27 Поля Галуа и их применение в компьютерных сетях

Множество G называют группой если для него определена бинарная операция * и:

1. Операция * является ассоциативной: $(a * b) * c = a * (b * c)$ -- соответствует умножению.
2. Существует нейтральный элемент -- соответствует единице.
3. Имеется унарная операция, позволяющая получить обратный элементу a элемент -- соответствует a^{-1}.

Группу называют *абелевой* если операция * коммутативна: $a * b = b * a$.

Если для группы определена операция умножения ($a * b = ab$), то группу называют *мультипликативной*.

Мультипликативную группу называют *циклической* если в ней существует такой элемент, что все остальные элементы являются степенями этого элемента: $b = a^k$. А сам элемент a называют *образующим* группу.

Множество R называют *кольцом* если для множества определены две бинарные операции # и * такие что:

1. Множество R является абелевой группой относительно операции # -- соответствует сложению.
2. Операция * является ассоциативной.
3. Выполняется закон дистрибутивности: $a * (b \# c) = a * b \# a * c$.

Если для группы определена операция *сложения* ($a \# b = a + b$), то группу называют *аддитивной*. Единичный элемент аддитивной группы соответствует нулю. Обратный элементу a элемент аддитивной группы соответствует $-a$.

На операцию * можно накладывать дополнительные ограничения. Если в кольце присутствует единица, то кольцо называют *кольцом с единицей*.

При выполнении закона коммутативности кольцо называют *коммутативным*.

Коммутативное кольцо называют *целостным* если его единица не равна нулю и $a * b = 0$ только при $a = 0$ или $b = 0$.

Кольцо называют *телом* если кроме нуля в кольце существуют другие элементы и эти элементы образуют группу относительно операции *.

Наконец, коммутативное тело F называют *полем*.

Подгруппой, *подкольцом*, *подполем* называют подмножества сохраняющие соответствующие свойства.

Поле, не содержащее подполей, называют *простым*. Простым будет поле, порядок которого равен простому числу.

Подкольцо *I* кольца *R* называют его *идеалом* (*двухсторонним идеалом*) если для любой пары элементов *a* из *I* и *r* из *R* их произведение принадлежит *I*.

Подкольцо *R*/*I* классов вычетов по модулю идеала *I* из кольца *R* называют *факторкольцом* кольца *R* по идеалу *I*.

Наименьшее из натуральных чисел *n*, такое что для любого элемента *r* из кольца *R* выполняется равенство *n* * *r* = 0, называют *характеристикой* кольца *R*.

Согласно теореме, каждое конечное целостное кольцо образует поле.

Согласно другой теореме, характеристикой конечного поля является простое число.

Поле *GF*(*p*) из целых чисел 0, 1 ... *p* - 1, порожденное в результате отображения *f*: **Z**/*p* -> *GF*(*p*), где **Z**/*p* -- факторкольцо множества целых чисел, в котором роль идеала играет простое число *p*, и *f*([*a*]) = *a*, называют *полем Галуа* (Galois field) порядка *p*.

При вычислениях с элементами поля Галуа используют целочисленную арифметику с приведением по соответствующему модулю.

В помехоустойчивом кодировании очень важное место занимают поля Галуа.

В помехоустойчивом кодировании все операции выполняются по, так называемой, арифметике Галуа. Т.е. результатом любой арифметической операции будет являться элемент из данного поля. Поля задаются целым числом. Пример: GF (Galua field) от 5 будет равно: GF(5) = 0, 1, 2, 3, 4. Пример сложения: 0 + 1 = 1, 4 + 1 = 0, 4 + 3 = 2. Умножение: 4 * 2 = 3. И т.д. (операции делаем по модулю).

Для бинарных же векторов арифметика намного сложнее. Сложение тут будет представляться операцией xor GF(4): (1 + 1 = 0, 2 + 2 = 0, 3+1=2). Умножение – умножением полиномы GF(8): (например, 5 = 101 = x^2 * 1 + x * 0 + 1 * 1, 7 = 111 = x^2 * 1 + x * 1 + 1 * 1. 5 * 7 = (x^2 + 1) * (x^2 + x + 1) = x^4 + x^3 + x^2 + x^2 + x + 1 = x^4 + x^3 + x + 1 = 11011 = 27). x^2 + x^2 складываются по xor (получается 0). Далее, так как результат не входит в используемое поле, необходимо использовать порождающий полином (выбирается самостоятельно). В качестве полинома используется неприводимое (простое) число. Используем x^3 + x + 1 = 1011 = 11. Вернёмся к умножению. Теперь складываем порождающий полином и результат умножения (всё ещё по модулю): (x^4 + x^3 + x + 1) + (x^3 + x + 1) = x^4.

Деление можно представить, как умножение полинома-делимого на полином, обратный делителю.

Источник лекция 4

https://github.com/IvanGrigorik/BSUIR_labs/blob/main/5_term/TOKS/Exam/Answers.pdf