Арифметика целых алгебраических чисел

Всюду в этом листке поле $\mathbb{F} \supset \mathbb{Q}$ является конечным расширением степени n, кольцо $\mathcal{O} \subset \mathbb{F}$ — целым замыканием $\mathbb{Z}$ в $\mathbb{F}$, а «идеал» по умолчанию означает *ненулевой* идеал кольца $\mathcal{O}$.

ТГ4½◇1. Покажите, что **а)** любой идеал $\mathfrak{a} \subset \mathcal{O}$ содержит базис поля $\mathbb{F}$ как векторного пространства над $\mathbb{Q}$ **б)** такой базис с минимальным по абсолютной величине определителем Грама билинейной формы следа $\operatorname{sp}(\alpha, \beta) \stackrel{\text{def}}{=} \operatorname{Sp}(\alpha\beta)$ одновременно является базисом $\mathfrak{a}$ как модуля над $\mathbb{Z}$ **в)** если $b\mathfrak{a} \subset \mathfrak{a}$ для некоторого числа $b \in \mathbb{F}$ и идеала $\mathfrak{a}$, то $b \in \mathcal{O}$.

ТГ4½◇2. Покажите, что $\mathfrak{a} \cap \mathbb{Z} \neq 0$ для любого идеала $\mathfrak{a} \subset \mathcal{O}$ и выведите отсюда, что **а)** факторкольцо $\mathcal{O}/\mathfrak{a}$ конечно **б)** множество идеалов, содержащих заданный идеал, конечно **в)** каждый простой идеал в $\mathcal{O}$ максимален **г)** каждый собственный идеал в $\mathcal{O}$ является произведением конечного числа простых.

ТГ4½◇3. Для любых идеалов $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}$ и элемента $c \in \mathcal{O}$ покажите, что **а)** если $\mathfrak{a}\mathfrak{b} = \mathfrak{b}$, то $\mathfrak{a} = \mathcal{O}$ **б)** если $\mathfrak{a}\mathfrak{b} = (c)\mathfrak{b}$, то $\mathfrak{a} = (c)$.

ТГ4½◇4 (классы идеалов). Покажите, что отношение $\mathfrak{a} \sim \mathfrak{b}$, означающее, что $(a)\mathfrak{a} = (b)\mathfrak{b}$ для некоторых ненулевых $a, b \in \mathcal{O}$, является эквивалентностью на множестве идеалов в $\mathcal{O}$, причём все идеалы эквивалентны друг другу, если и только если $\mathcal{O}$ является областью главных идеалов.

ТГ4½◇5 (лемма Гурвица). Обозначим через $\sigma_1, \dots, \sigma_n : \mathbb{F} \hookrightarrow \mathbb{C}$ все различные вложения, а через $e_1, \dots, e_n$ — какой-нибудь базис $\mathcal{O}$ как модуля над $\mathbb{Z}$, и пусть $C = \prod_j \sum_i |\sigma_j(e_i)|$. Зафиксируем натуральное $m \geqslant \sqrt[n]{C}$ и положим $M = m^n$. Покажите, что для любых $a \in \mathcal{O}$ и ненулевого $b \in \mathcal{O}$ найдутся такие $q \in \mathcal{O}$ и натуральное $t \leqslant M$, что $|N(ta - qb)| < |N(b)|$.

ТГ4½◇6 (число классов). Покажите, что множество классов идеалов конечно. Его мощность обозначается $h_{\mathbb{F}}$ и называется *числом классов* поля $\mathbb{F}$.

ТГ4½◇7. Покажите, что для любого идеала $\mathfrak{a} \subset \mathcal{O}$ существует такое натуральное $k \leqslant h_{\mathbb{F}}$, что идеал $\mathfrak{a}^k$ является главным.

ТГ4½◇8 (группа классов). Покажите, что **а)** $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{c} \;\Rightarrow\; \mathfrak{a} = \mathfrak{b}$ для любых идеалов $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ **б)** если $\mathfrak{a} \subset \mathfrak{b}$, то $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ для некоторого идеала $\mathfrak{c}$ **в)** умножение идеалов корректно задаёт на множестве классов структуру абелевой группы.

ТГ4½◇9 (порядки). Покажите что для любого простого идеала $\mathfrak{p} \subset \mathcal{O}$ и произвольного идеала $\mathfrak{a} \subset \mathcal{O}$ корректно определён *порядок* $\operatorname{ord}_{\mathfrak{p}} \mathfrak{a} \stackrel{\text{def}}{=} \max(m \in \mathbb{Z}_{\geqslant 0} \mid \mathfrak{a} \subset \mathfrak{p}^m)$ со свойствами: **а)** $\operatorname{ord}_{\mathfrak{p}} \mathfrak{p} = 1$ и $\operatorname{ord}_{\mathfrak{p}} \mathfrak{q} = 0$ для всех простых идеалов $\mathfrak{p} \neq \mathfrak{q}$ **б)** $\operatorname{ord}_{\mathfrak{p}} \mathfrak{a}\mathfrak{b} = \operatorname{ord}_{\mathfrak{p}} \mathfrak{a} + \operatorname{ord}_{\mathfrak{p}} \mathfrak{b}$ для любых $\mathfrak{a}$, $\mathfrak{b}$ и простого $\mathfrak{p}$ **в)** в любом разложении идеала $\mathfrak{a}$ в произведение простых из зад. ТГ4½◇2 (г) каждый простой идеал $\mathfrak{p}$ присутствует ровно $\operatorname{ord}_{\mathfrak{p}} \mathfrak{a}$ раз.

ТГ4½◇10 (ветвление и степень). Пусть $p \in \mathbb{Z}$ — простое и $(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$, где $\mathfrak{p}_1, \dots, \mathfrak{p}_m \subset \mathcal{O}$ попарно разные простые идеалы. Числа e_i называются *индексами ветвления*, а числа $d_i \stackrel{\text{def}}{=} \stackrel{\text{def}}{=} [\mathcal{O}/\mathfrak{p}_i : \mathbb{Z}/(p)]$ — *степенями* идеалов $\mathfrak{p}_i$ в p. Покажите, что $\sum d_i e_i = n$.

ТГ4½◇11. Пусть поле $\mathbb{F}$ нормально над $\mathbb{Q}$. Покажите, что **а)** для любого простого $p \in \mathbb{Z}$ группа $\operatorname{Gal} \mathbb{F}/\mathbb{Q}$ транзитивно действует на простых идеалах $\mathfrak{p} \supset (p)$ **б)** в разложении $(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ из предыдущей задачи все индексы e_i равны одному и тому числу e, а все степени d_i — одному и тому же d **в)** для любого простого идеала $\mathfrak{p}$ из разложения (p) имеется сюръективный гомоморфизм $\pi_p^{\mathfrak{p}}$ из группы[1] $G_{\mathfrak{p}} \stackrel{\text{def}}{=} \{\sigma \in \operatorname{Gal} \mathbb{F}/\mathbb{Q} \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$ в группу Галуа поля $\mathcal{O}/\mathfrak{p}$ над $\mathbb{F}_p$, переводящий $\sigma \in G_{\mathfrak{p}}$ в $\overline{\sigma} : [a]_{\mathfrak{p}} \mapsto [\sigma(a)]_{\mathfrak{p}}$ **г)** $|G_{\mathfrak{p}}| = ed$, $|\ker \pi_p^{\mathfrak{p}}| = e$ **д) (элемент Фробениуса)** если $e = 1$, то существует единственный такой автоморфизм $\varphi_p \in G_{\mathfrak{p}}$, что $[\varphi_p(\vartheta)]_{\mathfrak{p}} = [\vartheta^p]_{\mathfrak{p}}$ для всех $\vartheta \in \mathcal{O}$.

[1] Группы $G_{\mathfrak{p}}$ и $\ker \pi_p^{\mathfrak{p}} \lhd G_{\mathfrak{p}}$ называются соответственно группами *разложения* и *инерции* простого идеала $\mathfrak{p}$ в p.