

Оглавление

1	Алгебраическое введение	2
1.1	Кольцо целых алгебраических	2
1.2	Норма	2
2	Специальный метод решета числового поля	3
A	Приложение	5

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 $\mathbb{Q}(\alpha)$

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

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

Т(?). 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 $\mathfrak{O}_{\mathbb{Q}(\alpha)}$. Если $\mathbb{Z}[\alpha] = \mathfrak{O}_{\mathbb{Q}(\alpha)}$ то все ок. Но это не всегда 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 $\gamma \in \mathfrak{O}_{\mathbb{Q}(\sqrt{5})}$

Т(?). $\forall \beta \in \mathfrak{O}_{\mathbb{Q}(\alpha)} \rightarrow \beta \cdot f'(\alpha) \in \mathbb{Z}[\alpha]$, где $f'(x)$ - минимальный многочлен α

1.2 Норма

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.

$$r^t - s \equiv 0 \pmod{n}$$

$$r^t \equiv s \pmod{n}$$

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

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

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

Положим $m = r^k$ и $c = sr^{kd-t}$

$$m^d \equiv c \pmod{n}$$

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 А

Приложение