Выкладки к докладу по статье Abualrub, Oehmke

0.1 Идеалы в кольце $\mathbb{Z}_2[x]/(x^n-1)$

0.1.1 НОД всех делителей порождает сумму порождённых ими идеалов

Верно в Евклидовом кольце главных идеалов.

Пусть d_1, d_2 — два из них. Тогда для каких-то a, b верно, что $ad_1 + bd_2 = gcd(d_1, d_2)$. Следовательно, $gcd(d_1, d_2) \in I = (d_1) + (d_2)$. $I = (a)$, но тогда a — общий делитель d_1 и $gcd(d_1, d_2)$, в силу минимальности сумму среди идеалов, содержащих (d_1) и (d_2), наибольший, то есть $gcd(d_1, d_2)$.

У многочлена конечное число делителей, а НОД — ассоциативная операция. Повторяя процедуру на множестве делителей, в котором на каждом шаге произвольные два элемента заменяются на их НОД, а соответствующие два идеала на их сумму, получаем утверждение.

0.1.2 $(x-1)$ — единственный максимальный идеал.

Любой идеал содержится в $(x-1)$ по предыдущей выкладке, при этом сам он максимален.

0.1.3 Главный идеал, порождённый нильпотентом a, нильпотентен

Любой элемент этого идеала имеет вид ra.

0.2 Редукция по модулю p

0.2.1 Идеал, порождённый нильпотентами, нильпотентен

Индукция. Базовый случай дан рассмотрением главных идеалов.

Переход. Пусть a_i, $i \in \{1; \ldots; k+1\}$ нильпотентны. Пусть $(a_1, ..., a_k)$ нильпотентен. Идеал $(a_1, \ldots, a_{k+1}) = (a_1, ..., a_k) + (a_{k+1})$. Достаточно доказать нильпотентность сумм элементов из правого и из левого идеалов. Пусть a слева нильпотентен степени α, b справа — степени β. Взяв $(a+b)^{\alpha+\beta}$, гарантированно получим 0 по комбинаторным соображениям.

0.3 Характеризация пересечения максимальных идеалов

0.3.1 Элемент необратим <=> он содержится в максимальном идеале

.

Если обратим, он порождает всё кольцо. Иначе он порождает свой главный идеал, который содержится в некотором максимальном. В обратную сторону — обратимый элемент тянет в идеал единицу.