Оглавление

Глава 1

Алгебраическое введение

1.1 Кольцо целых алгебраических

Чтобы понять что тут вообще происходит, нужно немного алгебры.
Основное поле - $\mathbb{Q}$. Корни полиномов с коэффициентами из $\mathbb{Q}$ называют алгебраическими над $\mathbb{Q}$. Алгебраическое число называется целым алгебраическим, если его минимальный многочлен $g(x) \in \mathbb{Z}[x]$. Введем множество целых алгебраических поля $\mathbb{Q}(\alpha)$

$$\mathfrak{O}_{\mathbb{Q}(\alpha)} = \{x \mid x \in \mathbb{Q}(\alpha) \ \&\ x \text{ - целое алгебраическое}\}$$

T(?). *$\mathfrak{O}_{\mathbb{Q}(\alpha)}$ - кольцо. Кроме того $\mathbb{Z}[\alpha] \subseteq \mathfrak{O}_{\mathbb{Q}(\alpha)}$ - подкольцо.*

T(?). *K - поле, $R \subset K$ - подкольцо с однозначным разложением на множители. Тогда R содержит корни всех неприводимых унитарных многочленов из $R[x]$*

Нас будет интересовать подкольцо $\mathbb{Z}[\alpha]$ с однозначным разложением на множители. Но в каких случаях будет получаться это однозначное разложение? Теорема гарантирует однозначное разложение в $\mathbb{Z}[\alpha]$, если $\mathbb{Z}[\alpha] = \mathfrak{O}_{\mathbb{Q}(\alpha)}$. Но это не всегда так. Что делать когда это не так?

Пример. *Рассмотрим $\gamma = -\frac{1}{2} + \frac{\sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}]$. Но γ корень $x^2 + x - 1 \in \mathbb{Z}[x]$, значит $\gamma \in \mathfrak{O}_{\mathbb{Q}(\sqrt{5})}$*

T(?). *$\forall \beta \in \mathfrak{O}_{\mathbb{Q}(\alpha)} \to \beta \cdot f'(\alpha) \in \mathbb{Z}[\alpha]$, где $f'(x)$ - минимальный многочлен α*

1.2 Норма

Вспомним, что $\mathbb{Q}(\alpha)$ - в.п. над $\mathbb{Q}$. Введем в этом пространстве линейный оператор, соответствующий некоторому элементу $\beta \in \mathbb{Q}(\alpha)$

$$\mathcal{H}_\beta : \ \mathbb{Q}(\alpha) \xrightarrow[x \mapsto \beta x]{} \mathbb{Q}(\alpha)$$

Опр. *Норма* $\beta \in \mathbb{Q}(\alpha)$ *определяется следующим равенством*

$$\mathcal{N}(\beta) = det(\mathcal{H}_\beta)$$

Как вычислять эту норму для произвольного элемента? Пока не ясно. В алгоритме говорится, что норму элемента вида $\beta = a + b\alpha$ можно вычислить по формуле

$$\mathcal{N}(\beta) = F(a,b) = b^{degf} f(\frac{a}{b}), \text{ где } f \text{ - полином степени порождающий поле.}$$

Откуда эта формула? Как ее получить из определения? Нужно разбираться. Но пока будем считать, что все норм.

Пример. *Попробуем вычислить норму* $\beta = a + b\sqrt{5}$ *в* $\mathbb{Q}(\sqrt{5})$*.*
Найдем $\mathcal{H}_\beta = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$*. По определению эта матрица соответствует оператору, который* x *отправляет в* βx*. Подействуем этой матрицей на элементы* 1 *и* $\sqrt{5}$*. Им соответствуют векторы* $(1,0)$ *и* $(0,1)$*.*

$$\beta \cdot 1 = \beta = a + b\sqrt{5} \Rightarrow \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_3 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

$$\beta \cdot \sqrt{5} = 5b + a\sqrt{5} \Rightarrow \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_4 \end{pmatrix} = \begin{pmatrix} 5b \\ a \end{pmatrix}$$

Получили матрицу $\begin{pmatrix} a & 5b \\ b & a \end{pmatrix}$*. Делаем вывод, что* $\mathcal{N}(\beta) = det(\mathcal{H}_\beta) = a^2 - 5b^2$*. Попробуем вычислить по формуле. Поле* $\mathbb{Q}(\sqrt{5})$ *построено с помощью полинома* $f(x) = x^2 - 5$*.*

$$\mathcal{N}(\beta) = F(a,b) = b^2 f(\frac{a}{b}) = b^2((\frac{a}{b})^2 - 5) = a^2 - 5b^2$$

Магия...

Глава 2

Специальный метод решета числового поля

Пусть нужно факторизовать число

$$n = r^t - s$$

Нам нужно построить поле по некоторому полиному $f(x)$. Выберем d - степень полинома.

$$r^t - s \equiv 0 \; mod \; n$$

$$r^t \equiv s \; mod \; n$$

Положим $k = \lceil \frac{t}{d} \rceil$ и домножим обе части на r^{kd}

$$r^{t+kd} \equiv sr^{kd} \; mod \; n$$

$$r^{kd} \equiv sr^{kd-t} \; mod \; n$$

Положим $m = r^k$ и $c = sr^{kd-t}$

$$m^d \equiv c \; mod \; n$$

В качестве полинома возьмем

$$f(x) = x^d - c$$

Построим поле

$${}^{\mathbb{Q}[x]}/_{(f)} \cong \mathbb{Q}(\alpha), \text{ где } \alpha \text{ - корень } f(x)$$

Что же делать дальше?

Литература

[1] Text

Приложение A

Приложение