# Семинар №9 по курсу «Основы высшей алгебры и теории кодирования»

Репеев Роман, Шиманогов Игорь



Кольцо многочленов с коэффициентами в поле $F$ является евклидовым. Из общих свойств евклидовых колец (любое евклидово кольцо является кольцом главных идеалов) получаем, что всякий собственный идеал $I$ в $F[x]$ порождён одним многочленом: $I = (f)$.

**Определение 1 (Нормированный многочлен)**
Обратимые элементы в кольце многочленов — это многочлены степени 0, то есть ненулевые константы. Умножая на ненулевую константу, всегда можно добиться, чтобы старший коэффициент многочлена равнялся 1. Такие многочлены называются нормированными. Умножение многочлена на ненулевую константу не изменяет идеал, порождённый этим многочленом.

**Замечание 1**
*Если стремиться к однозначности представления вычета, то можно использовать то обстоятельство, что класс вычетов образуют многочлены, имеющие одинаковый остаток по модулю $f$. Возможные значения остатка — это многочлены степени меньше $d = deg\ f$. Значит, вычет однозначно задаётся многочленом степени меньше $d$. Для поддержания такого представления при выполнении арифметических операций нужно результат операции делить с остатком на $f$.*
*Из такого однозначного представления вычетов легко посчитать количество элементов в кольце $F[x]/(f)$ для конечного поля $F$, $|F| = q$. Всего есть $d$ коэффициентов, задающих остаток, каждый может принимать $q$ значений. Всего возможных остатков (и элементов в кольце вычетов) ровно $q^d$ штук.*

Интересный факт из общей теории делимости в кольцах:

**Утверждение 1**
Если $a \mid b$, то $(b) \subseteq (a)$.

Так как в евклидовых кольцах все идеалы главные, то для них отсюда выполняется такое

**Утверждение 2**
Элемент евклидова кольца $p$ прост тогда и только, тогда, когда идеал $(p)$ является максимальным.

Введем специальный термин для простых элементов в кольце многочленов.

**Определение 2 (Неприводимый многочлен)**
Многочлен $f \in F[x]$ называется неприводимым над полем $F$, если не существует разложения на собственные множители $f = gh$, $\deg g < \deg f$, $\deg h < \deg f$.

**Теорема 1 (Теорема о конечных полях)**
Каждое конечное поле характеристики $p$ изоморфно кольцу вычетов кольца многочленов $F_p[x]$ по модулю идеала, порождённого неприводимым многочленом.

**Доказательство** Пусть $F$ - конечное поле характеристики $p$. Рассмотрим сюръективный гомоморфизм значения $Ev_\alpha : \mathbb{F}_p[x] \to F$, где $\alpha$ — порождающий мультипликативной группы поля. Из теоремы о гомоморфизме получаем, что $\mathbb{F}_p[x]/\mathrm{Ker}\ Ev_\alpha \cong F$, а из свойств евклидовых колец $\mathrm{Ker}\ Ev_\alpha = (f)$, где $f$ - неприводимый многочлен. Таким образом, получаем одну из основных теорем о конечных полях.

**Следствие 1**
*Итак, чтобы найти конечное поле из $p^n$ элементов (а порядки у полей, как следует из выше сказанного, могут быть только такие), нужно найти неприводимый многочлен $f$ степени $n$ в кольце $\mathbb{F}_p[x]$ и взять кольцо вычетов $\mathbb{F}_p[x]/(f)$. Существование такого многочлена никак не следует из общей теории: в зависимости от поля коэффициентов множества неприводимых многочленов могут быть устроены поразному. Многочлены первой степени всегда неприводимые.*

**Пример 1**

$$\mathbb{F}[x]/(x+a) \cong F$$

**Задача 1 ($x^2+1$)**
Докажите, что $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

**Доказательство** Докажем, что $a+bx \cong a+bi$. Сложение, очевидно, уважается. Посмотрим, что происходит с умножением.

$$(a+bx)(c+dx) = ac+(bc+ad)x+bdx^2 = bd(x^2+1)+ac-bd+(bc+ad)x = ac-bd+(bc+ad)x$$

А значит, и умножение уважается.

Говоря про неприводимость многочленов нельзя не упомянуть следующую теорему, которая, в противоречие своему названию, доказывается лишь привлечением методов из анализа.

**Определение 3 (Алгебраическое замкнутое поле)**
Поле $F$ называется алгебраически замкнутым, если все неприводимые многочлены в $F[x]$ имеют степень 1.

**Теорема 2 (Основная теорема алгебры)**
Всякий многочлен положительной степени над полем $\mathbb{C}$ имеет корень.

**Лемма 1 (О малых степенях)**
Если $\deg f < 3$, то $f \in F[x]$ неприводим тогда и только тогда, когда в поле $F$ у многочлена $f$ нет корней. Однако, для степени 4 это уже не верно:

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$$

Для исследования неприводимости в $\mathbb{Q}[x]$ бывает полезна следующая теорема, которая, несмотря на свое название, критерием не является.

**Теорема 3 (Критерий Эйзенштейна)**
Если для многочлена $q = a_0 + a_1x + \cdots + a_nx^n$ с целыми коэффициентами существует такое простое число $p$ , что $p \nmid a_n$, $p \mid a_i$, $p^2 \nmid a_0$ , то этот многочлен неприводим.

**Пример 2**
*Многочлен $2x^4-6x^3+15x^2+21$ неприводим над полем $\mathbb{Q}$. (Для решения достаточно взять $p = 3$ и применить критерий Эйзенштейна.)*

**Пример 3**
*Для всякого $n > 0$ многочлен $x^n - 2$ неприводим над $\mathbb{Q}$. Достаточно взять $p = 2$ и применить критерий Эйзенштейна. Отсюда вытекает, что над полем рациональных чисел существуют неприводимые многочлены любой степени.*

**Замечание 2**
*Критерий Эйзенштейна даёт только достаточное условие неприводимости. Он неприменим, скажем, к многочленам $x^n + 1$, среди которых есть неприводимые.*

Применим основную теорему арифметики к кольцу многочленов: всякий многочлен раскладывается в произведение степеней неприводимых многочленов:

$$f(x) = {g_1}^{a_1}(x) \cdot \ldots \cdot {g_n}^{a_n}(x)$$

Это разложение однозначно с точностью до перестановки множителей и умножения на обратимые элементы (в нашем случае это константы). В частности, можно считать, что многочлен представлен произведением константы и неприводимых нормированных многочленов. Тогда мы можем воспользоваться Китайской теремой об остатках:

$$F[x]/(f) \cong F[x]/({g_1}^{a_1}) \oplus \cdots \oplus F[x]/({g_n}^{a_n})$$

**Задача 2**
Сколько обратимых элементов в кольце $\mathbb{F}_7/(x^2 - x + 1)$

**Решение** Проверим приводимость многочлена.
Дискриминант квадратного уравнения $x^2 - x + 1$ равен $D = (-1)^2 + 4 = 5$.
$5^{(7-1)/2} = 5^3 = (-2)^3 = -8 = -1$ (вычисления были в поле $\mathbb{F}_7$). Это значит, что 5 является квадратичным невычетом, поэтому у уравнения нет корней, а так как он второй степени, то отсюда следует, что он неприводим.

Тогда наше факторкольцо является полем, поэтому все его ненулевые элементы обратимы.
**Ответ:** $7^2 - 1 = 48$ элементов.

Вернемся к многочлену $x^4 + 1$. Над полем $\mathbb{R}$ он раскладывается на произведение двух неприводимых многочленов второй степени (их неприводимость следует из отсутствия корней).
А что будет в случае поля $\mathbb{Q}$?

**Пример 4**
*Пусть многочлен $x^4+1$ приводим в $\mathbb{Q}[x]$. У него все еще нет корней, поэтому единственный вариант — это разложение в произведение двух неприводимых многочленов второй степени: $x^4 + 1 = f(x)g(x)$ (многочлены с рациональными коэффициентами).*
*Но так как $\mathbb{Q} \subset \mathbb{R}$, то это же разложение будет иметь место и в $\mathbb{R}[x]$. Тогда имеем:*

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1) = f(x)g(x)$$

*Из основной теоремы арифметики мы знаем, что разложение единственное с точностью до умножения на константу.*
*Отсюда следует, что $f(x)$ или $g(x)$ равно $\alpha(x^2 + \sqrt{2}x + 1)$.*
*Так как в этих многочленах коэффициенты должны быть рациональны, то $\alpha$ рационально, иначе коэффициент при $x^2$ иррациональный. Но тогда коэффициент при $x$ равен произведению рационального и иррационального чисел, то есть иррациональный. Противоречие.*
*Значит, в $\mathbb{Q}[x]$ многочлен $x^4 + 1$ неприводим.*

**Задача 3**
Приводим ли многочлен $x^4 + 1$ в кольце $\mathbb{F}_3[x]$?

**Решение** Несложно проверить, что у многочлена нет корней. Но этого недостаточно, чтобы утверждать о неприводимости.
Заметим, что $2 = -1$ является квадратичным невычетом в $\mathbb{F}_3$, поэтому многочлен $x^2 - (-1) = x^2 + 1$ неприводим. Тогда кольцо $F = \mathbb{F}_3[x]/(x^2 + 1)$ является полем (в нем 9 элементов).
В этом поле уже есть квадратный корень из $-1$ — это вычет $\alpha$, содержащий $x$:

$$[x]^2 = [x^2] = [x^2 - (x^2 + 1)] = [-1]$$

Как в предыдущем примере, имеем разложение

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

Можно ли продолжить рассуждение так же, как в предыдущем примере, и сказать, что многочлен неприводим в $\mathbb{F}_3[x]$? Не получится, он приводим:

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

Почему так получилось, в чем разница? В прошлом примере мы пользовались тем, что у многочленов $x^2 \pm \sqrt{2}x + 1$ нет корней в $\mathbb{R}$. В данном случае это не выполняется, как показывает следующая задача.

**Задача 4**
Найти корень многочлена $x^2 - \alpha x + 1$, где $\alpha^2 = -1$ в поле $F = \mathbb{F}_3[x]/(x^2 + 1)$.

**Решение** Мы можем спокойно применить формулу для корней квадратного уравнения (так как характеристика поля $F$ равна 3):

$$x = \frac{1}{2} \cdot \left(\alpha \pm \sqrt{\alpha^2 - 4}\right)$$

В поле характеристики 3 выполняется $2 \cdot 2 = 4 = 1$, поэтому $\frac{1}{2} = 2$.
$\sqrt{\alpha^2 - 4} = \sqrt{-5} = \sqrt{1} = 1$. В итоге получим

$$x = 2\alpha \pm 2$$

Проверим, что $2\alpha + 2$ действительно является корнем:

$$4(\alpha + 1)^2 - \alpha \cdot 2(\alpha + 1) + 1 = 4\alpha^2 + 8\alpha + 4 - 2\alpha^2 - 2\alpha + 1 =$$

$$= 2\alpha^2 + 6\alpha + 5 = -2 + 0 + 5 = 3 = 0$$