Семинар №10 по курсу «Основы высшей алгебры и теории кодирования»

Репеев Роман, Шиманогов Игорь

Будем говорить, что многочлен над полем *раскладывается на линейные множители*, если он, ну, раскладывается на линейные множители, то есть:

$$f(x) = (x - a_1)(x - a_2)\dots(x - a_d), \quad d = \deg f, a_i \neq a_j \text{ при } i \neq j$$

В общем случае многочлен имеет в разложении неприводимые множители степени выше 1. Это можно исправить, используя конструкцию *расширения поля*.

Определение 1 (Расширение поля)
Поле K называется *расширением* поля F, если $F \subset K$.

Пример 1
Поле $\mathbb{R}$ является расширением поля $\mathbb{Q}$. Образ вложения многочлена $x^2 - x - 1 \in \mathbb{Q}[x]$ будет $x^2 - x - 1 \in \mathbb{R}[x]$. Казалось бы, ничего не поменялось, но в первом случае многочлен неприводим, а во втором — приводим.
Из этого вытекает сильное различие в алгебраических свойствах: факторкольцо по идеалу, порожденному данным многочленом, в первом случае является полем, а во втором — нет. Во втором случае есть делители нуля.

Пример 2
Еще один простой пример: $\mathbb{C}$ является расширением $\mathbb{R}$. Над ним приводим многочлен $x^2 + 1$, который неприводим в $\mathbb{R}[x]$.

Рассмотрим пример, который подведет нас к общей конструкции расширений полей.

Пример 3
Рассмотрим многочлен $x^5 + 1 \in \mathbb{F}_2$. Он приводим:

$$x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$$

Второй сомножитель неприводим над $\mathbb{F}_2$. Доказывать сейчас мы это не будем.
Рассмотрим теперь $F = \mathbb{F}_2/(x^4 + x^3 + x^2 + x + 1)$. Ясно, что $\mathbb{F}_2 \subset F$.
В поле F 16 элементов, его мультипликативная группа — это циклическая (как в любом поле) группа из 15 элементов. В ней есть подгруппа из 5 элементов, каждый элемент которой имеет порядок 5, то есть является корнем многочлена $x^5 + 1$.
Значит, в поле F многочлен $x^5 + 1$ раскладывается на линейные множители.

Обобщим этот пример, построив такую конструкцию для любого поля.

Теорема 1 (Теорема о поле разложения многочлена)
Для любого многочлена $f \in F[x]$, где F — поле, существует расширение $K \supset F$ (*поле разложения многочлена*), что f раскладывается на линейные множители в $K[x]$.

Доказательство Построим цепочку расширений:

$$F = F_0 \subset F_1 \subset \dots$$

Разложим f на неприводимые множители над полем F_i. Если все множители имеют степень 1, то мы победили.
Иначе, возьмем из разложения неприводимый многочлен g степени больше 1 и определим следующее расширение:

$$F_{i+1} = F_i[x]/(g)$$

Покажем, что g всегда имеет корень в F_{i+1}. Этот корень — вычет $[x]$.
Пусть $g = \sum g_k x^k,\ g_k \in F_i$. Тогда в F_{i+1}

$$g([x]) = \sum g_k [x]^k = \sum [g_k] \cdot [x^k] = \left[\sum g_k x^k\right] = [g] = [0]$$

Отсюда следует, что количество множителей степени 1 при переходе у очередному расширению возрастает по крайней мере на 1. Так как общее число таких множителей ограничено степенью f, то в определенный момент цепочка закончится.

Дальше мы будем рассматривать многочлен $x^q - x \in \mathbb{F}_p[x]$, где $q = p^n$.

Утверждение 1
Корни многочлена $x^q - x$ в поле разложения образуют поле.

Доказательство Напомним утверждение, называемое биномом двоечника: в поле характеристики p выполняется $(x + y)^p = x^p + y^p$.
Из него индукцией несложно получить, что для любого n выполняется $(x + y)^{p^n} = x^{p^n} + y^{p^n}$.
Тогда для всякой пары α, β корней многочлена $x^q - x$ выполнено:

$$(\alpha + \beta)^q = \alpha^q + \beta^q, \quad (\alpha\beta)^q = \alpha^q \beta^q$$

Тогда $\alpha + \beta$ и $\alpha\beta$ также являются корнями многочлена. То есть, множество корней замкнуто относительно сложения и умножения.
0 и 1, как видно из прямой подстановки, являются корнями. Так как множество корней

ненулевого многочлена конечно, то множества $\{k\alpha\}$ и $\{\alpha^k\}$ будут конечными, откуда получается, что это будут группы (это рассуждение применялось, когда мы говорили о циклических подгруппах).
Если точнее, то, что нам нужно — из этого следует, что для всякого α в множестве корней также будут $-\alpha$ и α^{-1}.
Получается, что мы доказали все аксиомы поля.

Введем понятие производной для многочленов. Оно, в общем-то, не отличается от такового в анализе, но так как мы говорим не о функциях в $\mathbb{R}$ или $\mathbb{C}$, а о формальных выражениях, то технически это понятие с анализом не имеет ничего общего.

Определение 2 (Производная многочлена)
Производная многочлена задается отображением $D : \ F[x] \mapsto F[x]$, удовлетворяющим условиям:

- $D(c) = 0$ для всякой константы c (т.е. многочлена степени 0 или нуля)
- $D(x^n) = nx^{n-1}$
- Линейность:

$$\forall\ \alpha, \beta \in F,\ f, g \in F[x] \quad D(\alpha f + \beta g) = \alpha D(f) + \beta D(g)$$

Лемма 1 (Формула Лейбница)
$D(fg) = D(f)g + fD(g)$

Утверждение 2
Пусть f и $D(f)$ взаимно просты. Тогда f не имеет кратных корней (не делится на квадрат).

Доказательство Предположим противное: $f = g^2 \cdot h$.
Тогда $D(f) = 2D(g)gh + g^2D(h)$. Значит, g является общим делителем f и $D(f)$ — противоречие.

Задача 1
Доказать, что в поле разложения многочлена $x^7 - 1 \in \mathbb{F}_5[x]$ больше 1000 элементов.

Решение Обозначим поле разложения F, его характеристика равна 5.
Если оно конечно (если нет, то элементов точно больше 1000), то в нем 5^n элементов.
Многочлен $x^7 - 1$ взаимно прост со своей производной $7x^6$ в этом поле. Поэтому у него ровно 7 различных корней.
Рассмотрим корень $\alpha \neq 1$. $\alpha^7 - 1 = 0$, то есть α — элемент порядка 7 (так как это простое число) в мультипликативной группе поля F^*, в которой $5^n - 1$ элемент. Порядок элемента делит порядок группы, т.е. $7 \mid 5^n - 1$.
Найдем наименьшее такое n, что $5^n \equiv 1 \mod 7$. Это порядок 5 в мультипликативной группе вычетов по модулю 7 (в ней 6 элементов). Он может быть равен 1, 2, 3 или 6.
Опытной проверкой можно убедиться, что первые три варианта не подходят, поэтому $n = 6$.
Значит, в F элементов не меньше, чем $5^6 > 1000$, ч.т.д.

Обратное утверждение также верно. Это доказывается с помощью формулы Лейбница, которой мы находим выражение для производной из вида разложения f на линейные сомножители. Итак,

Теорема 2 (Критерий отсутствия кратных корней)
$f \in F[x]$ не имеет кратных корней тогда и только тогда, когда f и $D(f)$ взаимно просты.

Замечание 1
Отметим, что это утверждение верно для любого поля, а не только поля разложения.

Задача 2
Есть ли нильпотентные элементы в $\mathbb{F}_7/(x^3+4x-2)$?

Решение Посмотрим, есть ли у многочлена кратные корни. $f = x^3+4x-2$. $D(f) = 3x^2+4$. Нормируем производную (домножение на обратимый элемент не влияет на делимости):

$$\frac{1}{3}D(x) = -2D(x) = x^2 - 8 = x^2 - 1 = (x+1)(x-1)$$

Убеждаемся, что ± 1 не являются корнями f, поэтому f взаимно прост с $D(f)$, следовательно, не имеет кратных корней.
Из этого следует, что в $\mathbb{F}_7/(f)$ нет нильпотентных элементов. Пусть $[g]^k = [0]$, то есть g^k делится на f. Тогда g делится на каждый неприводимый делитель f, а значит и на сам f, так как кратных корней в f нет.

Убедимся, что у многочлена $x^q - x$ нет кратных корней. Вычислим производную:

$$D(x^q - x) = qx^{q-1} - 1 = -1$$

Многочлен взаимно прост со своей производной -1, поэтому не имеет кратных корней.
Тогда получается, что многочлен $x^q - x$ имеет в поле разложения ровно q корней (так как там он раскладывается на линейные множители, при этом там q различных сомножителей, но и больше q корней быть не может), которые, как мы доказали, образуют поле.
Таким образом, мы показали, что для любого $q = p^n$ существует поле из q элементов.
Это можно было бы доказать иначе, доказав, что существует неприводимый многочлен любой степени над $\mathbb{F}_p$ для любого p.

Вспомним про гомоморфизм значения:

$$\mathrm{Ev}_\alpha : \mathbb{F}_p[x] \mapsto F \qquad \mathrm{Ev}_\alpha(f) = f(\alpha)$$

где α — элемент конечного поля F характеристики p.
Ядро этого гомоморфизма, как ядро любого гомоморфизма колец, является двусторонним идеалом, а так как мы находимся в евклидовом кольце, то этот идеал порожден одним многочленом.

Определение 3 (Минимальный многочлен)
Многочлен, которым порождено ядро Ev_α, называется *минимальным многочленом* m_α элемента α.

Утверждение 3
Минимальный многочлен неприводим.

Доказательство Пусть $m_\alpha(x) = f(x)g(x)$. Так как $m_\alpha(x)$ лежит в ядре Ev_α (раз уж оно им порождено), то $m_\alpha(\alpha) = 0$. Многочлены — область целостности, поэтому отсюда следует, что $f(\alpha) = 0$ или $g(\alpha) = 0$. То есть, один из сомножителей лежит в ядре Ev_α, то есть делится на m_α. Тогда степень этого сомножителя совпадает со степенью m_α, а степень второго равна нулю. Ну а это значит, что многочлен неприводим.

По теореме о гомоморфизме $\mathbb{F}_p/\mathrm{Ker}\ \mathrm{Ev}_\alpha \cong \mathrm{Im}\ \mathrm{Ev}_\alpha$. Из неприводимости минимального многочлена следует, что это факторкольцо является полем.
Значит, значения всех многочленов $f(\alpha)$ в $\mathbb{F}_p[x]$ образуют подполе поля F. Обозначим его $\mathbb{F}_p(\alpha)$.

Утверждение 4
$\mathbb{F}_p(\alpha)$ — наименьшее подполе поля F, содержащее α.

Доказательство Рассмотрим подполе, содержащее α. Из замкнутости по умножению следует, что оно содержит все степени α^k, а из замнкутости по сложению — все элементы $s\alpha^k$ и их линейные комбинации. Но это совпадает с $\mathbb{F}_p(\alpha)$.

Рассмотрим поле F из $q = p^n$ элементов.
Многочлен $x^q - x = x(x^{q-1} - 1)$ в этом поле раскладывается на линейные множители: второй сомножитель делится на $x - \alpha$ для любого $0 \neq \alpha \in F$, так как из теоремы Лагранжа для мультипликативной группы поля $\alpha^{q-1} = 1$.
Посмотрим на неприводимые делители этого многочлена над полем $\mathbb{F}_p$.

Утверждение 5
Многочлен $x^q - x$ делится на любой неприводимый многочлен $f \in \mathbb{F}_p[x]$ степени n.

Доказательство Рассмотрим неприводимый многочлен $f \in \mathbb{F}_p[x]$ степени n.
Кольцо вычетов $\mathbb{F}_p[x]/(f) = K$ — поле из $q = p^n$ элементов. Рассмотрим минимальный многочлен m_α элемента $\alpha = [x]$ этого поля.
Покажем, что $f \in \mathrm{Ker}\ \mathrm{Ev}_\alpha$:

$$f(\alpha) = \sum f_i \alpha^i = \sum f_i [x^i] = \left[\sum f_i x^i\right] = [f] = [0] \mod (f)$$

Поэтому f делится на m_α. Так как он неприводим, то он равен m_α с точностью до константного множителя.
В поле из q элементов $\alpha^q = \alpha$, поэтому $x^q - x \in \mathrm{Ker}\ \mathrm{Ev}_\alpha = (f)$, то есть $x^q - x \vdots f$, что и требовалось доказать.

Пропустим доказательство пары промежуточных утверждений и сформулируем без доказательства следующую теорему

Теорема 3 (О неприводимых делителях $x^q - x$)
Неприводимые делители многочлена $x^q - x$ в кольце $\mathbb{F}_p[x]$, $q = p^n$ — это в точности те неприводимые многочлены, степени которых делят n.

Задача 3
Делится ли многочлен $x^{1023} - 1$ на $x^4 + x + 1$ в поле характеристики 2?

Решение У обоих многочленов коэффициенты из поля $\mathbb{F}_2$, поэтому если первый многочлен делится на второй, то эта делимость будет выполняться и в $\mathbb{F}_2[x]$.
Но в этом кольце можно применить теорему и получить, что многочлен $x^{1024} - x = x(x^{1023} - 1)$ имеет следующие неприводимые делители — это неприводимые многочлены степени 10, 5, 2, 1 (все делители 10, так как $1024 = 2^{10}$).
Из них многочлен $x^{1023} - 1$ из многочленов степени 1 имеет неприводимый делитель $x + 1$ (так как многочлен x уже есть в разложении). Многочлен $x^4 + x + 1$ неприводим $\mathbb{F}_2[x]$, а степень его равна 4, поэтому делимости нет.

Теорема 4 (Изоморфизм полей с одинаковым количеством элементов)
Пусть F_1, F_2 — поля характеристики p, в каждом из которых $q = p^n$ элементов. Тогда $F_1 \cong F_2$.

Доказательство Любое конечное поле изоморфно факторкольцу по модулю идеала кольца $\mathbb{F}_p[x]$, порожденного неприводимым многочленом. Пусть $F_2 \cong \mathbb{F}_p[x]/(f), \deg f = n$.
Многочлен f неприводим и его степень равна n. Как было сказано ранее, он является делителем многочлена $x^q - x \in \mathbb{F}_p[x]$. Последний раскладывается в поле F_1 (в нем q элементов) на линейные множители. Значит, в F_1 у f есть корень α: $f(\alpha) = 0$.
Как в утверждении 5, убеждаемся, что f является минимальным многочленом элемента α: $f(\alpha) = 0$, поэтому $f \in \operatorname{Ker} \mathrm{Ev}_\alpha = (m_\alpha)$. Отсюда f делится на m_α (уже в кольце $\mathbb{F}_p[x]$).
Но в этом кольце он неприводим, значит, f совпадает с m_α с точностью до константного множителя.
Тогда $\mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(f) \cong F_2$ содержит ровно $p^n = q$ элементов. Это подполе поля F_1, причем $|\mathbb{F}_p(\alpha)| = |F_1|$, значит, они совпадают. Отсюда, $F_2 \cong F_1$.

Итак, конечные поля с одинаковым числом элементов изоморфны друг другу. Поэтому мы можем пользоваться обозначением $\mathbb{F}_{p^n}$, означающим поле с p^n элементов, не уточняя его природу.

Задача 4
Изоморфны ли кольца вычетов $\mathbb{F}_7[x]/(x^2 - 2x + 2)$ и $\mathbb{F}_7[x]/(x^2 + 1)$?

Решение Разложим многочлены на неприводимые множители в $\mathbb{F}_7$. Для этого нужно решить квадратные уравнения в этом поле.
Для $x^2 - 2x + 2$ дискриминант равен $D = 4 - 8 = -4 = 2^2 \cdot (-1)$.
Для $x^2 + 1$ также $D = 0 - 4 = -4 = 2^2 \cdot (-1)$.
$(-1)^{(7-1)/2} = (-1)^3 = -1$, значит, -1 является квадратичным невычетом по модулю 7, значит, и D. Отсюда имеем, что оба многочлена являются неприводимыми, следовательно, оба кольца вычетов являются полями. В каждом из них 7^2 элементов, поэтому они изоморфны.

Задача 5
Построить явно изоморфизм между полями в предыдущей задаче.

Решение Для этого нужно в одном кольце (точнее, поле) найти решение уравнения, задаваемого многочленом, порождающим второе.

Найдем в кольце $\mathbb{F}_7[x]/(x^2-2x+2)$ корень уравнения $t^2+1=0$. Преобразуем порождающий:

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

Здесь нам повезло, что все так красиво преобразуется. Итак, в первом кольце

$$[0]=[x^2-2x+2]=[(x-1)^2+1]=[x-1]^2+[1]$$

Значит, один из корней t^2+1 равен $[x-1]$.
Посмотрим еще раз, что мы сделали с точки зрения доказательства теоремы об изоморфизме. Мы взяли поле $F_2=\mathbb{F}_7[x]/(x^2+1)$, образованное с помощью неприводимого многочлена $f=x^2+1$. У f в $F_1=\mathbb{F}_7[x]/(x^2-2x+2)$ есть корень α, в нашем случае $\alpha=[x-1]$.
Затем мы имеем изоморфизм между F_2 и $\mathbb{F}_p(\alpha)$ — подполем поля F_1, которое представляет собой значения всех многочленов из $\mathbb{F}_p[x]$ в точке α. То есть по сути мы задаем такое отображение:

$$\varphi:\ F_2\mapsto\mathbb{F}_p(\alpha)\cong F_1$$

$$\varphi([1])=[1]\quad\varphi([x])=\alpha$$

В сущности это отображение и задает «подстановку α вместо x».
Таким образом, в нашем случае:

$$\varphi([1])=[1]\quad\varphi([x])=[x-1]$$

Остальные элементы получаются по линейности:

$$\varphi([a+bx])=[a]+[b\,(x-1)]=[(a-b)+bx]$$

Далее мы обсудим автоморфизм Фробениуса. Про него можно говорить долго и много, так как он оказывается полезным при изучении полей в целом. Однако, мы докажем наиболее интересный факт, описывающий все автоморфизмы конечного поля

Определение 4 (Автоморфизм Фробениуса)
Для конечного поля $\mathbb{F}_{p^n}$ отображение $F: x\to x^p$ называется автоморфизмом Фробениуса.

Доказательство Докажем корректность определения. Уважение умножения следует из коммутативности:

$$F(xy)=(xy)^p=x^py^p=F(x)F(y)$$

Уважение сложения следует из бинома двоечника:

$$F(x+y)=(x+y)^p=x^p+y^p=F(x)+F(y)$$

Ядро данного отображения нулевое, так как из того что в поле нет делителей нуля следует:

$$x^p=0\iff x=0$$

А так как поле конечно, то это отображение действительно является автоморфизмом.

Следующее утверждение позволяет лучше понять, как действует автоморфизм Фробениуса.

Лемма 2 (О неподвижных точках)
Если $F(x) = x$, то $x \in \mathbb{F}_p$. Иначе говоря, у автоморфизма Фробениуса есть неподвижные точки и это в точности элементы простого подполя.

Доказательство Условие $F(a) = a$ равносильно тому, что a является корнем многочлена $x^p - x$. Элементы простого поля являются корнями этого многочлена. Других корней нет, так как у многочлена над полем количество корней не превосходит степени.

Теорема 5 (О корнях многочлена)
Пусть $\beta \in \mathbb{F}_{p^n}$ — корень неприводимого в $\mathbb{F}_p[x]$ многочлена $f(x)$ степени n с коэффициентами из $\mathbb{F}_p$. Тогда $\beta, \beta^p \dots \beta^{p^{n-1}}$ все различны и исчерпывают список корней этого многочлена.

Доказательство Вначале докажем, что если β — корень f, то β^p — тоже корень
Поскольку $a^p = a$ для всех $a \in \mathbb{F}_p$ и в силу бинома двоечника, то для любого f с коэфициентами из простого подполя верно $(f(x))^p = f(x^p)$.
Если $f(\beta) = 0$, то $0 = (f(\beta))^p = f(\beta^p)$. Мы доказали, что $\beta, \beta^p \dots \beta^{p^{n-1}}$ — корни этого многочлена. Осталось доказать, что они все различны, тогда из леммы о числе корней многочлена будет следовать, что мы нашли все корни многочлена.
Пусть орбита действия автоморфизма Фробениуса, содержащая β, имеет размер k, то есть $F^k(\beta) = \beta$. Тогда $\beta^{p^k} = \beta$ и потому многочлен $x^{p^k} - x$ делится на многочлен f (минимальный многочлен элемента β). Из теоремы о неприводимых делителях таких многочленов заключаем, что $k = n$, а значит все указанные корни различны.

Теорема 6 (О автоморфизмах конечного поля)
Любой автоморфизм поля $\mathbb{F}_{p^n}$ является композицией автоморфизмов Фробениуса. Иначе говоря, группа автоморфизмов конечного поля циклическая, где автоморфизм Фробениуса является порождающим.

Доказательство Пусть $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ — автоморфизм. Он сохраняет 0 и 1: $\varphi(0) = 0, \varphi(1) = 1$, значит, сохраняет и любую сумму единиц, то есть все элементы простого подполя $\mathbb{F}_p$. Поэтому автоморфизм переводит корень β многочлена f степени n, неприводимого над простым полем, в другой корень:

$$\varphi(0) = \varphi(f(\beta)) = f(\varphi(\beta)) = 0$$

Таким образом, $\varphi(\beta) = F^k(\beta)$. Рассмотрим автоморфизм $\varphi' = (F^{-1})^{\circ k}\,\varphi$. Этот автоморфизм переводит β (а значит и линейные комбинации её степеней с коэфицентами из простого поля) в себя. Но так как $\mathbb{F}_p(\beta) = \mathbb{F}_q$, то это означает, что он сохраняет все элементы этого поля, а значит он тождественный, а значит $\varphi = F^k$.