Кольца.

Предупреждение. Этот текст НЕ является записью лекции! Здесь лишь собраны наиболее употребительные определения и теоремы, а также приведены несколько упражнений на понимание определений. (Так будет и дальше; в дальнейших hand-out'ах этот текст повторяться не будет.)

Определение 1. Множество R с двумя бинарными операциями $a, b \mapsto a + b$ («сложение») и $a, b \mapsto a \cdot b$ («умножение») называется *кольцом*, если оно образует группу по сложению (обратный элемент обозначают $(-a)$, нейтральный элемент — 0), а умножение связано со сложением свойством *дистрибутивности*: $a(b + c) = ab + ac$, $(a+b)c = ac+bc$ (мы пропускаем точку между сомножителями). Если есть нейтральный элемент и по умножению, то его обычно обозначают 1, а кольцо называют *кольцом с единицей*. Если умножение коммутативно (ассоциативно), то кольцо называется *коммутативным (ассоциативным)*.

Определение 2. Кольцо F называется *телом*, если $(F \setminus 0, \cdot)$ — группа. Если эта группа коммутативна, то F называется *полем*.

Определение 3. Кольцо R называется *целостным*, если из $a, b \in R$, $ab = 0$ следует, что один из элементов a, b нулевой. («Отсутствие делителей нуля.»)

Упражнение 1. Любое тело является целостным кольцом.

Упражнение 2. В любом кольце для всех элементов x верно равенство $0 \cdot x = x \cdot 0 = 0$.

Примеры. $\mathbb{Z}$, $\mathbb{Z}/N\mathbb{Z}$ — коммутативные ассоциативные кольца с единицей (первое — целостное, а второе — не всегда). $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — поля.

Если R — кольцо, то многочлены с коэффициентами в R образуют кольцо, которое обозначается $R[x]$. Степенны́е ряды с коэффициентами в R тоже образуют кольцо (степенной ряд с коэффициентами в R — выражение $\sum_{n\geqslant 0} r_n x^n$, $r_n \in R$; сложение и умножение определяются очевидным образом); это кольцо обозначается $R[[x]]$.

Рациональные функции одной переменной — отношения многочленов с (скажем) комплексными коэффициентами — образуют поле, которое обозначается $\mathbb{C}(x)$. Многочлены Лорана (многочлены от x, x^{-1}) образуют кольцо, а ряды Лорана (ряды с комплексными коэффициентами, где позволяется конечное число отрицательных степеней) — поле (проверьте!). Это поле обозначается $\mathbb{C}((x))$; также используется более наглядное обозначение $\mathbb{C}[[x, x^{-1}]$.

В поле комплексных чисел можно рассмотреть элементы с рациональной (целой) вещественной и мнимой частями; такие элементы называются гауссовыми числами (соотв. целыми гауссовыми числами), множество таких элементов обозначается $\mathbb{Q}[i]$ ($\mathbb{Z}[i]$).

Если рассмотреть множество $\mathbb{Q}[I]$, где $I^2 = 1$, т. е. множество выражений вида $a+bI$, $a, b \in \mathbb{Q}$, с «покоординатным» сложением и умножением $(a+bI)(c+dI) = (ac+bd)+(ad+bc)I$, то получится кольцо, но не поле: $(1-I)(1+I) = 0$. Наоборот, $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ — поле.

Функции $f\colon [0,1] \to \mathbb{R}$ образуют кольцо, которое не является целостным.

Кватернионы (выражения $a + bi + cj + dk$, $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$) образуют тело, которое обозначается $\mathbb{H}$.

Множество $\{0, x\}$ со сложением $x + x = 0$ и умножением $x^2 = 0$ образует коммутативное ассоциативное кольцо без единицы.

Множество векторов в пространстве с операциями сложения и векторного произведения образуют некоммутативное неассоциативное кольцо без единицы (это пример «кольца Ли»).

Определение 4. Элемент a коммутативного кольца R делится на элемент b этого кольца, если $a = bc, c \in R$.

Определение 5. Элемент a кольца R называется *простым (неразложимым)*, если из $a = bc, b, c \in R$ следует, что один из элементов b, c обратим (по умножению).

Определение 6. Коммутативное кольцо называется *фактори-*

альным, если любой его элемент может быть разложен на простые сомножители, причём единственным образом с точностью до перестановки сомножителей и умножения на обратимые элементы кольца.

Пример 1. Кольцо $\mathbb{Z}$ факториально (обобщение этого факта будет сформулировано ниже). Кольцо $\mathbb{Z}[i\sqrt{3}]$ не факториально: в нём $4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$. (Чтобы доказать простоту всех этих чисел, можно использовать *норму* $N(a+bi\sqrt{3}) = a^2+3b^2$, для которой $N(xy) = N(x)N(y)$.)

Определение 7. Пусть A — коммутативное ассоциативное кольцо с единицей. Подмножество $I \subset A$ называется *идеалом*, если оно является подгруппой по сложению, и для любых $a \in A, b \in I$ элемент ab принадлежит I.

Пример 2. $\{0\}$ и A — идеалы (их называют тривиальными идеалами кольца). Если $a_1, a_2, \ldots, a_n \in A$, то $(a_1, a_2, \ldots, a_n) = \{a_1r_1 + a_2r_2 + \ldots + a_nr_n \mid r_i \in A\}$ — идеал («идеал, порождённый элементами a_i»).

Определение 8. Идеал, порождённый одним элементом, называется *главным*. Кольцо называется *кольцом главных идеалов*, если все идеалы в нём главные.

Определение 9. Кольцо R называется *евклидовым*, если для некоторой функции $N\colon R \setminus 0 \to \mathbb{N}$ имеет место «возможность делить с остатком»: для любых a, b существует c: $a = bc$ или $N(a - bc) < N(b)$.

Пример 3. Кольцо $\mathbb{Z}$ — кольцо главных идеалов. (Это следует из приведённой ниже теоремы.) Кольцо $\mathbb{Z}[x]$ не является кольцом главных идеалов (чем бы был порождён идеал $(2, x)$?).

Пример 4. Кольца $\mathbb{Z}$ и $F[x]$ (F — поле) евклидовы. (Функция N равна абсолютной величине в первом случае и степени во втором.)

Теорема 1. Любое евклидово кольцо — кольцо главных идеалов. (Любой идеал порождён таким своим элементом, на котором функция N достигает минимума.)

Теорема 2. Если в кольце главных идеалов R произведение ab делится на простой элемент p, то один из элементов a, b делится на p.

(Ясно, что иначе $(a, p) = (1)$, поэтому $ax + py = 1$ для некоторых $x, y \in R$, откуда $b = abx + pby$ делится на p.)

Теорема 3. Каждый элемент кольца главных идеалов можно разложить на простые множители. (Рассмотрим элемент a_1, для которого это не так. Он не простой, поэтому его можно разложить в произведение двух необратимых элементов. Для одного из них (обозначим его a_2) тоже не должно быть разложения и т. д. Получаем бесконечную строго возрастающую цепочку идеалов

$$(a_1) \subsetneq (a_2) \subsetneq \ldots \subsetneq (a_n) \subsetneq \ldots$$

Объединение этих идеалов — идеал. Рассмотрим элемент, которым он порождён. Но тогда этот элемент лежит в одном из идеалов (a_i), что противоречит строгому возрастанию цепочки идеалов.)

Из двух последних теорем легко следует

Теорема 4. Целостное кольцо главных идеалов факториально.

Упражнение 3. Докажите, что условие целостности здесь существенно (иными словами, приведите пример нецелостного нефакториального кольца главных идеалов).