Лекция 13

Определение 1. Пусть R – область целостности, не являющаяся полем. Тогда R называется *евклидовым кольцом*, если задана функция (*евклидова норма*)

$$N\colon R \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

такая, что

1) $N(ab) \geq N(a)$ для любых $a, b \in R \setminus \{0\}$;

2) для любых $a, b \in R$, $b \neq 0$ возможно "деление с остатком", то есть существуют такие $q, r \in R$, что $a = bq + r$, причем либо $N(r) < N(b)$, либо $r = 0$.

Пример 1. *1)* $R = \mathbb{Z}$, $N(a) = |a|$.

2) $R = F[x]$, $N(f) = \deg f$.

3) **Задача.** *Докажите, что* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ *– евклидово кольцо с нормой* $N(z) = |z|$.

4) **Задача.** *Для каких* $c \in \mathbb{R}$ *кольцо* $\mathbb{Z}[ci] = \{a + bci \mid a, b \in \mathbb{Z}\}$ *является евклидовым кольцом с нормой* $N(z) = |z|$*?*

Определение 2. Область целостности R назовем *кольцом главных идеалов*, если любой идеал в нем главный, то есть равен (r) для некоторого $r \in R$.

Пример 2. *Идеал* (x, y) *в* $F[x, y]$ *не является главным. Действительно, если* $(x, y) = (f)$*, то* f *делит и* x *и* y*. Тогда* f *– константа и* $(f) = F[x, y]$.

Теорема 1. *Евсклидово кольцо является кольцом главных идеалов.*

Доказательство. Пусть R – евклидово кольцо с нормой N. И пусть $I \triangleleft R$. Если $I \neq \{0\}$, рассмотрим ненулевой элемент $a \in I$ с минимальной нормой. Пусть $b \in I$. Тогда $b = aq + r$. Предположим, что $r \neq 0$. Получаем $r \in I$, $N(r) < N(a)$. Противоречие с выбором a. Значит, $r = 0$, то есть $b \in (a)$. Следовательно, $I = (a)$. □

Определение 3. Пусть a и b – два элемента кольца главных идеалов. Рассмотрим $(a, b) = (d)$. Назовем d *наибольшим общим делителем* a и b. (НОД определен с точностью до обратимого множителя.)

Имеем $d \mid a$, $d \mid b$, $d = ua + vb$.

Определение 4. 1) Пусть R – область целостности. Необратимый элемент $r \in R$ называется *неприводимым*, если из $ab = r$ следует, что либо a, либо b обратим.

2) Два элемента $u, v \in R$ называются *ассоциированными*, если $u = cv$, где c – обратимый элемент.

3) Кольцо R называется *факториальным*, если любой элемент раскладывается в произведение неприводимых единственным способом с точностью до порядка и ассоциированности сомножителей.

Лемма 1. *Пусть* R *– кольцо главных идеалов,* p *– неприводимый элемент. Допустим, что* $p \mid ab$*. Тогда либо* $p \mid a$*, либо* $p \mid b$.

Доказательство. Пусть $s = \text{НОД}(a, p)$. Тогда $s \mid p$. Значит, либо s ассоциирован с p, либо с 1. Если $s = p$, то $p \mid a$. Если же $s = 1$, то существуют $u, v \in R$ такие, что $ua + vp = 1$. Домножим это равенство на b. Получим $uab + vpb = b$. Левая часть делится на p. Значит, и правая часть делится на p. □

Следствие 1. *Пусть R – кольцо главных идеалов, p – неприводимый элемент. Допустим, что $p \mid a_1 a_2 \dots a_k$. Тогда найдется j такой, что $p \mid a_j$.*

Теорема 2. *Кольцо главных идеалов факториально.*

Доказательство. **Существование.** Пусть R – кольцо главных идеалов и $a \in R$. Если a не является неприводимым, то $a = bc$ для некоторых необратимых b и c. Тогда имеем $(a) \subsetneq (b)$ и $(a) \subsetneq (c)$. Если оба множителя неприводимы, то получено разложение. Иначе какой-то из них снова можно разложить, что даст увеличение идеала и т.д. Если разложения так и не будет, получим бесконечно возрастающую цепочку $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \dots$

Рассмотрим $I = \cup(a_i)$. Легко видеть, что I – идеал. Значит, $I = (b)$. Но $b \in \cup(a_i)$, значит, найдется j такой, что $b \in (a_j)$. Тогда $I = (a_j)$. То есть бесконечно возрастающих цепочек не может быть.

Единственность. Пусть $a = p_1 \dots p_k = q_1 \dots q_m$ – два разложения на неприводимые. Тогда $p_1 \mid q_1 \dots q_m$. Значит, существует j такое, что $p_1 \mid q_j$. Так как p_1 и q_j неприводимы, они ассоциированы. Значит, перебрасывая обратимый элемент в другой множитель и меняя нумерацию, можно считать $p_1 = q_1$.

$$p_1 p_2 \dots p_k = p_1 q_2 \dots q_m.$$

Перенесем все в одну часть.

$$p_1(p_2 \dots p_k - q_2 \dots q_m) = 0.$$

Так как $p_1 \neq 0$ и в R нет делителей нуля, получаем $p_2 \dots p_k = q_2 \dots q_m$ и т.д. □

Теорема 3. *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 степни, 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 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 $(v + (f))(g + (f)) = 1 + (f)$. □

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

Лемма 2. *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 $\deg h(x) < \deg f(x)$. □

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 3. *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	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$\mathbf{x+1}$	$\mathbf{1}$
$x+1$	0	$x+1$	$\mathbf{1}$	$\mathbf{x}$

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

Определение 5. Пусть F – поле. *Характеристика* поля F – это минимальное натуральное n такое, что сумма n единиц равна нулю $1 + 1 + \ldots + 1 = 0$. Если такого n не существует, характеристика поля равна нулю. Обозначается характеристика через $\operatorname{char} F$.

Пример 4. *1)* $\operatorname{char}\mathbb{R} = \operatorname{char}\mathbb{C} = \operatorname{char}\mathbb{Q} = 0$.
2) $\operatorname{char}\mathbb{Z}_p = p$.
3) $\operatorname{char}\mathbb{Z}_p[x]/(f) = p$.

Лемма 3. *Характеристика поля – либо ноль, либо простое число.*

Доказательство. Допустим, что характеристика поля F равна lm.
$0 = \underbrace{1 + 1 + \ldots + 1}_{lm \text{ раз}} = \underbrace{(1 + \ldots + 1)}_{l \text{ раз}}\underbrace{(1 + \ldots + 1)}_{m \text{ раз}}$.
Так как в поле нет делителей нуля, одна из скобок равна 0. □

Определение 6. 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* $\operatorname{char} F = 0$, *то оно изоморфно* $\mathbb{Q}$. *Если же* $\operatorname{char} F = p$, *то оно изоморфно* $\mathbb{Z}_p$.

Доказательство. 1) Пусть $\operatorname{char} F = p$, рассмотрим
$K = \{0, 1, \underbrace{1 + 1, 1 + 1 + 1, \ldots, 1 + 1 + \ldots + 1}_{\text{(p-1) раз}}\}$
Тогда K – подполе в F, изоморфное $\mathbb{Z}_p$.
2) Пусть $\operatorname{char} F = 0$. Рассмотрим $L = \{0, 1, -1, 1 + 1, -(1 + 1), \ldots\}$. Тогда L – подкольцо в F, изоморфное $\mathbb{Z}$. Рассмотрим отношения всех элементов из L, такие, что знаменатель не ноль. Получим подполе K, изоморфное $\mathbb{Q}$. □

Следствие 2. *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 $|F| = p^n$. □

Пусть $\operatorname{char} F = p$. Рассмотрим следующее отображение $\varphi\colon F \to F$, $\varphi(x) = x^p$.

Предложение 2. *Отображение* φ *является иньективным 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 $\operatorname{Ker}\varphi = \{0\}$, поскольку из $a^p = 0$ следует $a = 0$. (В поле нет делителей нуля.) □

Определение 7. 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 гоморфизмов между полями сводится к изучению вложений.

Определение 8. Пусть E – подполе поля F. Тогда поле F называется *расширением* поля E.

Определение 9. 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 10. 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 $1, a, a^2, \ldots, a^n$ линейно зависимы над E. Значит, существуют $c_0, c_1, \ldots, c_n \in E$ такие, что $c_0 + c_1 a + c_2 a^2 + \ldots + c_n a^n = 0$, то есть a алгебраический над E. □

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 4 (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 $E \subset K$ такиже конечное и $\dim_E K = mn$.*

Доказательство. Пусть $\{f_1, \ldots, f_m\}$ – базис F над E и $\{k_1, \ldots, k_n\}$ – базис K над F. Тогда для любого $k \in K$ выполнено $k = \sum \lambda_i k_i$, $\lambda_i \in F$. При этом $\lambda_i = \sum_{j=1}^{n} \mu_{ij} f_j$, $\mu_{ij} \in E$. 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 $\sum_{ij} \mu_{ij} f_j k_i = 0$. Тогда $\sum_i (\sum_j \mu_{ij} f_j) k_i = 0$. Так как $\{k_1, \ldots, k_n\}$ – базис K, имеем для каждого i: $\sum_j \mu_{ij} f_j = 0$. Значит, так как $\{f_1, \ldots, f_m\}$ – базис F, получаем $\mu_{ij} = 0$ для всех i и j. □

Определение 11. 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 4. *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. □

Лемма 5. *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 $Q(a) = P(a)$. □

Следствие 3. *Поле, порожденное конечным числом алгебраических элементов дает конечное расширение.*

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

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, $F(\alpha) = F[\alpha] = F[y]/(f)$. □

Определение 12. Расширение $F[x]/(f)$ называется *присоединением корня* многочлена f к полю F.