Идеалы колец $\mathbb{Z}_4[x]/(x^n - 1)$ для $n = 2^e$

На основе статьи

Cyclic codes of length 2^e over $\mathbb{Z}_4$

`https://core.ac.uk/download/pdf/82251738.pdf`

Авторы: Taher Abualrub, Robert Oehmke

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

Главные, порождены делителями $x^n - 1$.
Разложим $x^n - 1$: $x^{2^e} - 1 = (x^{2^{e-1}} - 1)^2 = (x - 1)^n$.

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

Главные, порождены делителями $x^n - 1$.
Разложим $x^n - 1$: $x^{2^e} - 1 = (x^{2^{e-1}} - 1)^2 = (x - 1)^n$.

НОД всех делителей — $x - 1$. На другом языке сумма всех идеалов равна $(x - 1)$.
Следовательно, $(x - 1)$ — единственный максимальный идеал.
Он нильпотентен степени n. Следовательно, это кольцо Галуа.

Идеалы при сюръективном отображении

Пусть $\phi : A \to B$ — сюръективное отображение.
По теореме об изоморфизме $A/\ker\phi \cong B$

Следовательно, (максимальные) идеалы A, содержащие $\ker\phi$, биективны (максимальным) идеалам B.

Редукция по модулю p

1. $\phi : R = \mathbb{Z}_4[x]/(x^n - 1) \to \mathbb{Z}_2[x]/(x^n - 1)$.
2. $\ker \phi = (2)$
3. $\phi^{-1}((x-1)) = (2) + (x-1) = (2, x-1)$
4. Это единственный максимальный идеал, нильпотентный.
5. Является ли он главным?

Характеризация пересечения максимальных идеалов

Утверждение (курс коммутативной алгебры)

Элемент x принадлежит пересечению J максимальных идеалов коммутативного кольца A тогда и только тогда, когда $1 - xy$ обратим для любого $y \in A$

Характеризация пересечения максимальных идеалов

Утверждение (курс коммутативной алгебры)

Элемент x принадлежит пересечению J максимальных идеалов коммутативного кольца A тогда и только тогда, когда $1 - xy$ обратим для любого $y \in A$

Если элемент $a = 1 - xy_0$ необратим, он содержится в максимальном идеале m. По предположению $x \in m$. Тогда $xy_0 \in m$ и $1 \in m$. Противоречие, доказали, что все элементы J удовлетворяют этому свойству.

Характеризация пересечения максимальных идеалов

Утверждение (курс коммутативной алгебры)

Элемент x принадлежит пересечению J максимальных идеалов коммутативного кольца A тогда и только тогда, когда $1 - xy$ обратим для любого $y \in A$

Если элемент $a = 1 - xy_0$ необратим, он содержится в максимальном идеале m. По предположению $x \in m$. Тогда $xy_0 \in m$ и $1 \in m$. Противоречие, доказали, что все элементы J удовлетворяют этому свойству.

В другую сторону. Пусть m — какой-то максимальный идеал и $x \notin m$. Тогда $(x) + m = A$, в частности для каких-то $w \in m$ и y_0 $w + xy_0 = 1$. Следовательно, $1 - xy_0 \in m$, а значит, необратим.

Максимальный идеал в локальном кольце

Утверждение

Пусть (A, m) — локальное кольцо и $m = (a)$. Пусть $m = (a_1, \ldots, a_n)$. Тогда $m = (a_i)$ для какого-то $i \in 1, \ldots, n$.

Максимальный идеал в локальном кольце

Утверждение

Пусть (A, m) — локальное кольцо и $m = (a)$. Пусть $m = (a_1, \ldots, a_n)$. Тогда $m = (a_i)$ для какого-то $i \in 1, \ldots, n$.

Для $n = 1$ утверждение тавтологично. Пусть оно верно для $n = k$, рассмотрим $k + 1$.

Верно, что $a_1 = ra$ (1). Если r обратим, $m = (a_1)$. Иначе $r = \sum_1^{k+1} \alpha_i a_i$. Подставим в (1): $a_1(1 - \alpha_1 a) = \sum_2^{k+1} a\alpha_i a_i$. Множитель при a_1 обратим, поскольку максимальный идеал единственен, значит, $m = (a_2, \ldots, a_{k+1})$

Максимальный идеал в локальном кольце

Утверждение

Пусть (A, m) — локальное кольцо и $m = (a)$. Пусть $m = (a_1, \ldots, a_n)$. Тогда $m = (a_i)$ для какого-то $i \in 1, \ldots, n$.

Для $n = 1$ утверждение тавтологично. Пусть оно верно для $n = k$, рассмотрим $k + 1$.

Верно, что $a_1 = ra$ (1). Если r обратим, $m = (a_1)$. Иначе $r = \sum_1^{k+1} \alpha_i a_i$. Подставим в (1): $a_1(1 - \alpha_1 a) = \sum_2^{k+1} a\alpha_i a_i$. Множитель при a_1 обратим, поскольку максимальный идеал единственен, значит, $m = (a_2, \ldots, a_{k+1})$

Заключаем, что идеал $(2, x - 1) \subset R$ не является главным.

Классификация идеалов.

Мы зафиксировали, что R не является кольцом главных идеалов.

Пусть I — идеал и $g \in I$ — элемент минимальной степени.

Классификация идеалов.

Мы зафиксировали, что R не является кольцом главных идеалов.

Пусть I — идеал и $g \in I$ — элемент минимальной степени.

Пусть g — унитарный многочлен. Тогда на него можно делить с остатком в $\mathbb{Z}_4[x]$, получая остаток меньшей степени.

Поделив все элементы I, представленные собой в $Z_4[x]$, получили, что $I = (g)$. Нулевой элемент можно представить как $x^n - 1$, значит, $g \mid x^n - 1$.

Это рассуждение дословно повторяет общее рассуждение, классифицирующее идеалы $\mathbb{Z}_2[x]/(x^n - 1)$, на которое мы ссылались в начале.

Отступление: разложение $x^n - 1$ на множители

$$x^4 - 1 = (x^2 + 1)(x - 1)(x + 1) = (x^2 + 2x - 1)(x - 1)(x - 1) = (x^2 + 2x - 1)(x + 1)(x + 1)$$

Классификация идеалов

В R есть неглавные идеалы. Как минимум их элементы минимальной степени не унитарны.

Пусть g не унитарен. То есть старший коэффициент – двойка.
Если $2g \neq 0$, степень $2g$ меньше степени g, значит, $g = 2q$ для какого-то многочлена q с единичными коэффициентами.

Классификация идеалов

Пусть в I нет унитарных многочленов.

Рассмотрим множество элементов I, которые не делятся на g. Если оно не пусто, в нём есть элемент r минимальной степени u. Отметим, что $u \geq s = \deg(g)$. Рассмотрим $w = r - 2qx^{u-s}$.

Он имеет степень, меньшую r, следовательно, делится на $2q$ (или нулевой, что подходит). Тогда и r делится на $2q$. Противоречие.

Следовательно, в этом случае $I = (2q)$.
Мы также получили утверждение, что все неглавные идеалы содержат унитарный многочлен.

Классификация идеалов

Пусть I содержит унитарный многочлен.

Множество унитарных многочленов содержит элемент f минимальной степени t. Множество многочленов степени меньше t попадает в условия предыдущего случая и все его элементы делятся на $2q$.

Классификация идеалов

Пусть I содержит унитарный многочлен.

Множество унитарных многочленов содержит элемент f минимальной степени t. Множество многочленов степени меньше t попадает в условия предыдущего случая и все его элементы делятся на $2q$.

Пусть $a \in I$ — многочлен степени не меньше t.
Поделим его с остатком на f: $a = a'f + r = af + 2qr'$.

Таким образом $I = (f) + (2q) = (f, 2q)$

Классификация идеалов

Теорема

Итого имеем идеалы следующих видов:

1. (g), где g — делитель $x^n - 1$
2. $(2q)$, где q имеет единичные коэффициенты
3. $(f, 2q)$, где f унитарный.

Условие на $f = f_1 + 2f_2$ можно усилить. Вычитая множители вида $2qx^k$, можно добиться того, чтобы степень f_2 была меньше s.

Образ идеала при сюръективном отображении — идеал, а образующая отображается в образующую. Отсюда можно заключить также, что $\phi(f_1) \mid x^n - 1$, $\phi(q) \mid x^n - 1$ и в силу неравенства на степени $\phi(q) \mid \phi(f_1)$.

Классификация идеалов

Чего заключить нельзя:

Нельзя пользоваться подъёмом Гензеля и поднимать им разложение $x^n - 1$. К тому же их несколько.

Но даже если бы было можно, это бы не помогло описать все идеалы.

Example

Главный идеал $(x^3 + x^2 - x - 1) \subset \mathbb{Z}_4[x]/(x^4 - 1)$ не порождается делителем $x^4 - 1$.

Достаточно поделить: $x^4 - 1 = (x - 1)(x^3 + x^2 - x - 1) + 2(x^2 + 1)$.