Семинар №8 по курсу «Основы высшей алгебры и теории кодирования»

Репеев Роман, Шиманогов Игорь

Определение 1 (Тело)
Телом называется кольцо с единицей $1 \neq 0$, в котором ненулевые элементы образуют группу по умножению.

Определение 2 (Поле)
Полем называется коммутативное тело (умножение коммутативно).
Подытожим определение поля. Поле — это множество F с двумя определенными на нем операциями (обозначаем $+$ и $\cdot$), удовлетворяющее свойствам:

1°. Относительно сложения F образует группу с нейтральным элементом 0

2°. Относительно умножения $F^* = F/\{0\}$ образует группу с нейтральным элементом 1

3°. Дистрибутивность: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

4°. $0 \neq 1$

Замечание 1
В принципе, аксиоматически требовать $0 \neq 1$ *необязательно, так как* 1 *является элементом* F^**, в котором нет нуля. Но это отдельно подчеркивается. В принципе, множество из одного элемента вполне себе могло бы быть полем (здесь* $0 = 1$*), но это неинтересный случай, который в нашем курсе не называется полем.*

Поля хороши тем, что в них можно делить. Таким образом, мы можем решать линейные уравнения $ax + b = 0$ (и далеко не только).

Определение 3 (Простые поля)
К простым полям относятся:

1. $\langle \mathbb{Q}, +, \cdot \rangle$ — рациональные числа с операциями сложения и умножения
2. Вычеты по модулю простого числа $\mathbb{Z}/(p)$. Мы также будем обозначать их $\mathbb{F}_p$

Лемма 1
Всякое поле содержит простое подполе.
Простые поля не содержат собственных подполей.

Напомним, что такое область целостности. В нашем курсе под этим подразумевается *коммутативное кольцо с единицей без делителей нуля.*
Первые пункты следуют напрямую из определения. А так как ненулевые элементы все являются обратимыми, то

Утверждение 1
Всякое поле является областью целостности, в частности, в нем нет делителей нуля.

Рассмотрим произвольное поле, возьмем в нем аддитивную подгруппу, порожденную единицей $\langle 1 \rangle$. Это называют группой *кратных единицы.*

Определение 4 (Характеристика поля)
Если порядок группы кратных единицы в поле F конечен и равен p, то *характеристика* поля $\operatorname{char} F = p$.
Если порядок группы кратных единицы бесконечен, то $\operatorname{char} F = 0$.

Из отсутствия в поле делителей нуля следует, что если характеристика поля ненулевая, то это всегда **простое число**.
Более того, забегая вперед, порядок любого конечного поля равен p^n, где p — характеристика поля.
Продемонстрируем особенность работы с полями на примере простой леммы, которая понадобится нам позже.

Лемма 2 («Равенство двоечника»)
В поле с характеристикой $p > 0$ выполняется

$$(a+b)^p = a^p + b^p$$

Доказательство

$$(a+b)^p = a^p + b^p + \sum_{n=1}^{p-1} \binom{p}{n} a^n b^{p-n}$$

Отметим, что умножение на числа здесь — это не умножение на элементы поля, а «умножение» в смысле аддитивной записи. Тем не менее, мы можем записать (здесь 1 — это единица поля)

$$\underbrace{a + \cdots + a}_{n \text{ раз}} = \underbrace{(1 + \cdots + 1)}_{n \text{ раз}} a = \overline{n} a$$

где $\overline{n}$ — число n в группе $\langle 1 \rangle$, то есть «умножение» совпадает с настоящим умножением на

элемент поля, входящий в $\langle 1 \rangle$.
Для любого слагаемого в сумме

$$\binom{p}{n} = \frac{p \cdot (p-1)!}{n!(p-n)!}$$

Так как p — простое число, а в знаменателе все сомножители меньше p, то $\binom{p}{n}$ будет делиться на p, а значит, равняться нулю в нашем поле.
Таким образом, $(a+b)^p = a^p + b^p$, ч.т.д.

Теорема 1
Коммутативное кольцо R с $0 \neq 1$ является полем тогда и только тогда, когда оно не содержит собственных идеалов (отличных от R и $\{0\}$).

Определение 5 (Максимальный идеал)
Идеал I кольца R называется *максимальным*, если он не содержится строго ни в каком собственном идеале, то есть для идеала J выполняется $I \subsetneq J \Rightarrow J = R$.

Теорема 2 (О максимальном идеале)
Факторкольцо R/I коммутативного кольца R с $1 \neq 0$ является полем тогда и только тогда, когда I — макисмальный идеал.

Определение 6 (Кольцо многочленов)
Пусть R — коммутативное кольцо с единицей. *Кольцо многочленов* $R[x]$ состоит из всех *финитных* последовательностей $(f_0, f_1, \dots, f_n, 0, \dots)$ элементов кольца R (то есть таких, где начиная с какого-то момента все элементы нулевые).

Определение 7 (Степень многочлена)
Для ненулевого многочлена наибольшее число d такое, что $f_d \neq 0$, называется *степенью* многочлена $\deg f = d$.
Для нулевого многочлена степень не определена (иногда для удобства полагают $\deg 0 = -\infty$).

Мы не будем вдаваться в тонкости различий между многочленами в данном определении и *функций, представимых многочленами*. Но стоит помнить, что многочлен суть последовательность коэффициентов, поэтому, например, может возникнуть ситуация, когда различные многочлены задают одну и ту же функцию (пример 7.50 в учебнике).
Операции сложения и умножения многочленов задаются естественным образом.

Нас, в основном, будут интересовать многочлены с коэффициентами из полей. Это удобно по многим причинам. Например, чтобы использовать алгоритм Евклида (и вообще делить многочлены с остатком), нужно делить на старший коэффициент в делителе (а значит, это деление должно быть определено).
Тем не менее, для многих вещей достаточно, чтобы кольцо, над которым определен многочлен было целостным. В предыдущем примере с делением, например, делить на многочлен $x - a$ (с единичным старшим коэффициентом) можно в любом кольце.

Теорема 3 (Логарифмическое свойство степени)
Если R — область целостности, то для любых многочленов $f, g \neq 0$ выполняется

$$\deg(fg) = \deg f + \deg g$$

Доказательство Это связано с тем, что коэффициент при старшей степени $f_{\deg f} \cdot g_{\deg g}$ не обращается в ноль.

Для колец многочленов над полем $F[x]$ работает деление с остатком, поэтому кольца многочленов над полем являются евклидовыми (с нормой равной степени многочлена).

Утверждение 2
Остаток от деления многочлена f на $x - a$ равен $f(a)$.

Это известный из школы и дегко доказуемый факт. На нем основывается важная лемма.

Лемма 3 (О числе корней многочлена)
Количество корней ненулевого многочлена $f \in F[x]$ над полем F не превосходит $\deg f$.

Замечание 2
Стоит отметить, что доказательство строится на предыдущем утверждении, поэтому требование, чтобы F было полем слишком сильное. Напомним, что делить на $x - a$ можно не только в поле. Поэтому основным опорным фактом является отсутствие делителей нуля, так что утверждение остается справедливым, если F — область целостности.

Пример 1
Если F не является областью целостности, то утверждение может быть неверным. Например, многочлен второй степени $x^2 - 1$ имеет в кольце $\mathbb{Z}/(8)$ четыре корня: $\pm 1, \pm 3$.

Вернемся к многочленам над полем. В поле разрешимо единственным образом любое линейное уравнение. Следующим шагом будет решение квадратных уравнений.
Для этого введем одно понятие.

Определение 8
Квадратичным вычетом в поле $\mathbb{Z}/(p)$ по простому модулю p называется такое a, что

$$\exists x : \quad a^2 \equiv x \mod p$$

В противном случае a называется квадратичным невычетом.

Теорема 4 (Критерий квадратичного вычета)
Элемент $a \in \mathbb{Z}/(p)$ является квадратичным вычетом тогда и только тогда, когда

$$a^{(p-1)/2} \equiv 1 \mod p$$

Замечание 3
Стоит отметить, что $\left(a^{(p-1)/2}\right)^2 = a^{p-1} \equiv 1 \mod p$*, согласно малой теореме Ферма, поэтому* $a^{(p-1)/2} \equiv \pm 1 \mod p$.
То есть все вычеты в степени $\frac{p-1}{2}$ *равны* 1*, а все невычеты —* -1.

Итак, квадратичный вычет — это элемент, который является квадратом какого-то элемента.

Рассмотрим квадратное уравнение $ax^2 + bx + c = 0 \Leftrightarrow ax^2 + bx = -c$
Умножим каждую часть на $4a$ и прибавим b^2:

$$4a^2x^2 + 4abx + b^2 = -4ac + b^2$$

Обозначим $-4ac + b^2 = D$, тогда

$$(2ax + b)^2 = D$$

Здесь встает вопрос, является ли дискриминант квадратичным вычетом. Если нет, то у данного уравнения нет решений, а так как все преобразования были равносильными, то и у изначального.
Если же да, то обозначим $\sqrt{D}$ один из корней. Всего корней многочлена $t^2 - D$ не больше двух, поэтому без ограничения общности будем считать, что их два: $\pm\sqrt{D}$ (либо они будут совпадать).
Итак, если D является квадратичным вычетом, то

$$2ax + b = \pm\sqrt{D} \Leftrightarrow 2ax = -b \pm \sqrt{D}$$

Дальше хотелось бы разделить на $2a$. Это, конечно же, можно сделать, но только если мы не будем делить на ноль. $a \neq 0$, так как иначе уравнение не было бы квадратным, а вот с двойкой интереснее: мы можем делить на 2, если $\operatorname{char} F \neq 2$. На самом деле, если бы характеристика поля была равна 2, то уже умножение на $4a$ в начале не имело бы смысла: мы бы умножали на ноль.
Итак, мы доказали

Утверждение 3
В поле $F, \operatorname{char} F \neq 2$ корни квадратного уравнения $ax^2+bx+c = 0$ находятся по классической формуле

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Замечание 4
На самом деле, при $\operatorname{char} F > 2$ *характеристика будет нечетной, поэтому если* $D \neq 0$ *(в случае нулевого дискриминанта понятно, что* $\sqrt{D} = 0$ *и только), то* $\pm\sqrt{D}$ *не могут совпадать, так как у них должна быть разная четность.*