§1. Коммутативные кольца и поля.

1.1. Определения. Множество $\mathbb{F}$ называется *полем*, если на нём заданы две бинарных операции

$$\mathbb{F} \times \mathbb{F} \longrightarrow \mathbb{F} \ :$$

сложение $(a,b) \longmapsto a+b$ и умножение $(a,b) \longmapsto ab$ со свойствами:

1) аксиомы сложения

   а) коммутативность (переместительный закон): $a+b=b+a \quad \forall\, a,b\in\mathbb{F}$

   б) ассоциативность (сочетательный закон): $a+(b+c)=(a+b)+c \quad \forall\, a,b,c\in\mathbb{F}$

   в) существование нейтрального элемента (нуля): $\exists\, 0\in\mathbb{F}: \quad a=0=a \quad \forall\, a\in\mathbb{F}$

   г) существование противоположного: $\forall\, a\in\mathbb{F} \quad \exists\,(-a)\in\mathbb{F}: \quad a+(-a)=0$

2) аксиомы умножения

   а) коммутативность: $ab=ba \quad \forall\, a,b\in\mathbb{F}$

   б) ассоциативность: $a(bc)=(ab)c \quad \forall\, a,b,c\in\mathbb{F}$

   в) существование нейтрального элемента (единицы): $\exists\, 1\in\mathbb{F}: \quad a\cdot 1=a \quad \forall\, a\in\mathbb{F}$

   г) существование обратного: $\forall\, a\in\mathbb{F},\ a\neq 0 \quad \exists\, a^{-1}\in\mathbb{F}: \quad a\cdot a^{-1}=1$

3) аксиома дистрибутивности (распределительный закон): $a(b+c)=ab+ac \quad \forall\, a,b\in\mathbb{F}$

4) аксиома нетривиальности: $0\neq 1$

Эти аксиомы формализуют хорошо известные свойства сложения и умножения чисел в полях $\mathbb{Q}$ и $\mathbb{R}$. Множество A с одной операцией $A\times A \longrightarrow A$, удовлетворяющей четырём аксиомам сложения, называется *абелевой группой*, и первые два набора аксиом утверждают, что всякое поле $\mathbb{F}$ является абелевой группой относительно сложения, а множество $\mathbb{F}^*$ всех ненулевых элементов $\mathbb{F}$ является абелевой группой относительно умножения. Последние две аксиомы регулируют взаймодействие этих двух структур между собой.

Упражнение 1.1. Убедитесь, что требование $a\neq 0$ в аксиоме 2г необходимо, т.к. нуль не может иметь обратного в силу остальных аксиом, а также проверьте, что равенство $0\neq 1$ равносильно требованию $\mathbb{F}\neq\{0\}$.

Множество K с двумя операциями, удовлетворяющими всем аксиомам поля, за исключением аксиом существования обратного элемента, существования единицы и нетривиальности, называется *коммутативным кольцом*. Если в кольце имеется $1\neq 0$, то K называется коммутативным кольцом *с единицей*. Важнейшим отличием кольца от поля является невозможность деления. Фундаментальными примерами колец являются кольцо целых числа $\mathbb{Z}$ и кольцо многочленов. Чётные числа $2\,\mathbb{Z}\subset\mathbb{Z}$ доставляют типичный пример кольца без единицы.

Целый ряд привычных свойств сложения и умножения чисел и многочленов формально вытекает из предыдущих аксиом.

Упражнение 1.2. Покажите, что в любом коммутативном кольце нуль единственен, и единица, если существует, тоже единственна. Покажите, что противоположный и обратный элементы $(-a)$, a^{-1} всегда определяются по a однозначно (если существуют), а также что $0\cdot a=0$, и $(-1)\cdot a=(-a)$.

1.1.1. Пример: комплексные числа. Будем называть *комплексным числом* радиус-вектор точки на плоскости $\mathbb{C}$ с фиксированной декартовой системой координат XOY. Всякое комплексное число $z=(x,y)$ имеет *модуль* $|z|=\sqrt{x^2+y^2}$ и *аргумент* $\operatorname{Arg}(z)$ — ориентированную длину дуги, которую надо пройти по единичной окружности от точки $(1,0)$, задающей направление оси OX, до точки $z/|z|$, задающей направление радиус-вектора z (подчеркнём, что аргумент определён не однозначно, а лишь с точностью до любого целого числа оборотов). Операции над комплексными числами определяются следующим образом: сложение — это обычное сложение векторов на плоскости, а умножение — это умножение модулей с одновременным сложением аргументов. Таким образом, всякое комплексное число имеет вид

$z = x \cdot 1 + y \cdot i = x + iy$, где $i = (1, 0)$ — это базисный орт оси OY, и умножение всех точек плоскости на такое число представляет собой поворотную гомотетию с центром в нуле на угол $\operatorname{Arg}(z)$ и растяжением в $|z|$ раз.

Упражнение 1.3. Проверьте выполнение всех аксиом поля и убедитесь, что ограничение сложения и умножения комплексных чисел на ось OX задают на этой оси обычные сложение и умножение точек вещественной числовой прямой.

То обстоятельство, что комплексные числа образуют поле, и с ними можно алгебраически манипулировать по обычным правилам раскрытия скобок, имеет много замечательных последствий. Например, поскольку комплексное число z с модулем 1 и аргументом φ имеет вид $z = \cos\varphi + i\,\sin\varphi$, то перемножая два таких числа, получаем:

$$\begin{aligned}\cos(\varphi_1 + \varphi_2) + i\,\sin(\varphi_1 + \varphi_2) = z_1 z_2 = (\cos\varphi_1 + i\,\sin\varphi_1)(\cos\varphi_2 + i\,\sin\varphi_2) = \\ = (\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2) + i\,(\cos\varphi_1\sin\varphi_2 + \sin\varphi_1\cos\varphi_2)\ ,\end{aligned}$$

что даёт известные «формулы сложения аргументов[1]».

Упражнение 1.4. Раскрывая скобки у $\cos(n\varphi) + i\,\sin(n\varphi) = z^n = (\cos\varphi + i\,\sin\varphi)^n$ выразите $\cos(n\varphi)$ и $\sin(n\varphi)$ через $\cos\varphi$ и $\sin\varphi$.

Упражнение 1.5. Покажите, что $\sin(n\varphi)/\sin\varphi$ является при нечётном n многочленом от $\sin^2\varphi$. Найдите корни этого многочлена и его старший коэффициент.

Упражнение 1.6. Как переводится на тригонометрический язык формула суммирования геометрической прогрессии $1 + z + z^2 + \cdots + z^n$?

1.1.2. Пример: кольцо вычетов $\mathbb{Z}/n\mathbb{Z}$. Элементом этого кольца является *класс вычетов* по модулю n, т. е. подмножество в $\mathbb{Z}$, состояшее из всех чисел, дающих фиксированный остаток от деления на n. Всего имеется n таких классов. Сложение и умножение классов вычетов индуцируется сложением и умножением в кольце $\mathbb{Z}$: если обозначить через $[a]$ класс, состоящий из всех чисел вида $a + nx$ (где x пробегает $\mathbb{Z}$), то, по определению,

$$[a] + [b] \stackrel{\text{def}}{=} [a + b] \qquad\qquad [a] \cdot [b] \stackrel{\text{def}}{=} [ab]\ .$$

Упражнение 1.7. Проверьте корректность этого определения, т. е. независимость классов $[a+b]$ и $[ab]$ от выбора представителей $a \in [a]$ и $b \in [b]$, и проверьте выполнение в $\mathbb{Z}/n\mathbb{Z}$ всех аксиом коммутативного кольца.

В кольцах $\mathbb{Z}/n\mathbb{Z}$ наблюдается целый спектр явлений, отличающих кольца от полей. Например, в кольце $\mathbb{Z}/10\mathbb{Z}$ произведение классов $[2]$ и $[5]$ равно нулю, хотя каждый из них отличен от нуля, а в кольце $\mathbb{Z}/9\mathbb{Z}$ ненулевой класс $[3]$ имеет нулевой квадрат. Ненулевой элемент a кольца K называется *делителем нуля*, если $ab = 0$ для некоторого ненулевого $b \in K$. Ненулевой элемент a кольца K называется *нильпотентом*, если $a^n = 0$ для некоторого $n \in \mathbb{N}$. Кольцо с единицей и без делителей нуля называется *целостным*.

Упражнение 1.8. Составьте таблицы сложения и умножения в кольце $\mathbb{Z}/n\mathbb{Z}$ для $n = 3, 4, 5, 6, 7, 8$. Найдите в этих кольцах все делители нуля, все нильпотенты, и все обратимые элементы. Для обратимых элементов составьте таблицу обратных. Какие из этих колец являются полями?

Чтобы выяснить при каких n кольцо $\mathbb{Z}/n\mathbb{Z}$ является полем, достаточно понять, при каких n все ненулевые вычеты по модулю n обратимы. Число a обратимо по модулю n тогда и только тогда, когда уравнение

$$ax + ny = 1 \qquad (1\text{-}1)$$

разрешимо в целых числах. Совокупность $I = I(a, n)$ всех чисел вида $ax + ny$ (с фиксированными a, n и произвольными x, $y \in \mathbb{Z}$) образует кольцо, и вместе с каждым числом содержит также и все его кратные. Поэтому остаток от деления любого $b \in I$ на любое $d \in I$ также лежит в I, а стало быть, наименьшее положительное $d \in I$ делит все числа из I нацело. Таким образом, $I = d\mathbb{Z}$ состоит из всех чисел, кратных d. В частности, d является общим делителем a и n и нацело делится на любой другой общий делитель чисел a и n. Итак, уравнение (1-1) разрешимо тогда и только тогда, когда $d = \text{нод}(a, n) = 1$. При фиксированном n это равенство выполняется для всех a некратных n, если и только если n простое. При простом p поле $\mathbb{Z}/p\mathbb{Z}$ обозначается $\mathbb{F}_p$.

[1] вообще вся школьная тригонометрия — это лишь изощрённый способ записи обычных действий над многочленами от точки z, лежащей на единичной окружности

1.1.3. Пример: кольцо формальных степенных рядов. Пусть K — коммутативное кольцо с единицей. Кольцо формальных степенных рядов $K[[t]]$ состоит из бесконечных формальных выражений вида

$$A(t) = a_0 + a_1 t + a_2 t^2 + \cdots ,$$

сложение и умножение которых определяется стандартными правилами раскрытия скобок и приведения подобных слагаемых: коэффициенты при t^m у суммы $S(t) = A(t)+B(t) = s_0+s_1t+s_2t^2+\cdots$ и произведения $P(t) = A(t)B(t) = p_0 + p_1 t + p_2 t^2 + \cdots$ рядов $A(t) = \sum a_\nu t^\nu$ и $B(t) = \sum b_\mu t^\mu$ вычисляются по правилам

$$\begin{aligned} s_\nu &= a_\nu + b_\nu \\ p_\nu &= \sum_{\alpha+\beta=\nu} a_\alpha b_\beta = a_0 b_\nu + a_1 b_{\nu-1} + \cdots + a_0 b_\nu \end{aligned} \tag{1-2}$$

Говоря формально, эти правила задают операции на *множестве последовательностей* (a_ν), (b_ν), и буква t служит лишь для удобства интерпретации формул (1-2). Начальный коэффициент a_0 называется *свободным членом*. Первый ненулевой коэффициент ряда называется *младшим*. Заметим, что когда в K нет делителей нуля, младший коэффициент произведения двух рядов в точности равен произведению младших коэффициентов сомножителей. В частности, кольцо формальных степенных рядов с коэффициентами из целостного кольца само является целостным.

Упражнение 1.9. Проверьте, что обратимыми элементами в $K[[t]]$ являются в точности ряды с обратимым свободным членом, и вычислите ряды, обратные к рядам $1-t$ и $1+t+t^2$.

Кольцо формальных степенных рядов от нескольких переменных определяется по индукции:

$$K[[t_1, t_2, \dots , t_n]] = K[[t_1, t_2, \dots , t_{n-1}]]\,[[t_n]]$$

и представляет собой множество формальных сумм вида $F(t) = a_0 + \sum\limits_{\nu_1,\dots,\nu_n \in \mathbb{N}} a_{\nu_1\dots\nu_n} t_1^{\nu_1} t_2^{\nu_2} \cdots t_n^{\nu_n}$.

1.1.4. Пример: кольцо многочленов. В условиях предыдущего примера, кольцо многочленов $K[t] \subset K[[t]]$ определяется как подкольцо, состоящее из всех рядов с конечным числом ненулевых коэффициентов. Последний ненулевой коэффициент многочлена f называется *старшим*, а его номер называется *степенью* f и обозначается $\deg f$. Если кольцо K целостное, то старший коэффициент произведения будет, как и младший, равен произведению старших коэффициентов сомножителей. Поэтому степень произведения всегда равна сумме степеней. В частности, обратимыми элементами кольца многочленов являются только обратимые константы. Многочлен f называется *неприводимым*, если равенство $f = gh$ возможно только когда один из множителей g, h является обратимой константой.

Упражнение 1.10 (деление с остатком). Пусть $f \in K[t]$ имеет обратимый старший коэффициент. Покажите, что любой многочлен $g \in K[t]$ представляется в виде $g = qf + r$, где $q, r \in K[t]$ и либо $\deg r < \deg f$, либо $r = 0$.

Важным отличием многочленов от формальных рядов является возможность подставлять в многочлен вместо формальной переменной элементы из K. Число $a \in K$ называется *корнем* многочлена $f(t)$, если $f(a) = 0$. Согласно упр. 1.10, при любом $a \in K$ каждый многочлен $f \in K[t]$ можно представить в виде $f(t) = q(t)(t-a) + r$, где $\deg r = 0$, т. е. $r \in K$. Подставляя $t = a$, получаем, что $r = g(a)$. В частности, a тогда и только тогда является корнем f, когда f делится в $K[t]$ на $(t-a)$.

Упражнение 1.11. Пусть K — поле. Покажите, что:

а) многочлен $f \in K[t]$, имеющий своими корнями набор попарно различных чисел $a_1, a_2, \dots, a_m \in K$, делится в $K[t]$ на $\prod\limits_{\nu=1}^{m} (t - a_\nu)$;

б) всякий многочлен f положительной степени имеет не более $\deg f$ корней.

1.1.5. Пример: алгебраические числа. Алгебраическими числами называются выражения вида

$$a_0 + a_1\vartheta + \cdots + a_{n-1}\vartheta^{n-1} , \tag{1-3}$$

в которых $a_\nu \in \mathbb{Q}$, а ϑ предполагается удовлетворяющим некоторому фиксированному полиномиальному уравнению n-ой степени $f(\vartheta) = 0$ с рациональными коэффициентами. Совокупность таких чисел обозначается $\mathbb{Q}[\vartheta]$. Действия над ними производятся по формальным правилам раскрытия скобок с учётом соотношения $f(\vartheta)=0$. Так, например, сложение и умножение в $\mathbb{Q}[\sqrt{2}]\overset{\text{def}}{=}\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\,,\ \vartheta^2-2=0\}$ происходит по формулам

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}$$
$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2\,bd)+(cb+ad)\sqrt{2}$$

Упражнение 1.12. Проверьте, что $\mathbb{Q}[\sqrt{2}]$ является полем.

Упражнение 1.13. Будет $\mathbb{Q}[\vartheta]$ полем, когда ϑ задаётся уравнениями: а) $\vartheta^3+1=0$ б) $\vartheta^3+2=0$.

Более формально, кольцо $\mathbb{Q}[\vartheta]$ можно определить как кольцо классов вычетов $\mathbb{Q}[t]/f\cdot\mathbb{Q}[t]$ (ср. с примером из n° 1.1.2). Элементом такого кольца является множество всех многочленов $g\in\mathbb{Q}[t]$, имеющих одинаковый фиксированный остаток от деления на f, а сложение и умножение индуцируется сложением и умножением $\mathbb{Q}[t]$: если обозначать через $[g]$ класс, состоящий из всех многочленов вида $g+fq$ (где q пробегает $\mathbb{Q}[t]$), то

$$[g]+[h]\overset{\text{def}}{=}[g+h]\qquad\qquad [g]\cdot[h]\overset{\text{def}}{=}[gh]\,.$$

Упражнение 1.14. Проверьте независимость классов $[g+h]$, $[gh]$ от выбора представителей $g\in[g]$, $h\in[h]$, а также выполнение в $\mathbb{Q}[t]/f\mathbb{Q}[t]$ всех аксиом коммутативного кольца с единицей.

В этих терминах алгебраическое число ϑ представляет собой класс $[t]$, а выражение (1-3) есть класс многочлена $a_0+a_1t+\ \cdots\ +a_{n-1}t^{n-1}$. Мы можем заменить $\mathbb{Q}$ на произвольное коммутативное кольцо K с единицей и для каждого многочлена $f\in K[t]$ определить *алгебраическое расширение* $K[\vartheta]\overset{\text{def}}{=}K[t]/f\cdot K[t]$. Исходное кольцо K вкладывается в $K[t]$ как классы констант, а ϑ обозначает класс вычетов $[t]$, содержащий t. Отметим, что по построению ϑ является корнем многочлена f. Например, поле комплексных чисел представляет собой квадратичное расширение $\mathbb{C}=\mathbb{R}[\sqrt{-1}]=\mathbb{R}[t]/(t^2+1)\mathbb{R}[t]$, а $i=\sqrt{-1}$ есть класс t по модулю t^2+1.

Упражнение 1.15. Пусть K — поле. Используя те же рассуждения, что и в примере n° 1.1.2, покажите, что кольцо алгебраических чисел $K[t]/f\cdot K[t]$ является полем тогда и только тогда, когда многочлен f неприводим.

1.1.6. Пример: кольца функций. Пусть K — коммутативное кольцо, а X — произвольное множество. Множество всех K-значных функций на X обозначается K^X и образует кольцо относительно операций поточечного сложения и умножения значений функций:

$$f+g: x\mapsto f(x)+g(x)$$
$$fg: x\mapsto f(x)g(x)\,.$$

Тождественно нулевая функция является в K^X нулём, а тождественно единичная (если в K есть единица) — единицей. Иначе K^X можно воспринимать как *прямое произведение* семейства копий кольца K, занумерованных элементами $x\in X$. Если множество X состоит из n элементов, то вместо K^X обычно пишут K^n и изображают элементы такого кольца «координатными строчками» $(a_1,a_2,\dots,a_n)$. Сложение и умножение таких строк производится покоординатно.

Поскольку произведение любых двух функций с непересекающимися носителями[2] равно нулю, в кольце K^X много делителей нуля, даже если K — поле. Обратимыми элементами K^X являются функции, принимающие обратимое значение в каждой точке.

В геометрии и анализе часто рассматриваются различные подкольца колец $\mathbb{R}^X$ и $\mathbb{C}^X$: непрерывные, гладкие, аналитические, алгебраические, интегрируемые и т. п. функции.

1.1.7. Пример: прямые суммы колец. Обобщая предыдущий пример, мы можем из любого семейства колец K_ν (где ν пробегает произвольное множество индексов X) образовать кольцо $\prod K_\nu$, элементами которого являются всевозможные наборы (x_ν) с $x_\nu\in K_\nu$, а сложение и умножение определяется покоординатно. Это кольцо называется *прямым произведением* колец K_ν и может восприниматься как множество «функций»на X, имеющих в каждой точке $\nu\in X$ свою «область значений»K_ν. Прямое произведение конечного набора колец $K_1,K_2,\dots,K_n$ обычно обозначается через $K_1\times K_2\times\ \cdots\ \times K_n$.

Упражнение 1.16. Постройте изоморфизм[3] $\mathbb{Z}/6\,\mathbb{Z}\simeq\mathbb{Z}/2\,\mathbb{Z}\times\mathbb{Z}/3\,\mathbb{Z}$.

[2] *носителем* функции $X\xrightarrow{f}K$ называется множество $\mathrm{Supp}(f)=\{x\in X\mid f(x)\neq 0\}$.

[3] точное определение см. ниже

1.2. Гомомрфизмы. Отображение колец $A \xrightarrow{\varphi} B$ называется *гомоморфизмом*, если $\forall\, a_1, a_2 \in A$ в кольце B выполнены соотношения:

$$f(a_1 + a_2) = f(a_1) + f(a_2)$$
$$f(a_1 a_2) = f(a_1) f(a_2)$$

Взаимно-однозначные гомоморфизмы называются *изоморфизмами*. Гомоморфизмы, являющиеся вложениями, часто называют *мономорфизмами* или *инъективными* морфизмами. Гомоморфизмы, которые являются отображениями «на», часто называют *эпиморфизмами* или *сюрьективными* морфизмами. Гомоморфизм, отображающий все элементы из A в нуль кольца B называется *нулевым*. Вообще $\varphi(A) \subset B$ всегда является подкольцом в B, а полный прообраз нуля $\varphi^{-1}(0) \subset A$ — подкольцом в A. Они называются, соответственно, *образом* и *ядром* гомоморфизма φ и обозначаются $\operatorname{im}\varphi \overset{\text{def}}{=} \varphi(A)$ и $\ker\varphi \overset{\text{def}}{=} \varphi^{-1}(0)$.

Упражнение 1.17. Проверьте, что $\varphi(0) = 0$ и $\varphi(-a) = -\varphi(a)\ \forall\ a$ при любом гомоморфизме колец $A \xrightarrow{\varphi} B$. Покажите, что при ненулевом гомоморфизме колец с единицей, вообще говоря, $\varphi(1) \neq 1$, но когда в B нет делителей нуля, единица всегда переходит в единицу.

Упражнение 1.18. Проверьте, что всякий ненулевой гомоморфизм из любого поля в любое кольцо инъективен.

1.2.1. Пример: гомоморфизмы поднятия и вычисления. С каждым отображением множеств $X \xrightarrow{\varphi} Y$ связан *гомоморфизм поднятия* (или *гомоморфизм обратного образа*[4])

$$\varphi^* \,:\, K^Y \xrightarrow{f \mapsto f\circ\varphi} K^X$$

между кольцами функций на X и Y со значениями в произвольном коммутативном кольце K. Он действует в направлении, противоположном к φ, и если в кольце K есть единица, то он переводит единицу кольца K^Y в единицу кольца K^X.

В геометрии и анализе, где множества X и Y наделяются дополнительной структурой (мерой, топологией, структурой вещественного, комплексного или алгебраического многообразия и т. п.), функции и отображения тоже рассматриваются не любые, а согласованные с этой структурой.

С алгебраической точки зрения, наделение множества X дополнительной структурой означает выбор в кольце K^X специального подкольца $K[X] \subset K^X$, называемого *структурным кольцом* (или *кольцом регулярных функций*) соответствующей теории. Например, это может быть кольцо измеримых, или непрерывных, или гладких, или голоморфных, или рациональных функций. Такие подкольца, например, в $\mathbb{R}^X$, можно, вообще говоря, задавать и абстрактно, при помощи тех или иных алгебраических свойств, даже и не апеллирующих к геометрии. После чего возникает теория, в которой *регулярными отображениями* пространств $X \xrightarrow{\varphi} Y$ следует, по определению, считать такие, для которых $K^Y \xrightarrow{\varphi^*} K^X$ переводит подкольцо регулярных функций $K[Y] \subset K^Y$ на Y в подкольцо регулярных функций $K[X] \subset K^X$ на X.

Упражнение 1.19. Проверьте, что такое алгебраическое определение регулярного отображения согласуется с непосредственным определением регулярности в известных Вам теориях. Например, отображение топологических пространств (или множеств с мерой) непрерывно (соотв. измеримо) тогда и только тогда, когда его композиция с любой непрерывной (соотв. измеримой) функцией является непрерывной (соотв. измеримой) функцией.

Упражнение 1.20. Из каких функций состоит ядро гомоморфизма подъёма? Проверьте, что инъективность гомоморфизма подъёма непрерывных функций $C^0(Y) \xrightarrow{\varphi^*} C^0(X)$ относительно непрерывного отображения топологических пространств $X \xrightarrow{\varphi} Y$ равносильна тому, что $\varphi(X)$ всюду плотно в Y.

В случае, когда $X = \{*\}$ состоит из одной точки, гомоморфизм поднятия, отвечающий вложению

$$\{*\} \overset{y}{\hookrightarrow} Y$$

этой точки в качестве некой точки $y \in Y$, называется *гомоморфизмом вычисления* в точке y и обозначается ev_y. Поскольку $K^{\{*\}} = K$,

$$\operatorname{ev}_y \,:\, K^Y \xrightarrow{f \mapsto f(y)} K$$

[4]по-английски *pull back*

действительно сопоставляет каждой функции $Y \xrightarrow{f} K$ её значение $\mathrm{ev}_y(f) = f(y)$ в точке y. Гомоморфизм ev_y всегда эпиморфен, а его ядро состоит из всех функций, обращающихся в нуль в точке y.

Гомоморфизмы вычисления дают возможность чисто алгебраически восстанавливать точки пространства X из кольца $K[X]$ регулярных функций. А именно, мы можем по определению называть K-точкой кольца A с единицей всякий гомоморфизм $A \xrightarrow{p} K$, переводящий единицу в единицу. Более того, каждому гомоморфизму колец $B \xrightarrow{\varphi^*} A$ можно сопоставить отображение из множества K-точек B в множество K-точек A, переводящее K-точку $B \xrightarrow{p} K$ в K-точку $\varphi(p) = p \circ \varphi^*$ кольца A, т. е. интерпретируя отображение точек тоже как *подъём* относительно φ^*.

Упражнение 1.21. Имеется ли биекция между точками отрезка $[\,0\,,\,1\,]$ и $\mathbb{R}$-точками кольца непрерывных функций на этом отрезке? Изменится ли ответ, если заменить отрезок на полуинтервал? Изменятся ли ответы, если заменить непрерывные функции а) на гладкие б) на полиномиальные?

В анализе имеются и другие примеры гомоморфизмов вычисления. Например, для некоторых формальных рядов из $\mathbb{C}[[t]]$ (называемых *сходящимися*) можно определить их значение в точке $z \in \mathbb{C}$. Подчеркнём, что это определение не является алгебраическим, ибо не сводится к выполнению конечного числа арифметических действий, а требует перехода к пределу. И утверждения о том, что абсолютно сходящиеся ряды образуют кольцо, а отображения ev_z являются $\mathbb{C}$-точками этого кольца, суть нетривиальные теоремы из анализа, а не из алгебры. Однако, буде эти теоремы доказаны, мы можем утверждать, что все формальные алгебраические тождества в кольце $\mathbb{C}[[t]]$ при применении к сходящимся рядам дадут соответствующие тождества для чисел в $\mathbb{C}$.

1.2.2. Пример: простое подполе, характеристика и гомоморфизм Фробениуса. Для любого кольца с единицей K имеется канонический гомоморфизм $\mathbb{Z} \xrightarrow{c} K$, переводящий единицу в единицу. Для произвольного $n \in \mathbb{N}$

$$c(\pm n) = \pm(\underbrace{1 + 1 + \cdots + 1}_{n}) .$$

Если c инъективен, то говорят, что K имеет *характеристику нуль*, в противном случае *характеристикой* называют наименьшее натуральное число, лежащее в ядре c.

Упражнение 1.22. Покажите, что если K — поле положительной характеристики p, то p — простое число, и образ $c(\mathbb{Z})$ изоморфен $\mathbb{F}_p$.

В условиях последней задачи, $\mathbb{F}_p = c(\mathbb{Z}) \subset K$ называется *простым подполем*. Поскольку при простом p все биномиальные коэффициенты $\binom{p}{k} \equiv 0 \pmod{p}$ при $k \neq 1, p$, отображение $x \mapsto x^p$ в любом поле характеристики p переводит суммы в суммы: $(x_1 + x_2)^p = x_1^p + x_2^p$, а значит, является гомоморфизмом. Он называется *гомоморфизмом Фробениуса*. На простом подполе гомоморфизм Фробениуса действует тождественно, так как для любого элемента a из простого подполя

$$a^p = (\underbrace{1 + 1 + \cdots + 1}_{a})^p = \underbrace{1^p + 1^p + \cdots + 1^p}_{a} = a$$

(это наблюдение известно как *малая теорема Ферма*).

Упражнение 1.23. Покажите, что кольца $\mathbb{F}_2[\vartheta]$ и $\mathbb{F}_3[\vartheta]$, где $\vartheta^2 + \vartheta - 1 = 0$, являются полями. Выясните, какова характеристика этих полей, из скольких элементов они состоят, и опишите, как действует на них гомоморфизм Фробениуса.

1.3. Факторизация, идеалы и структура гомоморфизмов. Конструкции колец $\mathbb{Z}/n\mathbb{Z}$ и $K[\vartheta] = K[t]/f(t)K[t]$ являются частными случаями общей конструкции, называемой *факторизацией* (или *склейкой*). Из любого множества M можно получать новые множества M', склеивая вместе некоторые элементы. При этом возникает эпиморфное *отображение факторизации*

$$M \xrightarrow{\pi} M' , \tag{1-4}$$

и прообразы элементов $m' \in M'$ задают разбиение множества M в объединение непересекающихся подмножеств:

$$M = \bigsqcup_{m' \in M'} \pi^{-1}(m')$$

Если писать $m_1 \sim m_2$ для тех элементов из M, которые склеваются вместе отображением π, то мы получим на множестве M *бинарное отношение*, которое

$$(\textit{рефлексивно}): \quad m \sim m \quad \forall\, m \in M \tag{1-5}$$
$$(\textit{симметрично}): \quad m_1 \sim m_2 \Longleftrightarrow m_2 \sim m_1 \quad \forall\, m_1, m_2 \in M \tag{1-6}$$
$$(\textit{транзитивно}): \quad m_1 \sim m_2 \;\&\; m_2 \sim m_3 \Rightarrow m_1 \sim m_3 \quad \forall\, m_1, m_2, m_3 \in M \tag{1-7}$$

Рефлексивные симметричные транзитивные бинарные отношения[5] называются *отношениями эквивалентности*.

Упражнение 1.24. Убедитесь, что всякое отношение эквивалентности определяет разбиение множества M в объединение непересекающихся классов, состоящих из попарно эквивалентных элементов, так что склеивая все эквивалентные элементы друг с другом, мы получим отображение (1-4), где M' будет множеством классов эквивалентности.

Если M является кольцом, то можно попытаться наделять его фактор множества M' структурой кольца, индуцированной с M, т. е. задавая операции над классами эквивалентности по тем же правилам, что и в примерах n° 1.1.2, n° 1.1.5:

$$\pi(a) + \pi(b) \stackrel{\text{def}}{=} \pi(a+b)\ , \quad \pi(a)\pi(b) \stackrel{\text{def}}{=} \pi(ab)\ .$$

Иначе говоря, мы хотим задать на M' структуру кольца так, чтобы отображение факторизации (1-4) было гомоморфизмом.

Упражнение 1.25. Убедитесь, что в этом случае:

а) класс $\pi^{-1}(0) = \ker(\pi)$ обязан быть подкольцом в M и вместе с каждым элементом a должен содержать также и все его кратные ma (с произвольными $m \in M$)

б) $m_1 \sim m_2$ тогда и только тогда, когда $m_1 - m_2 \in \ker(\pi)$

Подкольцо I коммутативного кольца K называется *идеалом*, если $a \in I \Rightarrow ba \in I \;\; \forall\, b \in K$. Таким образом, если на фактор множестве кольца K индуцируется структура коммутативного кольца, то класс эквивалентности нуля представляет собою некоторый идеал $I \subset K$, а все остальные классы эквивалентности получаются из него аддитивными сдвигами, т. е. имеют вид

$$[b] = b + I = \{b + a \mid a \text{ пробегает } I\}\ . \tag{1-8}$$

На самом деле эти ограничения на склейку не только необходимы, но и достаточны для того, чтобы фактор множество кольца K наследовало с K кольцевую структуру.

Упражнение 1.26. Убедитесь, что сдвиги любого идеала $I \subset K$ на произвольные элементы кольца либо не пересекаются, либо совпадают, так что подмножества (1-8) задают разбиение K в объединение непересекающихся классов эквивалентности.

Классы (1-8) назывются *смежными классами* или *классами вычетов* по модулю идеала I и иногда обозначаются через $b\,(\mathrm{mod}\, I)$. Множество всех классов вычетов обозначается через K/I и называется фактор кольцом K по идеалу I. Сложение и умножение классов в K/I определяется правилами

$$[a] + [b] \stackrel{\text{def}}{=} [a+b] \qquad\qquad [a]\cdot[b] \stackrel{\text{def}}{=} [ab]\ .$$

Упражнение 1.27. Проверьте корректность этого определения, т. е. независимость классов $[a+b]$ и $[ab]$ от выбора представителей $a \in [a]$ и $b \in [b]$.

Гомоморфизм $\pi_I : K \xrightarrow{a \mapsto [a]} K/I$ называется *гомоморфизмом факторизации* по идеалу I. В действительности, наши рассуждения доказывают

1.3.1. ПРЕДЛОЖЕНИЕ. *Ядро произвольного гомоморфизма колец $K \xrightarrow{\varphi} L$ является идеалом в K, и $K/\ker\varphi = \operatorname{im}\varphi$. В частности, всякий эпиморфизм колец является гомоморфизмом факторизации по ядру, а произвольный гомоморфизм колец распадается в композицию эпиморфизма*

[5] т. е. абстрактные наборы упорядоченных пар $(m_1, m_2) \in M \times M$, удовлетворяющие свойствам (1-5)–(1-7)

факторизации по ядру и вложения образа:

$$\begin{tikzcd} K \arrow[rr, "\varphi"] \arrow[dr, two heads, "\pi"'] & & L \\ & K/\ker\varphi = \operatorname{im}\varphi \arrow[ur, hook, "\iota"'] & \end{tikzcd}$$

□

В любом кольце K имеются *тривиальные* идеалы $I = \{0\}$ и $I = K$.

Упражнение 1.28. Покажите, что ненулевой идеал в кольце с единицей тогда и только тогда совпадает со всем кольцом, когда он содержит единицу.

1.3.2. ПРЕДЛОЖЕНИЕ. *Коммутативное кольцо K с единицей тогда и только тогда является полем, когда в нём нет нетривиальных идеалов.*

Доказательство. Если K поле, $I \subset K$ — идеал, и $b \in I$ отличен от нуля, то $1 = b^{-1}b \in I$, и значит $I = K$. Наоборот, для каждого $b \in K$ множество

$$(b) \overset{\text{def}}{=} bK = \{bc \mid c \in K\} \tag{1-9}$$

сотавляет идеал в K, ненулевой, если $b \neq 0$. Если в K нет нетривиальных идеалов, $(b) = K$. В частности, $1 \in (b)$, т. е. $bc = 1$ для некоторого c. □

1.3.3. Пример: области главных идеалов и евклидовы кольца. Идеалы вида (1-9) называются *главными*. Целостное кольцо с единицей, все идеалы которого главные, называется *областью главных идеалов*. Например, кольцо $\mathbb{Z}$ и кольцо многочленов от одной переменной с коэффициентами в произвольном поле являются областями главных идеалов. В самом деле, в этих кольцах можно делить с остатком, и всякий идеал I вместе с любыми двумя элементами $a, d \in I$ будет содержать и остаток от деления a на d. Беря в качестве d наименьшее натуральное число (соответств. ненулевой многочлен наименьшей степени) из I, мы видим, что все элементы из I должны нацело разделиться на d, т. е. $I = (d)$. Это рассуждение дословно переносится и на ряд других важных для приложений колец.

Целостное кольцо K с единицей называется *евклидовым*, если на нём существует *евклидова норма* (или *высота*) — функция $K \setminus \{0\} \xrightarrow{\nu} \mathbb{Z}_{\geqslant 0}$, такая что для любых ненулевых $a, b \in K$ выполняется соотношение $\nu(ab) \geqslant \nu(a)$ и имеются $q, r \in K$ (зависящие от a, b), такие что $a = bq + r$ и либо $r = 0$, либо $\nu(r) < \nu(b)$.

В кольце $\mathbb{Z}$ высотой служит абсолютная величина, в кольце $K[t]$ (где K — поле) высотой служит степень многочлена.

Упражнение 1.29. Покажите, что кольца $\mathbb{Z}[i] \overset{\text{def}}{=} \{a + bi \in \ \mid a, b \in \mathbb{Z},\ i^2 = -1\}$ и $\mathbb{Z}[\omega] \overset{\text{def}}{=} \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z},\ \omega^2 + \omega + 1 = 0\}$ являются евклидовыми относительно высоты $\nu(z) = |z|^2$.

Упражнение 1.30. Покажите, что в любом евклидовом кольце $\nu(ab) = \nu(a)$ тогда и только тогда, когда b обратим.

Упражнение 1.31. Покажите, что всякое евклидово кольцо является областью главных идеалов.

Отметим, что обратное неверно (правда, первые примеры областей главных идеалов, не являющихся евклидовыми кольцами, встречаются только в довольно продвинутой теории чисел и/или алгебраической геометрии, так что для полноценной работы с ними требуется некая техника[6]).

[6]впрочем, см. замечание 3 на стр. 365 в книге *Э. Б. Винберг. Курс алгебры.* М. «Факториал»(1999).