + c_2 a^2 + \dots + c_n a^n = 0$, то есть a алгебраический над E . \square

Для любого алгебраического элемента a можно определить минимальный многочлен $f_{min}(x)$ такой, что это многочлен минимальной степени с коэффициентами из E , для которого верно $f_{min}(a) = 0$. Легко показать, что f_{min} неприводим над E и любой многочлен $h(x)$, для которого $h(a) = 0$ делится на f_{min} . Отсюда следует, что f_{min} определен однозначно с точностью до пропорциональности.

Теорема 2 (Теорема о башне расширений). Пусть $E \subset F$ и $F \subset K$ – конечные расширения полей, причем $\dim_E F = m$, $\dim_F K = n$. Тогда расширение $E \subset K$ также конечное и $\dim_E K = mn$.

Доказательство. Пусть $\{f_1, \dots, f_m\}$ – базис F над E и $\{k_1, \dots, k_n\}$ – базис K над F . Тогда для любого $k \in K$ выполнено $k = \sum \lambda_i k_i$, $\lambda_i \in F$. При этом $\lambda_i = \sum_{j=1}^m \mu_{ij} f_j$, $\mu_{ij} \in E$. Получается, что $k = \sum_{i,j} \mu_{ij} f_j k_i$. Таким образом, система $f_j k_i$ полная в K над E . Докажем линейную независимость. Пусть $\sum_{i,j} \mu_{ij} f_j k_i = 0$. Тогда $\sum_i (\sum_j \mu_{ij} f_j) k_i = 0$. Так как $\{k_1, \dots, k_n\}$ – базис K , имеем для каждого i : $\sum_j \mu_{ij} f_j = 0$. Значит, так как $\{f_1, \dots, f_m\}$ – базис F , получаем $\mu_{ij} = 0$ для всех i и j . \square

Определение 7. Пусть $E \subset F$ – расширение полей. Пусть S – некоторое подмножество F . Назовем минимальное подполе в F , содержащее E и S полем, порожденным S над E и будем обозначать $E(S)$.

Лемма 3. Поле $E(S)$ состоит из элементов $\frac{g(s_1, \dots, s_n)}{h(s_1, \dots, s_n)}$ для всех возможных конечных наборов s_1, \dots, s_n и многочленов $g, h \in E[y_1, \dots, y_n]$ с условием $h(s_1, \dots, s_n) \neq 0$.

Доказательство. Так как в поле $E(S)$ лежат все s_i и коэффициенты из E , и в этом поле можно складывать и умножать, значит, любой многочлен $g(s_1, \dots, s_n) \in E(S)$. Так как в этом поле можно делить, $\frac{g(s_1, \dots, s_n)}{h(s_1, \dots, s_n)} \in E(S)$. С другой стороны, множество дробей $\frac{g(s_1, \dots, s_n)}{h(s_1, \dots, s_n)}$ замкнуто относительно сложения, умножения, взятия противоположного и обратного к ненулевому элементу. Значит, это подполе. \square

Лемма 4. Пусть элемент $a \in F$ алгебраический над $E \subset F$ причем $\deg f_{min} = n$. Тогда $E(a) = \{P(a) \mid \deg P < \deg f_{min}\}$. В частности расширение $E \subset E(a)$ конечное степени n .

Доказательство. Рассмотрим $\frac{g(a)}{h(a)} \in E(a)$. Так как $h(a) \neq 0$, $h(x)$ не делится на $f_{min}(x)$. Значит, так как f_{min} неприводим, НОД(h, f_{min}) = 1, то есть существуют $u(x)$ и $v(x)$ такие, что $uh + vf_{min} = 1$. Домножим числитель $\frac{g(x)}{h(x)}$ на 1:

$$\frac{g(x)}{h(x)} = \frac{g(uh + vf_{min})}{h} = gu + \frac{gvf_{min}}{h}.$$

Теперь подставим сюда $x = a$, учитывая $f_{min}(a) = 0$, получаем $\frac{g(a)}{h(a)} = g(a)u(a) = Q(a)$. Далее поделим $Q(x)$ на $f_{min}(x)$ с остатком: $Q(x) = q(x)f_{min}(x) + P(x)$, $\deg P < n$. Подставляя a , получаем $Q(a) = P(a)$. \square

Следствие 2. Поле, порожденное конечным числом алгебраических элементов дает конечное расширение.

Доказательство. В цепочке $E \subset E(a_1) \subset E(a_1, a_2) \subset \dots \subset E(a_1, \dots, a_n)$ все расширения конечны. Значит, и $E \subset E(a_1, \dots, a_n)$ конечно. \square

Предложение 4. Пусть $f(y) \in F[y]$ – неразложимый многочлен. Обозначим

$$\alpha = y + (f) \in F[y]/(f).$$

Тогда $F[y]/(f) = F(\alpha)$, причем α – это корень $f(x)$, рассматриваемого как многочлен из $F(\alpha)[x]$.

Доказательство. Очевидно, что α лежит в $F[y]/(f)$. Значит, $F(\alpha) \subseteq F[y]/(f)$. С другой стороны $F[y]/(f) = \{g(y) + (f)\} = \{g(\alpha)\}$. Это показывает обратное включение.

Элемент α алгебраический над F так как $f(\alpha) = f(y) + (f) = 0$. Так как f неприводим, это минимальный многочлен α . Значит, $F(\alpha) = F[\alpha] = F[y]/(f)$. \square

Определение 8. Расширение $F[x]/(f)$ называется *присоединением корня* многочлена f к полю F .