**Множества с двумя алгебраическими операциями кольца и поля**

Предположим, что существует множество R, на котором расположены две алгебраические операции: сложение и умножение.

Принято считать, что умножение имеет свойство правой дистрибутивности по отношению к сложению:

.

И соответственно сложение имеет свойство левой дистрибутивности по отношению к умножению. В случае, если операция умножения коммутативна, тогда данные свойства равнозначны.

Применяя свойства дистрибутивности, подразумеваем двустороннюю дистрибутивность.

Допустим, операция сложения на множестве R имеет нейтральный элемент, т. е. 0.

Приравняв у и z к нулю, получим: x \* 0 = x \* 0 + x \* 0, владея свойством сокращения для операции сложения, получаем, что x \* 0 = 0.

В случае наличия у элемента y противоположный элемент, т. е. отрицательный, приравняв z к (-y), получим: 0 = x \* 0 = x \* y + x \*(-y), отсюда следует, x \*(-y) = -x \* y.

Полем называется такое ассоциативное коммутативное кольцо с единицей k, в котором всякий ненулевой элемент обратим: .

Таким образом, по определению в поле отсутствуют делители нуля.

Кольцом называется множество с двумя алгебраическими операциями R (+, \*), если:

 0.

Обратимыми называют те элементы кольца R, которые имеют обратные относительно операции умножения, множество R в данном случае обозначается через .

Множество является группой по умножению, называемой мультипликативной группой кольца R для ассоциативного кольца с единицей.

Умножение в R дистрибутивно относительно сложения.

Ассоциативное кольцо — это кольцо, в котором операция умножения обладает свойством ассоциативности.

Кольцо с единицей — наличие нейтрального элемента для операции умножения.

(R, +) — абелева группа (аддитивная группа кольца R).

Приведем некоторые примеры колец и полей.

Допустим R — любое ассоциативное коммутативное кольцо и x — некоторый символ. Формальная сумма вида p = , где называется многочленом над кольцом R.

Нулевой многочлен не имеет степени. Многочлены над R можно складывать и перемножать по обычным правилам, и они образуют кольцо R [x]. Если кольцо R имеет единицу е, то многочлен нулевой степени p = e будет единицей кольца R [x]. Если , то число n называется степенью этого многочлена и обозначается deg (p).

Если R не имеет делителей нуля, то deg (pq) = deg (p) + deg (q), и потому R [x] также не имеет делителей нуля. В то же время обратимыми элементами кольца многочленов будут в точности обратимые элементы R, рассматриваемые как многочлены нулевой степени.

Данная конструкция позволяет рассматривать и многочлены от нескольких переменных по определению: R [x,y] = R [x][y] (= R [y][x]).

Аддитивная группа этого кольца — хорошо известная нам бесконечная циклическая группа. Мультипликативная группа содержит всего 2 элемента — 1 и -1 — и потому изоморфна .

Множество Z целых чисел с операциями сложения и умножения дает важный пример ассоциативного коммутативного кольца с единицей. Элементы, не входящие в , необратимы, хотя и не являются делителями нуля.

Рассмотрим поля R, Q, и C соответственно вещественных, рациональных и комплексных чисел.

Построенное поле из двух элементов обозначается GF (2).

Если p — простое число, то все вычеты по модулю p, кроме 0, обратимы относительно операции умножения. Любое поле содержит по крайней мере 2 элемента: 0 и e. Этот «минимальный» запас элементов и достаточен для образования поля: операции определяются очевидным образом.

Рассматривая группу с дополнительной операцией умножения, мы получаем поле из p элементов, которое обозначается GF (p).

Будем считать, что R является ассоциативным коммутативным кольцом. Кольцо матриц ассоциативно, но, вообще говоря, не коммутативно.

Множество квадратных матриц порядка n с элементами из кольца R образует кольцо относительно операций сложения и умножения матриц.

Если det (A) — обратимый элемент кольца R, то матрица A обратима в кольце матриц: , где — присоединенная к А матрица.

Если R содержит единицу , то матрица Е = diag (, ,..., ) будет единицей кольца матриц.

Для любой матрицы имеет смысл понятие определителя det (A) R, причем det (AB) = det (A) det (B).

 = — группа матриц порядка n с обратимым определителем. Любая вырожденная матрица будет делителем нуля. В случае поля R это означает, что det (A) 0, то есть матрица невырождена.

В самом деле, из det (A) = 0 следует, что столбцы А линейно зависимы: , причем не все коэффициенты нулевые.

А \* В = 0, где А является делителем нуля в том случае, если В — ненулевая матрица.

Подкольцо кольца с единицей может не иметь единицы. Например, подкольцо четных чисел 2 Z Z не имеет единицы. Более того, может случиться, что и R, и K имеют единицы, но они не равны друг другу.

Например, для подкольца , состоящего из матриц с нулевой последней строкой и последним столбцом, = diag (1,1,...,1,0) = diag (1,1,...,1).

Допустим, — некоторое подкольцо. К, + — подгруппа коммутативной группы R,+, можно образовать факторгруппу R / K, элементами которой являются смежные классы r + K.

Поскольку К \* К К, для произведения двух смежных классов имеет место включение: (r + K) \* (s + K) r \* s + r \* K + K \* s + K.

Подкольцо К называется идеалом кольца R, если : x \* K K и K \* y K.

Мы видим, что если К является идеалом в R, произведение смежных классов (r + K) \* (s + K) содержится в смежном классе r \* s + K. Значит, в факторгруппе R / K определена операция умножения, превращающая ее в кольцо, называемое факторкольцом кольца R по идеалу К.

Подкольцом является подмножество , если оно является кольцом относительно тех же операций, которые определены в R.

Согласно данной интерпретации, К является подгруппой аддитивной группы R и замкнуто относительно умножения: .

К будет обладать свойствами ассоциативности, коммутативности или отсутствием делителей нуля, если R обладает такими свойствами.

Отображение, сохраняющее обе кольцевые операции: и называется гомоморфизмом колец .

Пусть — сюръективный гомоморфизм колец. Тогда S изоморфно факторкольцу R / Ker. Если эти изоморфные кольца отождествить, то отождествляется с естественным гомоморфизмом кольца R на свое факторкольцо.

Ядро группового гомоморфизма аддитивных групп называется ядром гомоморфизма . Ядро гомоморфизма колец является идеалом.

Пусть — гомоморфизм колец, I = Ker , — любой элемент. Тогда, (x \* I) = (x) \* (I) = (x) \* 0 = 0. Значит, x \* I Ker = I.

Аналогично проверяется, что I \* x I.

Взаимно однозначный гомоморфизм является изоморфизмом.

Отсутствие в R делителей нуля еще не гарантирует их отсутствие в факторкольце. Такие свойства как ассоциативность, коммутативность и наличие единицы сохраняются при переходе к факторкольцу

Приведем примеры.

Всякий ненулевой идеал I в S совпадает со всем полем, если кольцо S является полем. В самом деле, если , x 0, то для всякого имеем: , откуда .

Если любой его элемент, то множество I = x \* S является идеалом кольца S, называемым главным идеалом с образующим элементом x.

Этот идеал обозначается (x). Если S кольцо с единицей и элемент x обратим, то (x) = S.

Факторкольцо Z / nZ — это множество вычетов по модулю n с операциями сложения и умножения. Идеалом кольца Z является подкольцо nZ, так как для любого целого m m (nZ) nZ. Если число n не является простым, то Z / nZ имеет делители нуля.

Допустим, что I — идеал кольца R. Тогда, соотнося каждому элементу смежный класс r + I, получаем сюръективный гомоморфизм , который называется естественным гомоморфизмом кольца на факторкольцо.

Предположим, что I R [x] является множество всех многочленов , у которых = 0. Тогда I = xR [x]. Так как p \* I = (p \* x) R [x] I, значит, получаем идеал кольца многочленов.

Каждый смежный класс q + I содержит элемент , поэтому (q + I) \* (s + I) = (+ I) \* (+ I) = \* + I.

