Кольца целых

Пусть $d \in \mathbb{Z}$ свободно от квадратов. Определим *квадратичное поле* $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}\langle x^2 - d\rangle$.

Задача 1. Докажите, что кольцо целых $\mathbb{Q}(\sqrt{d})$ порождено

a) единицей и элементом $\sqrt{d}$ при $d \equiv 2, 3 \bmod 4$;

b) единицей и элементом $(\sqrt{d}+1)/2$ при $d \equiv 1 \bmod 4$.

Задача 2. Пусть $K = \mathbb{Q}(\sqrt{d})$, $\mathcal{O}_K$ — его кольцо целых.

a) Докажите, что элемент $\mathcal{O}_K$ вида $a + b\sqrt{d}$ обратим если и только если $a^2 - db^2 = \pm 1$.

b) Докажите, что при $d < 0$ все обратимые элементы $\mathcal{O}_K$ являются корнями из единицы, и что число их конечно.

c^*) Докажите, что всегда найдётся такой обратимый $u \in \mathcal{O}_K$, что всякий обратимый элемент $\mathcal{O}_K$ записывается в виде $\pm u^m$, $m \in \mathbb{Z}$.

Задача 3. Пусть $K = \mathbb{Q}(\sqrt{d})$, пусть $p \in \mathbb{Z} \subset \mathcal{O}_K$ — простое целое число.

a) Докажите, что фактор по главному идеалу $(p) \subset \mathcal{O}_K$ изоморфен $\mathbb{F}_p[x]/(x^2 - d)\mathbb{F}_p[x]$.

b) Докажите, что идеал $(p) \subset \mathcal{O}_K$ прост, если d не является квадратом в $\mathbb{F}_p$, а в противном случае распадается в произведение двух идеалов, совмещаемых действием группы Галуа $\mathrm{Gal}(K, \mathbb{Q})$. Какие доказанные ранее утверждения про числа Гаусса и Эйзенштейна отсюда следуют?

c) Докажите, что фактор $\mathcal{O}_K$ по любому простому идеалу изоморфен $\mathbb{F}_p$ или $\mathbb{F}_{p^2}$ для некоторого p.

Задача 4. Пусть $K = \mathbb{Q}(\zeta_p)$, $\mathcal{O}_K$ — его кольцо целых.

a) Докажите, что $\mathbb{Z}(\zeta_p) \subset \mathcal{O}_K \subset \frac{1}{p}\mathbb{Z}(\zeta_p)$.
Hint: Вычислите след элемента $\mathbb{Q}(\zeta_p)$.

b) Докажите, что главный идеал $(1 - \zeta_p) \subset \mathcal{O}_K$ прост.
Hint: Вычислите норму элемента $1 - \zeta_p$.

c^*) Докажите, что p-тая степень идеала $(1 - \zeta_p)$ совпадает с (p).

d^*) Докажите, что кольцо целых кругового поля $\mathbb{Q}(\zeta_p)$ совпадает с $\mathbb{Z}(\zeta_p)$.
Hint: Исследуйте делимость на степени $1 - \zeta_p$.

Задача 5. Пусть $K = \mathbb{Q}(\zeta_p)$, $\sigma_q : K \to K$ — автоморфизм, переводящий ζ_p в ζ_p^q. Пусть $p^* = (-1)^{\frac{p-1}{2}} p$ (сверьте с ответом к задаче 3b) прошлого листка).

a) Докажите, что элемент $\tau = \sqrt{p^*} \in \mathbb{Q}(\zeta_p)$ содержится в $\mathbb{Z}(\zeta_p)$, а значит и $\mathcal{O}_K$.

b) Докажите, что $\sigma_q(\tau) = \left(\frac{q}{p}\right)\tau$, где символ Лежандра

$$\left(\frac{q}{p}\right) = \begin{cases} 1 & q \neq 0 \text{ квадрат в } \mathbb{Z}/p\mathbb{Z}; \\ -1 & q \neq 0 \text{ не квадрат в } \mathbb{Z}/p\mathbb{Z}; \\ 0 & q = 0. \end{cases}$$

c) Пусть I_q — максимальный идеал $\mathcal{O}_K$, сорержащий q. Докажите, что для всякго $x \in \mathcal{O}_K$ выполнено $\sigma_q(x) \equiv x^q \bmod I_q$ (то есть $\sigma_q(x) - x^q \in I_q$).

d) Пусть теперь p и q — различные нечётные простые целые числа. Докажите, что $\tau \notin I_q$ и $\sigma_q(\tau)/\tau \equiv (p^*)^{(q-1)/2} \bmod I_q$.

e) Выведите из этого *квадратичный закон взаимности*: для всяких различных нечётных простых целых чисел выполнено

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}.$$