Алгебраическая теория чисел
БФУ им. И.Канта – Малыгина Е.С.

Лекция №8

4 Факторизация и идеалы

4.1 Основные определения

Определения:

Пусть R – кольцо, $a \in R$.

Если существует элемент $b \in R$, такой, что $ab = 1$, то a и b называются *единицами* кольца R.

Элемент a называется *неприводимым*, если $a \neq 0$, не является единицей и условие $a = bc$ влечет, что либо b – единица, либо c – единица.

Элемент a называется *простым*, если $a \neq 0$, не является единицей и условие $a|bc$ влечет, что либо $a|b$, либо $a|c$.

Если $a = ub$, где u – единица, то элемент a называется *ассоциированным с* b: $a \sim b$.

Будем считать, что кольцо R является *кольцом с единственным разложением на множители*, если всякий $a \in R$, не являющийся единицей, можно записать как $a = \nu_1\nu_2...\nu_n$, где ν_i – неприводимые элементы, и $a = s_1...s_m$, где s_j – неприводимые элементы, тогда $n = m$.

Множество $\mathfrak{a} \subset R$ называется *идеалом* кольца R, если:

- $\mathfrak{a}$ – аддитивная абелева группа;
- $\alpha \cdot \mathfrak{a} \subseteq \mathfrak{a}$ для $\forall \alpha \in R$.

Идеал $\mathfrak{a}$ называется *главным идеалом*, если $\mathfrak{a} = (a) = aR = \{a \cdot r | r \in R\}$.

Кольцо R называется *кольцом главных идеалов*, если всякий идеал $\mathfrak{a} \subset R$ является главным.

Конечно порождённый идеал имеет вид $(\alpha_1, ..., \alpha_n) = \sum_{i=1}^{n} \beta_i \alpha_i$, $\beta_i \in R$.

Наибольшим общим делителем двух идеалов называется

$$\text{НОД}(\mathfrak{a}, \mathfrak{b}) = \{\alpha + \beta | \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\}.$$

$\text{НОД}(\mathfrak{a}, \mathfrak{b}) = 1$ тогда и только тогда, когда $\mathfrak{a} + \mathfrak{b} = (1) = R$.

Лемма 1. *Пусть K – числовое поле, тогда всякий идеал $\mathfrak{a}$ кольца O_K имеет вид: $\mathfrak{a} = (\alpha_1, ..., \alpha_n)$, где $\alpha_i \in O_K$.*

4.2 Свойства нётеровых колец

Теорема 1. *Пусть R – коммутативное кольцо (с единичным элементом). Следующие условия эквивалентны:*

1. *Любой идеал в R – конечно порождён.*
2. *$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq ... \subseteq \mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = ...$ До $\mathfrak{a}_n$ – вложенная цепочка, после – цепочка стабилизируется.*
3. *Любое непустое множество идеалов S содержит максимальный элемент.*

Определение 1. Кольцо, удовлетворяющее одному из условий теоремы выше, называется нётеровым.

Теорема 2. *Кольцо O_K – нётерово.*

4.3 Фактор-кольца

Определение 2. $O_K/\mathfrak{a} = \{x + \mathfrak{a} | x \in O_K\}$, $x + \mathfrak{a} = \overline{x} = [x]$.

При этом операции над классами идеалов определены следующим образом:

- $\overline{x} + \overline{y} = \overline{x + y}$
- $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$

Лемма 2. *Пусть $\mathfrak{a} \neq 0$ – идеал в O_K, $\alpha \neq 0$, $\alpha \in \mathfrak{a}$. Тогда $N_{K/\mathbb{Q}}(\alpha) \in \mathfrak{a}$.*

Теорема 3. *Пусть идеал $\mathfrak{a} \neq 0$, $\mathfrak{a} \subset O_K$. Тогда фактор-кольцо O_K/α – конечно.*

4.4 Простой и максимальный идеалы

Определение 3. Идеал $\mathfrak{p} \neq 0$, $\mathfrak{p} \subsetneqq O_K$ называется простым, если

$$\alpha \cdot \beta \in \mathfrak{p} \Rightarrow \begin{bmatrix} \alpha \in \mathfrak{p}, \\ \beta \in \mathfrak{p}. \end{bmatrix}$$

Определение 4. Идеал $\mathfrak{m} \neq 0$, $\mathfrak{m} \subsetneqq O_K$ называется максимальным, если $\nexists \mathfrak{a} \subset O_K : \mathfrak{m} \subsetneqq \mathfrak{a} \subsetneqq O_K$.

Замечание 1. $O_K/\mathfrak{p}$ – кольцо целостности; $O_K/\mathfrak{m}$ – поле.

Теорема 4. *Пусть K – числовое поле. Любой идеал из O_K будет максимальным тогда и только тогда, когда он является простым.*

4.5 Дробные идеалы

Определение 5. Дробным идеалом кольца O_K называется подмножество $\mathfrak{a}$, удовлетворяющее следующим условиям:

1. $\mathfrak{a}$ – аддитивная абелева группа.
2. $x\mathfrak{a} \subset \mathfrak{a}$, $\forall x \in O_K$.
3. $\exists y \neq 0$, $y \in O_K : y\mathfrak{a} = \mathfrak{b} \subset O_K$.

Замечание 2. Идеал из O_K является дробным. Но дробный идеал не всегда лежит в O_K.

Лемма 3. *Идеал $\mathfrak{a} \subset K$ является дробным идеало кольца O_K тогда и только тогда, когда $\mathfrak{a} = \frac{1}{\beta}\mathfrak{b}$, где $\mathfrak{b}$ – идеал в O_K, $\beta \neq 0$, $\beta \in O_K$.*

Лемма 4. *Пусть $\mathfrak{a} \neq 0$, $\mathfrak{a} \subset O_K$. Определим $\mathfrak{a}^{-1} = \{\beta \in K | \beta \cdot \mathfrak{a} \subset O_K\}$, $\beta \cdot \mathfrak{a}$ – целый. Тогда*

1. *$\mathfrak{a}^{-1}$ – дробный идеал.*
2. *$O_K \subset \mathfrak{a}^{-1}$.*
3. *$\mathfrak{a}^{-1} \cdot \mathfrak{a}$ – идеал в O_K.*

4.6 Деление и факторизация идеалов

Определение 6. Пусть $\mathfrak{a} \neq 0$, $\mathfrak{b} \neq 0$ – идеалы в O_K. Будем говорить, что идеал $\mathfrak{a}$ делит идеал $\mathfrak{b}$ и записывать $\mathfrak{a}|\mathfrak{b}$, если $\mathfrak{a} \supseteq \mathfrak{b}$.

Лемма 5. *Пусть $\mathfrak{a} \neq 0$, $\mathfrak{b} \neq 0$ – идеалы, $\mathfrak{p}$ – простой идеал и $\mathfrak{p}|\mathfrak{a}\mathfrak{b}$, тогда либо $\mathfrak{p}|\mathfrak{a}$, либо $\mathfrak{p}|\mathfrak{b}$.*

Лемма 6. *Пусть* $\mathfrak{a} \neq 0$ *– идеал в* O_K*. Тогда существуют простые идеалы* $\mathfrak{p}_1, ..., \mathfrak{p}_r$*, такие, что* $\mathfrak{a} | \mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_r$*.*

Следствие 1. *1. Пусть* $\mathfrak{a}$ *– ненулевой идеал,* $\mathfrak{p}$ *– простой идеал и* $\mathfrak{a} \subseteq \mathfrak{p}$*. Тогда* $\mathfrak{a} \subsetneqq \mathfrak{p}^{-1} \cdot \mathfrak{a} \subset O_K$*.*

2. $\mathfrak{p}^{-1} \cdot \mathfrak{p} = O_K$*.*

Теорема 5. *Пусть* K *– числовое поле,* $O_K \subset K$*. Любой ненулевой идеал* $\mathfrak{a}$ *имеет единственное разложение на множители* $\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i$*.*

Следствие 2. *1. Если* $\mathfrak{a} = \mathfrak{p}_1 ... \mathfrak{p}_n$*, то* $\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1} ... \mathfrak{p}_n^{-1} \Rightarrow \mathfrak{a} \cdot \mathfrak{a}^{-1} = (1) = O_K$*.*

2. Пусть $\mathfrak{a} \neq 0, \mathfrak{b} \neq 0$ *– идеалы в* O_K*. Пусть также* $\mathfrak{a} \supset \mathfrak{b}$ *(*$\mathfrak{a} | \mathfrak{b}$*). Тогда существует идеал* $\mathfrak{c} \subset O_K | \mathfrak{b} = \mathfrak{a}\mathfrak{c}$*.*