Дополнение для 10 дз, необязательное

Задачи

Задача 9. Найти базис Грёбнера для идеала $(x^3yz - xz^2, xy^2z - xyz, x^2y^2 - z)$.

Доказательство квадратичного закона взаимности. Напомню, что квадратичный закон взаимности говорит, что $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ для различных нечётных простых p и q. Основная идея состоит в том, чтобы явно написать корень из q по модулю p для достаточно большого расширения $\mathbb{F}_{p^n}$ поля $\mathbb{F}_p$, а затем свести всё к вопросу — принадлежит этот корень подполю $\mathbb{F}_p$ или нет.

Задача 10. Пусть p и q различные нечётные простые.
а) Покажите, что для подходящего n поле $\mathbb{F}_{p^n}$ содержит первообразный корень степени q из единицы.
б) Покажите, что сумма

$$C(a) = \sum_{t \in \mathbb{F}_q^*} \left(\frac{1 - at^{-1}}{q}\right) = 0$$

при $a \neq 0 \in \mathbb{F}_q$ сделав замену переменных.
в) Пусть ω – первообразный корень степени q из единицы в поле $\mathbb{F}_{p^n}$. Рассмотрим выражение

$$\tau = \sum_{i \in \mathbb{Z}/q} \left(\frac{i}{q}\right) \omega^i.$$

Непосредственно возведя в квадрат проверьте, что

$$\tau^2 = (-1)^{\frac{q-1}{2}} q.$$

Вспомните вычисление определителя с корнями из единицы – по-моему это он. г) Покажите, что для всякого $x \in \mathbb{F}_{p^n}$ верно, что $x \in \mathbb{F}_p$, тогда и только тогда, когда $x^p = x$ (вообще говоря, этот пункт не обязательно использовать дальше, но идея всех вычислений состоит примерно в этом).
д) Воспользуйтесь $\mathbb{F}_p$-линейностью возведения в степень p и вычислите $\tau^p = \left(\frac{p}{q}\right)\tau$.
е) Вычислите y^{p-1} двумя способами и получите квадратичный закон взаимности.