

Теория чисел (практика)

Владимир Латыпов
donrumata03@gmail.com

Vladimir Latypov
donrumata03@gmail.com

Содержание

1 Разбор ДЗ 1	3
1.1 Поле	3
1.2 Корректность определения локализации $S^{-1}R$	3
1.3 Пример, где условие $\cdot s$ существенно: \mathbb{Z}	3
1.4 Прообраз идеала при гомоморфизме — тоже идеал	3
2 Гауссовы числа	3
3 Практика 2	3
3.1 Раскладываем на простые множители в кольце Гауссовых чисел	3

1 Разбор ДЗ 1

1.1 Поле

Теорема 1.1.1 $\frac{\mathbb{Z}}{p\mathbb{Z}}$ — поле из p элементов

Доказательство Решим уравнение $\bar{a} \cdot \bar{b} + \bar{c} \cdot \bar{d} = 1$ алгоритмом Евклида, тогда $\bar{a} \cdot \bar{b} = 1$.
□

1.2 Корретность определения локализации $S^{-1}R$

Показываем, что отношение из определения $S^{-1}R$ — отношение эквивалентности:
 $(a_1, s_1) \sim (a_2, s_2) \stackrel{\text{def}}{\iff} (a_1 s_2 - a_2 s_1) \cdot s$ для некоторого s .

Без s транзитивность для не областей целостности не докажется.

Д: домножим накрест равенства, вынесем за скобку.

1.3 Пример, где условие $\cdot s$ существенно: \mathbb{Z}

$$S = \{1, 2, 4\}$$

$$S^{-1}R \cong \mathbb{F}_3$$

Разберём 18 случаев, расположим в 3 ряда, 6 колонок.

1.4 Прообраз идеала при гомоморфизме — тоже идеал

Замечание 1.4.2 Уже доказали для ядра (прообраза $\{0\}$)

Доказательство Для начала покажем, что это

□

2 Гауссовы числа

Определение 2.3 $\mathbb{Z}[i]$ — целые Гауссовы числа ($\Re, \Im \in \mathbb{Z}$)

Поле частных $\mathbb{Q}[i] (\cong \mathbb{Q}[i] = \mathbb{Z}[i] + i\mathbb{Z}[i])$ вкладывается в \mathbb{C} .

Евклидова норма определяется почти как для комплексных: $d(a + bi) = a^2 + b^2$.

Целые гауссовы числа — тоже Евклидово кольцо: для деления с остатком

- делим как комплексные числа
- берём ближайшее из $\mathbb{Z}[i]$

3 Практика 2

3.1 Раскладываем на простые множители в кольце Гауссовых чисел

От 1 до 10-и

- 1
- $2 = (1 + i)(1 - i) = -i(1 + i)^2$
- 3
- $5 = (2 - i)(2 + i)$
- 7

Замечание 3.1.4 Если сумма квадратов частей — простое число, то и само Гауссово число простое ($a^2 + b^2$ — простое $\Rightarrow a + bi$ — простое + в силу мультипликативности нормы « $\|a + bi\| = a^2 + b^2$ » имеем $N(a + bi) = N(x) + N(y)$)

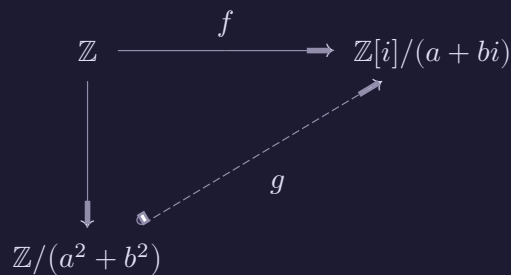
$$1 + 3i = (1 + i)(2 + i)$$

Нарисовали на координатах схемку 5×5 простых гауссовых чисел.

Теорема 3.1.5

$$\mathbb{Z}[i]/(a + bi) \cong \mathbb{Z}/(a^2 + b^2)$$

Доказательство



$$\mathbb{Z} \xrightarrow{f} \mathbb{Z}[i]/(a + bi).$$

Покажем, что $a^2 + b^2 \ni \ker f = \mathbb{Z} \cap_{\text{внутри } \mathbb{Z}[i]} (a + bi)$.

□

Замечание 3.1.6 $a, b \neq 0$ $a + bi$ — простое $\Leftrightarrow a^2 + b^2$ — простое

Пример 3.1.7

Easy to learn

Great output

Intuitive

Our best Typst yet

Responsive design in print
for everyone

One more thing...

$\mathbb{Z}[i]/(2) = \mathbb{Z}[i]/(1 + i)^2 = \mathbb{F}_2[\varepsilon]/(\varepsilon^2)$ (где ε — нильпотент)

dfgdsfg dfgdsfg dfgdsfgdfgdsfg dfgdsfg dfgdsfg
dfgdsfg dfgdsfg dfgdsfgdfgdsfg dfgdsfg dfgdsfg
dfgdsfg dfgdsfg dfgdsfgdfgdsfg dfgdsfg dfgdsfg
dfgdsfg dfgdsfg dfgdsfgdfgdsfg dfgdsfg dfgdsfg
dfgdsfg dfgdsfg dfgdsfgdfgdsfg dfgdsfg dfgdsfg

Теорема 3.1.8 (*theorem 8: Китайская теорема об остатках*)
 $\gcd(m, n) = 1 \implies \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$