Алгебра 8
30.10.97

Идеалы

Часть 1. Дискриминант идеала.

Пусть F — числовое поле, т.е. конечное расширение $\mathbb{Q}$. Кольцо целых алгебраических чисел, содержащихся в F, будем обозначать $A = \mathcal{O}(F)$. Например, $\mathcal{O}(\mathbb{Q}(\sqrt{-3})) = \mathbb{Z}[\omega] = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, а $\mathcal{O}(\mathbb{Q}(\sqrt{-5})) = \mathbb{Z}[\sqrt{-5}]$. Поле F является полем частных своего кольца целых A: если $\alpha \in F$ удовлетворяет уравнению $a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0$ с целыми коэффициентами $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, то $a_0\alpha$ удовлетворяет уже унитарному уравнению с целыми коэффициентами.

Если $I \subset A$ — идеал, то можно выбрать базис поля F над $\mathbb{Q}$ из элементов $\beta_1, \ldots, \beta_n$, лежащих в I. В самом деле, пусть $\alpha_1, \ldots, \alpha_n$ — какой-то базис $F : \mathbb{Q}$. Возьмем какое-нибудь целое число a так, чтобы $a\alpha_1, \ldots a\alpha_n \in A$. Возьмем еще какое-нибудь число $\gamma \in I$. Тогда $\beta_1 := \gamma a\alpha_1, \ldots, \beta_n := \gamma a\alpha_n$ уже лежат в I и по-прежнему составляют базис $F : \mathbb{Q}$.

Если $\beta_1, \ldots, \beta_n \in I \subset A$ — базис $F : \mathbb{Q}$, то дискриминант этого базиса является целым числом: $D(\beta_1, \ldots, \beta_n) \in \mathbb{Z}$ (потому что след $Tr_{F/\mathbb{Q}}(\beta)$ целого числа является целым). Поэтому среди всех базисов $\beta_1, \ldots, \beta_n \in I$ существуют базисы с минимальным по модулю дискриминантом.

Proclaim Теорема. Пусть $\beta_1, \ldots, \beta_n \in I$ — базис $F : \mathbb{Q}$ с минимальным по модулю дискриминантом. Тогда $I = \mathbb{Z}\beta_1 \oplus \ldots \oplus \mathbb{Z}\beta_n$, т.е. I является свободным $\mathbb{Z}$-модулем с базисом $\beta_1, \ldots, \beta_n$.

Доказательство: Пусть $I \ni \beta = c_1\beta_1 + \ldots + c_n\beta_n$, $c_i \in \mathbb{Q}$. Мы хотим доказать, что на самом деле все c_i лежат в $\mathbb{Z}$. Если это не так, можно считать, что $c_1 \notin \mathbb{Z}$. Пусть $c_1 = [c_1] + \{ c_1 \}$ — разложение на целую и дробную часть, $0 < \{ c_1 \} < 1$. Рассмотрим новый базис $\alpha_1 = \beta - [c_1]\beta_1, \alpha_2 = \beta_2, \ldots, \alpha_n = \beta_n$ поля F над $\mathbb{Q}$. Очевидно, $\alpha_i \in I$. Матрица перехода от старого базиса к новому верхнетреугольна, и на диагонали у нее стоят $\{c_1\}, 1, \ldots, 1$. Значит, определитель матрицы перехода равен $\{c_1\}$. Как мы знаем из прошлой лекции, $D(\alpha_1, \ldots, \alpha_n) = \{c_1\}^2 D(\beta_1, \ldots, \beta_n)$. Отсюда $|D(\alpha_1, \ldots, \alpha_n)| < |D(\beta_1, \ldots, \beta_n)|$ — противоречие. $\square$

Пусть $\beta_1, \ldots, \beta_n \in I$ и $\beta'_1, \ldots, \beta'_n \in I$ — два базиса I над $\mathbb{Z}$. Тогда матрица перехода от одного базиса к другому, равно как и ее обратная, имеют целые коэффициенты. Это означает, что их определители равны ± 1. Поэтому $D(\beta_1, \ldots, \beta_n) = D(\beta'_1, \ldots, \beta'_n) =: D(I) \in \mathbb{Z}$. Это корректно определенное целое число называется *дискриминантом идеала* I. В частности, бывает дискриминант и у самого кольца A. Например, $D(\mathbb{Z}[\sqrt{-1}]) = -4$.

Часть 2. Идеалы.

Идеал $I \subset A$ называется *главным*, если он состоит из всех кратных числа $\alpha \in A:\ I = \{\beta\alpha,\ \beta \in A\}$. Тогда он обозначается $(\alpha) \subset A$. Как мы проходили на первом занятии, в евклидовых кольцах все идеалы главные. Но например идеал $(2, 1 + \sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$, порожденный двумя числами: 2 и $1 + \sqrt{-5}$, не является главным. Как мы вскоре увидим, это явление напрямую связано с неоднозначностью разложения на простые множители: $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.

Множество классов эквивалентности по отношению $\alpha \sim \beta \Leftrightarrow \alpha - \beta \in I$ наследует от A структуру кольца и называется *факторкольцом* A/I. Например, $\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$ — обычное кольцо остатков по модулю n. По аналогии с понятием простого числа вводится понятие *простого идеала*: $I \subset A$ называется простым, если из $\alpha \cdot \beta \in I$ следует, что либо $\alpha \in I$, либо $\beta \in I$. Например, главный идеал $(\gamma) \subset A$ прост тогда и только тогда, когда число $\gamma \in A$ простое. Еще простоту идеала I можно сформулировать в терминах факторкольца $A/I:\ I$ прост тогда и только тогда, когда в кольце A/I нет делителей нуля.

Если же факторкольцо A/I является полем, то идеал $I \underset{\neq}{\subset} A$ *максимальный*, т.е. если $I \subset J \underset{\neq}{\subset} A$ (включение идеалов), то $I = J$. Обратное тоже верно. В случае $A = \mathbb{Z}$ максимальные и простые идеалы — это одно и то же. Но вообще говоря, бывают простые немаксимальные идеалы, например, идеал $(x^2 - y^3) \subset \mathbb{C}[x, y]$. Простой он потому, что многочлен $x^2 - y^3$ неразложим, а немаксимальный потому, что класс $\overline{x} \in \mathbb{C}[x, y]/(x^2 - y^3)$ необратим.

Идеалы можно пересекать: если $I, J \subset A$ — идеалы, то $I \cap J$ — тоже идеал. Еще их можно складывать: $I + J := \{\, \alpha + \beta \mid \alpha \in I,\ \beta \in J \,\}$, это тоже идеал. Наконец, их можно перемножать: $I \cdot J := \{\, \alpha_1 \cdot \beta_1 + \ldots + \alpha_k \cdot \beta_k \mid \alpha_i \in I,\ \beta_i \in J \,\}$; и это тоже идеал. Например, в кольце $\mathbb{Z}[\sqrt{-5}]$ имеем $(2) + (1 + \sqrt{-5}) = (2, 1 + \sqrt{-5})$; $(2) \cdot (2) = (4)$; $(2) \cap (2) = (2)$.