Лекция 2
Коммутативные кольца

▷Определение и примеры коммутативных колец ▷Факторизация ▷Идеалы ▷НОД, взаимная простота и идеалы в кольце $\mathbb{Z}$ ▷Поле $\mathbb{Z}/p\mathbb{Z}$ ▷Определение и примеры гомоморфизмов колец ▷Простое подполе и характеристика ▷Гомоморфизм Фробениуса и малая теорема Ферма ▷Теорема о структуре гомоморфизма ▷Прямые суммы колец ▷Китайская теорема об остатках

§1. Определение и примеры коммутативных колец

1.1. Коммутативное кольцо с единицей — это множество A, на котором заданы две бинарные операции (сложение и умножение), которые удовлетворяют всем аксиомам поля (см. Опр.1.2 лекции 1) кроме аксиомы нетривиальности (4) и аксиомы существования обратного элемента (2г).

Выкидывая аксиому (4), мы допускаем в качестве колец *тривиальные кольца*, состоящие из одного нуля. Это делается исключительно ради формального удобства некоторых предстоящих в дальнейшем построений. Напротив, отсутствие обратных элементов является важным существенным отличием колец от полей: *деление* в кольце возможно не всегда, и поэтому между элементами кольца возникает новое нетривиальное отношение — они могут делиться или не делиться друг на друга.

Как и в прошлой лекции, к определению автоматически прилагается целый ряд дополнительных свойств операций:

> Задача 2.1. Докажите, что в любом кольце выполнены следующие свойства сложения и умножения (ср. с Пр.1.2.2):
> а) ноль единственен;
> б) противоположный элемент единственен;
> в) $0 \cdot a = 0 \quad \forall a \in A$;
> г) $(-1) \cdot a = (-a)$;
> д) единица единственна.

1.1.1. Несколько новых понятий. Нетривиальность деления принуждает к введению новых названий для тех явлений, которые не были заметны в рамках полей.

Элемент a кольца A назывется *обратимым*, если существует элемент $a^{-1} \in A : \ a \cdot a^{-1} = 1$ (в поле все ненулевые элементы были обратимы). Множество обратимых элементов кольца A обозначается A_* и называется *мультипликативной группой* кольца A или *группой обратимых элементов*.

Ненулевой элемент a кольца A называется *делителем нуля*, если существует ненулевой элемент $b \in A$, такой что $ab = 0$ (в поле такого не бывает, поскольку умножив обе части последнего равенства на b^{-1}, получим $a = 0$). Кольцо без делителей нуля называется *целостным*.

Ненулевой элемент a называется *нильпотентным*, если $a^n = 0$ для некоторого натурального n. Разумеется, все нильпотенты автоматически являются делителями нуля (и в поле отсутсутствуют).

Задача 2.2. Докажите, что обратимый элемент не может быть делителем нуля, и что если обратный элемент существует, то единственен.

Задача 2.3. Докажите, что делители нуля не могут быть обратимы.

Рассмотрим некоторые примеры колец,

1.2. Кольцо $\mathbb{Z}$ целых чисел — простейший нетривиальный пример кольца. Это кольцо замечательно тем, что "не содержит ничего лишнего": нуль 0, единица 1, противоположный к единице элемент -1 и всевозможные их суммы (чуть позже мы увидим, что $\mathbb{Z}$ — не единственное кольцо с такими свойствами). Обратимыми элементами в $\mathbb{Z}$ являются только 1 и -1. Кольцо $\mathbb{Z}$ является целостностным.

1.3. Расширения $\mathbb{Q}[\vartheta]$ поля $\mathbb{Q}$, рассматривавшиеся в n° 1.5.2 лекции 1, все являются коммутативными кольцами вне зависимости от соотношения, которому удовлетворяет ϑ. Более того, аксиомы кольца останутся выполненными, если заменить $\mathbb{Q}$ на произвольное коммутативное кольцо. Один пример (восходящий к Гауссу) здесь заслуживает особого внимания.

1.4. Гауссовы целые числа $\mathbb{Z}[i] = \{x + iy \in \mathbb{C} | \ x, y \in \mathbb{Z}\}$ составляют целостное (как и всякое подкольцо в поле) подкольцо в $\mathbb{C}$. Обратимых элементов в $\mathbb{Z}[i]$ роно четыре: 1, -1, i, $-i$ (почему?). Геометрически $\mathbb{Z}[i]$ изображается целочисленной решёткой на комплексной плоскости.

Кольцо $\mathbb{Z}[i]$ имеет много приложений в арифметике. Например, оно играет важную роль в задаче об описании целых чисел, представимых в виде суммы двух квадратов. Дело в том, что квадратичная форма $x^2 + y^2$ над $\mathbb{Z}[i]$ разлагается в произведение двух линейных множителей: $x^2 + y^2 = (x + iy)(x - iy)$, и задача представления натурального числа в виде суммы квадратов двух целых чисел оказывается равносильной задаче о разложимости натурального числа как элемента $\mathbb{Z}[i]$ в произведение двух комплексно-сопряженных множителей, также лежащих в $\mathbb{Z}[i]$.

При таком подходе задача сильно проясняется. Скажем, если число m разложено в произведение $m = m_1 m_2$, и оба сомножителя m_1, m_2 представимы в виде суммы квадратов двух целых чисел, то и m представимо: равенства

$$m_1 = a_1^2 + b_1^2 \qquad \text{и} \qquad m_2 = a_2^2 + b_2^2$$

означают, что $m_1 = z_1 \bar{z}_1$, $m_2 = z_2 \bar{z}_2$ (где $z_\nu = a_\nu + b_\nu \in \mathbb{Z}[i]$), а значит

$$m = (z_1 z_2)\overline{(z_1 z_2)} = |z_1 z_2|^2 = (a_1 b_1 - a_2 b_2)^2 + (a_1 b_2 + a_2 b_1)^2$$

Если доказать для кольца $\mathbb{Z}[i]$ аналог *основной теоремы арифметики* (что будет сделано на следующей лекции), то это вычисление полностью сводит исходную задачу к исследованию того, какие *простые* натуральные числа остаются простыми и в $\mathbb{Z}[i]$.

К сожалению, недостаток времени вынуждает меня здесь прервать дальнейшее обсуждение этой проблемы, но настойчивый заинтересовавшийся читатель сможет разобраться в ней до конца, решив следующие две (не являющиеся обязательными для понимания дальнейшего и довольно трудные) задачи[1]:

Задача 2.4. Докажите, что для представимости числа $n \in \mathbb{N}$ в виде суммы двух квадратов целых чисел (ноль тоже разрешается в качестве одного из двух квадратов!) необходимо и достаточно, чтобы это число имело вид

$$n = p_1 \cdot p_2 \cdot \cdots \cdot p_s \cdot k^2 ,$$

где $k \in \mathbb{Z}$ — любое, а $p_1, \ldots, p_s$ — натуральные простые числа, представимые в виде суммы двух квадратов.

Задача 2.5. Докажите, что простое $p \in \mathbb{N}$ тогда и только тогда представимо в виде суммы двух квадратов, когда имеет вид $p = 4d + 1$ (т. е. имеет остаток 1 от деления на 4).

1.5. Кольцо $k[x]$ многочленов над полем k. Это кольцо состоит из *формальных выражений* вида

$$P(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n,$$

где $a_\nu \in k$, k — поле, $n \in \mathbb{N}$, а x — *формальный символ*, называемый *переменной*. Подчеркну, что с точки зрения кольцевой структуры мы рассматриваем многочлены лишь как слова, и содержательную информацию для нас будет нести лишь последовательность символов[2] $(a_0, a_1, a_2, \ldots, a_n)$.

1.5.1. Определение сложения и умножения. При описании операций, удобно считать, что многочлен есть *бесконечное* вправо выражение $a_0 + a_1 x + a_2 x^2 + \cdots$, в котором, однако, лишь конечное число коэффициентов a_ν *отлично от нуля*. Тогда сумму и произведение многочленов

$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots \qquad \text{и} \qquad B(x) = b_0 + b_1 x + b_2 x^2 + \cdots$$

можно определить при помощи алгоритмов для вычисления последовательности коэффициентов суммы и произведения по коэффициеньам A и B. А именно, назовём *суммой* $S(x) = A(x) + B(x) = s_0 + s_1 x + s_2 x^2 + \cdots$ многочлен, коэффициенты s_ν которого вычисляются по правилу

$$s_\nu = a_\nu + b_\nu,$$

а *произведением* $P(x) = A(x)B(x) = p_0 + p_1 x + p_2 x^2 + \cdots$ — многочлен с коэффициентами

$$p_\nu = \sum_{\alpha+\beta=\nu} a_\alpha b_\beta = a_0 b_\nu + a_1 b_{\nu-1} + \cdots + a_0 b_\nu$$

Задача 2.6. Убедитесь, что эти формулы в точности соответствуют известным вам правилам раскрытия скобок и приведения подобных слагаемых.

[1]Эти, а также рад других задач о Гауссовых числах, предполагается подробно обсудить на упражнениях. При их решении очень помогает владение техникой вычетов и разложения на простые множители (см. конец этой и следующей лекций, а также книгу Роузена и Айэрленда “Классическое введение в современную теорию чисел”).

[2]Если вы откроете толстую книжку вроде Ленга, то увидите, что многочлены там “строго определяются” именно как последовательности коэффициентов $(a_0, a_1, a_2, \ldots, a_n)$, а x и $+$ вообще в определении не упоминаются!

Очень важное наблюдение состоит в том, что при перемножении *бесконечных сумм* $A(x)$ и $B(x)$ на значение коэффициента при x^k у произведения *влияет лишь конечное число* коэффициентов каждого из сомножителей, а потому он вычисляется за конечное число шагов.

1.5.2. Степень. Номер самого правого ненулевого коэффициента называется *степенью* многочлена $a_0+a_1x+a_2x^2+\cdots$. Легко заметить (внимательно продумайте это!), что *степень произведения* двух многочленов равна *сумме степеней* сомножителей, а *старший и младший коэффициенты* произведения равны, соответственно, *произведению старших и младших коэффициентов* сомножителей. Из этого немедленно следует, что в кольце $k[x]$ многочленов над полем k нет делителей нуля, а обратимые элементы в $k[x]$ — это в точности многочлены степени нуль , не равные нулю тождественно (т. е. ненулевые константы и только они).

> Задача 2.7. Докажите, что $k[x]$ действительно является кольцом (т. е. проверьте, что определённые выше сложение и умножение удовлетворяют аксиомам коммутативного кольца с единицей).

1.6. Кольцо формальных степенных рядов $k[[t]]$ над полем k состоит из бесконечных формальных выражений вида $a_0 + a_1t + a_2t^2 + \cdots$, где в отличие от кольца многочленов *допускается бесконечно много ненулевых коэффициентов*. Операции определяются также, как и в кольце многочленов. Для бесконечных рядов теряет смысл понятие степени, но попрежнему полезно бывает следить за *младшим* (т. е. самым левым ненулевым) членом и *свободным* членом a_0. Так, ввиду того, что младший коэффициент произведения рядов равен произведению младших коэффициентов сомножителей, кольцо $k[[t]]$ является целостным.

1.6.1. Предложение. *Множество обратимых элементов в $k[[t]]$ состоит из всех рядов с ненулевым свободным членом:*

$$k[[t]]_* = \{A(t) = a_0 + a_1t + a_2t^2 + \cdots \mid \quad a_0 \neq 0\}.$$

Доказательство. Ряд с нулевым свободным членом $a_0 = 0$, очевидно, необратим: из его произведения с любым рядом выносится t. Пусть теперь $a_0 \neq 0$. Методом *неопределенных коэффициентов* подберём такой ряд

$$B(t) = b_0 + b_1t + b_2t^2 + \cdots ,$$

чтобы $A(t)B(t) = 1$. Приравнивая в левой и правой частях коэффициенты при одинаковых степенях t, получаем систему уравнений:

$$\begin{array}{rcl} a_0b_0 &=& 1 \\ a_0b_1 + a_1b_0 &=& 0 \\ a_0b_2 + a_1b_1 + a_2b_0 &=& 0 \\ \cdots && \\ a_0b_\nu + a_1b_{\nu-1} + \cdots + a_\nu b_0 &=& 0 \\ \cdots && \end{array},$$

из которой b_ν последовательно определяются по рекуррентным формулам:

$$\begin{array}{rcl} b_0 &=& a_0^{-1} \\ b_k &=& -a_0^{-1}(a_1b_{k-1} + a_2b_{k-2} + \cdots + a_kb_0). \end{array}$$

Предложение доказано.

1.6.2. Пример. Если $A(t) = 1 - t$, то предыдущее вычисление даёт:

$$(1-t)^{-1} = 1 + t + t^2 + t^3 + \cdots$$

(формула суммирования геометрической прогрессии).

Задача 2.8. Вычислите $(1+t+t^2)^{-1}$.

1.7. Кольца $A[x]$ и $A[[x]]$ многочленов и формальных степенных рядов *над кольцом* A определяются дословно также как и над полем, только коэффициенты берутся уже не из поля k, а из кольца A. Поскольку в этом случае коэффициенты могут быть необратимы, все полученные выше результаты об отсутствии делителей нуля и обратимых элементах в $k[x]$ и $k[[x]]$ над произвольным кольцом A перестают быть верными, и свойства колец $A[x]$ и $A[[t]]$ во многом зависят от соответствующих свойств кольца A.

Задача 2.9. Опишите обратимые элементы в кольце $\mathbb{Z}[x]$.

Задача 2.10. Докажите, что ряд обратим в кольце $A[[t]]$ тогда и только тогда, когда его свободный член обратим в кольце A.

1.8. Многие переменные. Кольцо многочленов от многих переменных $A[x_1, \ldots, x_n]$ определяется по индукции:

$$A[x_1, \ldots, x_n] \stackrel{\text{def}}{=} B[x_n], \quad \text{где } B = A[x_1, \ldots, x_{n-1}].$$

При вычислениях в таком кольце следует иметь в виду все оговорки из предыдущего пункта. Легко видеть, что это индуктивное определение равносильно явному, согласно которому кольцо $A[x_1, \ldots, x_n]$ есть множество формальных сумм вида:

$$F(x) = a_0 + \sum_{\nu_1, \ldots, \nu_n \in \mathbb{N}} a_{\nu_1 \ldots \nu_n} x_1^{\nu_1} x_2^{\nu_2} \cdots x_n^{\nu_n},$$

в которых лишь конечное число коэффициентов отлично от нуля.

Аналогично определяются кольца $A[[t_1, \ldots, t_n]]$.

1.9. Кольца функций. Пусть X — произвольное множество, а A — любое кольцо. Множество всех функций на X со значениями в A обозначается[3] A^X и наделяется структурой кольца при помощи операций *поточечного сложения* и *поточечного умножения* значений функций: если $f\colon x \mapsto f(x)$ и $g\colon x \mapsto g(x)$ — две функции, то

$$f + g\colon x \mapsto f(x) + g(x) \qquad f \cdot g\colon x \mapsto f(x)g(x).$$

Нулем и единицей в A^X будут функции $0(x) \equiv 0$ и $1(x) \equiv 1$.

Если $Y \subset X$ — любое подмножество, то ему соответствует *индикаторная фунркция*:

$$I_Y(x) \stackrel{\text{def}}{=} \begin{cases} 1, \text{ если } x \in Y \\ 0, \text{ если } x \notin Y \end{cases}$$

Если $Y \neq \emptyset$, то $I_Y(x) \neq 0(x)$. Если $Y_1 \cap Y_2 = \emptyset$, то $I_{Y_1} \cdot I_{Y_2} = 0(x)$. Поэтому в A^X много делителей нуля. Обратимыми, очевидно, будут те и только те функции, значения которых во всех точках X являются обратимыми элементами в A.

[3] Обозначение связано с тем, что на m-элементном множестве M имеется ровно k^m различных функций со значениями в k-элементном множестве K (это — мудрёная перефразировка известной комбинаторной задачи о числе автомобильных номеров)

В анализе часто рассматриваются различные подкольца в A^X, например: непрерывных, гладких, интегрируемых и т.п. функций.

1.10. Кольцо вычетов $\mathbb{Z}/n\mathbb{Z}$. По определению, элементом этого кольца является *подмножество в $\mathbb{Z}$, состояшее из всех чисел, имеющих один и тот же остаток от деления на n.* Такое подмножество называется *классом вычетов по модулю n.* Множество всех классов вычетов обозначается $\mathbb{Z}/n\mathbb{Z}$ и состоит из n элементов (ибо всего имеется n различных остатков от деления на n: $0, 1, 2, \dots, (n-1)$). Класс вычетов, в котором лежит целое число $a \in \mathbb{Z}$, мы будем обозначать $[a]_n$ или просто $[a]$, когда понятно, что за n имеется в виду. Принадлежность двух чисел a и b одному классу обозначается записью:

$$a \equiv b \pmod n.$$

В этом случае говорят, что *a сравнимо с b по модулю n.* Сами записи такого вида называют *сравнениями.* Они во многом аналогичны равенствам. А именно, они *рефлексивны* (т. е. $a \equiv a$, *симметричны* (т. е. $a \equiv b$ тогда и только тогда, когда $b \equiv a$) и *транзитивны* (т. е. если $a \equiv b$ и $b \equiv c$, то $a \equiv c$).

Задача 2.11. Докажите, что обе части сравнения можно умножить на одно и то же число или сложить с одним и тем же числом, а так же вычесть из обеих частей одно и то же число.

Предупреждение. Сокращать обе части сравнения на одно и то же число часто бывает нельзя, например: $3 \cdot 6 \equiv 3 \pmod{15}$, но $6 \not\equiv 1 \pmod{15}$.

1.10.1. Сложение и умножение классов вычетов индуцируется сложением и умножением в кольце $\mathbb{Z}$:

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

Это типичный пример *некорректного описания.* Действительно, вычеты — *подмножества* в $\mathbb{Z}$, и мы должны определить для двух таких подмножеств $[a]$ и $[b]$ новое подмножество, которое будет их суммой (или произведением). Написанная формула означает, что для этого мы *выбираем в $[a]$ конкретного представителя*, а именно, число a, и в $[b]$ — конкретного представителя, число b, и объявляем суммой $[a] + [b]$ класс, в котором лежит число $a + b$. A priori могло бы так случиться, что взяв других представителей $a_1 \in [a]$ и $b_1 \in [b]$ (при этом $[a_1] = [a]$ и $[b_1] = [b]$!), мы получим *другой* класс $[a_1 + b_1] \neq [a + b]$. Тогда такое "определение" в действительности ничего бы не определило! К счастью, в нашем случае корректность можно *доказать.*

1.10.2. Предложение. (Проверка корректности.) *Классы $[a+b]$ и $[ab]$ не зависят от выбора представителей a в классе $[a]$ и b в классе $[b]$.*

Доказательство. Пусть $a_1 \in [a]$, $b_1 \in [b]$. Это значит, что $a_1 = a + kn$, $b_1 = b + mn$, где $m, k \in \mathbb{Z}$. Но тогда:

$$\begin{aligned} a_1 + b_1 &= a + b + (k+m)n \\ a_1 b_1 &= ab + (bk + am + kmn)n. \end{aligned}$$

Поэтому, $a_1 + b_1 \equiv a + b \pmod n$ и $a_1 b_1 \equiv ab \pmod n$.

Задача 2.12. Докажите, что $\mathbb{Z}/n\mathbb{Z}$ — коммутативное кольцо (проверьте выполнение аксиом).

В кольцах $\mathbb{Z}/n\mathbb{Z}$ можно увидеть весь спектр явлений, перечисленных в начале лекции. Так классы $[2]_{10}$ и $[5]_{10}$ в кольце $\mathbb{Z}/10\mathbb{Z}$ имеют нулевое произведение, хотя каждый из них сам нулю не равен. Класс $[3]_{27}\in\mathbb{Z}/27\mathbb{Z}$ нильпотентен: $[3]_{27}^3 = [3^3]_{27} = [0]_{27}$, а класс $[4]_{27}\in\mathbb{Z}/27\mathbb{Z}$ — обратим: $[4]_{27}\cdot[7]_{27} = [28]_{27} = [1]_{27}$.

Задача 2.13. Составьте таблицы сложения и умножения в $\mathbb{Z}/n\mathbb{Z}$ для $n = 3$, 4, 5, 6, 7, 8. Найдите в этих кольцах все обратимые элементы, все делители нуля и все нильпотенты. Какие из колец являются полями?

§2. Факторизация

2.1. Разбиения и факторы Переход от кольца $\mathbb{Z}$ к кольцу $\mathbb{Z}/n\mathbb{Z}$ является примером важной общематематической конструкции — *факторизации* или (*склейки*). Состоит она в следующем. Пусть M — произвольное множество. Разбиением M называется представдение M в виде объединения попарно непересекающихся подмножеств, называемых *классами разбиения.*

Задача 2.14. Пусть на множестве M задано *бинарное отношение* (т. е. некоторые пары элементов объявлены “соотносящимися”, или более научно, выделено подмножество в $M\times M$). Поместим в один класс все элементы, находящиеся в заданном отношении друг с другом. Докажите, что при этом тогда и только тогда получится разбиение множества M на непересекающиеся классы, когда рассматриваемое отношение *рефлексивно*, *симметрично* и *транзитивно* (такие бинарные отношения называются *отношениями эквивалентности.*

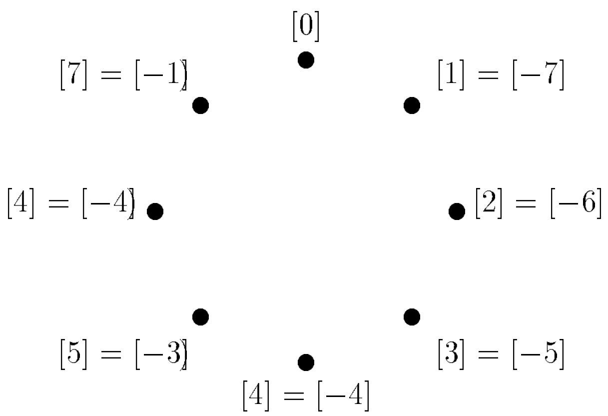

Рис. 1. Циферблат $\mathbb{Z}/8\mathbb{Z}$

Фактор-множеством данного множества M по данному разбиению называется новое множество $\bar{M}$, элементами которого являются классы рассматриваемого разбиения. Иными словами, $\bar{M}$ получается из M склеиванием всех элементов, лежащих в одном классе, в одну точку. Например, относя к одному классу все вещественные числа, отличающиеся друг от друга на целое кратное 2π, мы получим разбиение множества $\mathbb{R}$, фактор по которому геометрически изображается единичной окружностью. Переход от $\mathbb{Z}$ к $\mathbb{Z}/n\mathbb{Z}$ также удобно представлять себе аналогичной геометрической картиной и изображать элементы $\mathbb{Z}/n\mathbb{Z}$ в виде “циферблата”, — это бывает полезно при вычислениях (см. рис.рис.1 для n=8).

2.2. Спуск кольцевой структуры на фактор. Если множество $M = A$ — кольцо, то фактор-множество $\bar{A}$ по какому-либо разбиению можно пытаться наделить структурой кольца, *индуцированной с* A, то есть как и выше положить

$$[a]+[b]\overset{\text{def}}{=}[a+b] \qquad \text{и} \qquad [a][b]\overset{\text{def}}{=}[ab]\,,$$

где через $[a]$ обозначается класс разбиения, содержащий элемент a. Эти операции тавтологически удовлетворяют аксиомам кольца (ибо они наследуются из *кольца* A – продумайте это!), если только они *корректно определены*. Выясним, при каких условиях на разбиение это имеет место.

2.2.1. Свойства класса [0]. Заметим прежде всего, что класс $[0]$ с необходимостью будет нулевым элементом в факторе, ибо $[a]+[0] = [a+0] = [a]$ $\forall a\in A$. Поэтому подмножество, составляющее класс $[0]$, далеко не любое: если операции корректны, то $\forall\, a, b\in[0]$ имеем

$$[0] = [0] - [0] = [a] - [b] = [a - b] ,$$

т. е. $a - b\in[0]$ и класс $[0]$ замкнут относительно вычитания, а стало быть, и относительно перехода к противоположному элементу, а тем самым, и относительно сложения.

> Задача 2.15. Докажите, что для подмножества $M \subset A$ условие замкнутости относительно разности равносильно тому, что M замкнуто относительно сложения, имеющегося в A, и для этого сложения на M выполняются все четыре аксиомы сложенеия.

Далее, $\forall\, b\in A$ и $\forall\, a\in[\,0]$ имеем $[0] = [0b] = [0][b] = [a][b] = [ab]$, откуда, $ab\in[0]$. Это означает, что элементы класса $[0]$ не выходят из этого класса при умножении *на любые* элементы кольца (в частности класс $[0]$ сам является замкнутым относительно умножения).

2.3. Определение. *Подмножество кольца называется подкольцом, если оно замкнуто относительно сложения и умножения, и удовлетворяет относительно этих операций всем аксиомам кольца.*

2.4. Определение. *Подкольцо $\mathfrak{I} \subset A$ называется идеалом, если оно выдерживает умножение на произвольные (не обязательно ему принадлежащие) элементы объемлющего кольца: $\forall\, a\in A$ и $\forall\, x\in\mathfrak{I}$ всегда $ax \in \mathfrak{I}$.*

Итак, Для того, чтобы операции на факторе были корректны, необходимо, чтобы класс $[0]$ был идеалом в A.

2.4.1. Свойства остальных классов. Если операции над классами корректны, то вычисление $[a] - [a] = [a - a] = [0]$ может быть проделано при помощи любого другого представителя $\tilde{a}\in[a]$, что даёт

$$[[0] = [\tilde{a}] - [a] = [\tilde{a}] - [a] = [\tilde{a} - a] ,$$

т. е. $\forall\,\tilde{a}\in[a]$ выполнено условие $\tilde{a} - a \in [0]$. Верно и обратное: если $\tilde{a} - a \in [0]$, то

$$[a] = [a] + [0] = [a] + [\tilde{a} - a] = [a + \tilde{a} - a] = [\tilde{a}] ,$$

т. е. $\tilde{a}\in[a]$.

Таким образом, каждый класс $[a]$ состоит из тех и только тех элементов $\tilde{a}$, для которых $\tilde{a} - a \in [0]$. Инче говоря, $[a]$ имеет вид $[a] = a + [0]$, т. е. получается "параллельным сдвигом" класса $[0]$ на элемент a. В частности, все классы находятся во взаимно-однозначном соответствии с классом $[0]$, и всё разбиение полностью определяются заданием идеала $[0] \subset A$.

2.5. Факторизация по идеалу. Итог предыдущего анализа можно сформулировать так: для того чтобы индуцированные с A операции на факторе кольца A по некоторому разбиению были корректны, необходимо, чтобы класс $[0]$ был идеалом в A, а все остальные классы $[a]$ имели вид:

$$[a] = a + [0] = \{\tilde{a}\in A \mid \tilde{a} - a\in[0]\} .$$

Для данного идеала $\mathfrak{I} \subset A$ два элемента $a, b\in A$, для которых $a - \tilde{a}\in\mathfrak{I}$, называются *сравнимыми по модулю идеала* $\mathfrak{I}$. Объединение всех попарно-сравнимых друг с другом элементов кольца назывется *классом вычетов по модулю идеала.*

2.5.1. Предложение. *Фактор-множество $\bar{A}$ кольца A тогда и только тогда является кольцом относительно операций, индуцированных с A, когда A является множеством классов вычетов по модулю некоторого идеала $\mathfrak{I} \subset A$.*

Название и обозначение. При выполнении условий теоремы фактор обозначается через $A/\mathfrak{I}$ и называется *фактором кольца A по идеалу $\mathfrak{I}$.*
Доказательство. С учётом вышесказанного, нам остается только проверить корректность операций на множестве классов вычетов по модулю идеала. Пусть $[a] = [\tilde{a}]$ и $[b] = [\tilde{b}]$, то есть $\tilde{a} = a + r,\ \tilde{b} = b + s$, где $s, r \in \mathfrak{I}$. Тогда

$$a + b = (\tilde{a} + \tilde{b}) + (r + s) \quad \text{и} \quad (r + s) \in \mathfrak{I},$$

$$ab = \tilde{a}\tilde{b} + (rb + sa + rs) \quad \text{и} \quad (rb + sa + sr) \in \mathfrak{I}.$$

Теорема доказана.

§3. Примеры идеалов

3.1. Тривиальные идеалы. Идеалы $\{0\}$ и A, имеющиеся в любом кольце, называются *тивиальными*. При этом $A/\{0\} = A$ и $A/A = \{0\}$.

Задача 2.16. Докажите, что для того чтобы идеал совпадал со всем кольцом необходимо и достаточно, чтобы он содержал какой-нибудь обратимый элемент кольца.

Задача 2.17. Докажите, что кольцо тогда и только тогда является полем, когда в нем нет нетривиальных идеалов.

3.2. Нильрадикал. *Нильрадикалом* кольца A называется множество всех нильпотентных элементов кольца A в объединении с нулем:

$$\mathfrak{n} = \{a \in A \mid a^n = 0 \ \text{ для некоторого } n \in \mathbb{N}\}.$$

Нильрадикал является идеалом в A. Действительно, если $a^n = 0$, то $\forall b \in A\ (ab)^n = a^n b^n = 0$ и $\forall b\colon\ b^m = 0$ из формулы бинома заключаем, что $(a - b)^{n+m-1} = 0$.

3.3. Главные идеалы. *Главным идеалом, порожденным* $d \in A$ называется множество всех элементов кольца, кратных d: $\{ad |\ a \in A\}$ (проверьте, что это действительно идеал). Он обозначается символом (d) или dA. Фактор-кольцо $A/(a)$ называется *кольцом вычетов по модулю a*. В частности, $\mathbb{Z}/n\mathbb{Z}$ есть $\mathbb{Z}/(n)$, где $(n) \subset \mathbb{Z}$ — главный идеал, порожденный n. Тривиальные идеалы также главные: $\{0\} = (0)$, $\ A = (1)$. Кольцо, в котором все идеалы исчерпываются главными, называется *кольцом главных идеалов*.

Следующий факт является важнейшим в арифметике целых чисел:

3.4. Теорема. *$\mathbb{Z}$ является кольцом главных идеалов.*

Доказательство. Пусть $\mathfrak{I} \subset \mathbb{Z}$ — нетривиальный идеал. Тогда он содержит какие-либо *натуральные* числа. Пусть d — наименьшее натуральное число в $\mathfrak{I}$. Я утверждаю, что $\mathfrak{I} = (d)$.

Действительно, $(d) \subset \mathfrak{I}$, ибо $d \in \mathfrak{I} \Rightarrow kd \in \mathfrak{I}\ \ \forall k \in \mathbb{Z}$.

Докажем противоположное включение. Пусть $a \in \mathfrak{I}$ — любое. Деля a на d с остатком, мы можем представить a в виде $a = kd + r$, где $0 \le r \le d-1$ — остаток, а $k \in \mathbb{Z}$. Так как $r = a - kd$ и $a, d \in \mathfrak{I}$, то $r \in \mathfrak{I}$. Следовательно, $r = 0$, ибо d вбыиралось наименьшим натуральнм числом в $\mathfrak{I}$. Значит, $a = kd \in (d)$ и $\mathfrak{I} \subset (d)$.

Теорема доказана.

3.5. Конечно-порождённые идеалы. Пусть A — кольцо. Для любого набора элементов $\{a_1, a_2, \ldots, a_n\}$ обозначим через $(a_1, a_2, \ldots, a_n)$ или $a_1A + a_2A + \cdots + a_nA$ множество всех элементов в A, представимых в виде

$$a = a_1x_1 + a_2x_2 + \cdots a_nx_n \qquad \text{с} \quad x_1, \ldots, x_n \in A.$$

Оно является идеалом в A, и называется *идеалом, порожденным* $(a_1, a_2, \ldots, a_n)$. Сами элементы a_i в этом случае называются *образующими* идеала.

> Задача 2.18. Докажите, что идеал (x, y), порожденный x и y в кольце $k[x, y]$ многочленов от двух переменных, не является главным.

3.6. НОД и взаимная простота в кольце $\mathbb{Z}$. Пусть $m_1, \ldots, m_k \in \mathbb{Z}$ — какие-то целые числа. Идеал $(m_1, m_2, \ldots, m_k) \subset \mathbb{Z}$ состоит из всех целых чисел m, представимых в виде $m = m_1x_1 + \cdots + m_kx_k$ с целыми $x_1, \ldots, x_k$ (геометрически — это множество всех векторов числовой прямой, которые можно отложить, имея k векторов $m_1, \cdots, m_k$). По теореме Теор.3.4 он является главным, т. е. $(m_1, m_2, \ldots, m_k) = (d)$ для некоторого $d \in \mathbb{N}$. Число d представимо в виде

$$d = m_1x_1 + \cdots + m_kx_k,$$

делит каждое из чисел m_ν и делится на любое другое число D, являющееся общим делителем для всех m_ν. Таким образом, $d = \text{НОД}(m_1, m_2, \ldots, m_k)$ — *наибольший общий делитель.* Замечу, что по школьному определению НОД есть наибольшее натуральное число, делящее каждое из m_ν, и a priori неясно, что оно должно делиться нацело на любой другой делитель и представляться в виде $m_1x_1 + \cdots + m_kx_k$.

Числа $m_1, \ldots, m_k$ называются *взаимно простыми в совокупности*, если

$$\text{НОД}(m_1, m_2, \ldots, m_k) = 1,$$

и *попарно взаимно простыми*, если

$$\text{НОД}(m_i, m_j) = 1 \ \forall i \neq j.$$

Совокупная взаимная простота равносильна (по предыдущему) возможности представить единицу в виде $1 = m_1x_1 + \cdots + m_kx_k$ с целыми x_ν. В частности, два числа a и b взаимно просты тогда и только тогда, когда существуют целые x и y такие, что $ax + by = 1$.

3.6.1. Предложение.

а) *Если a делит bc $(a, b, c \in \mathbb{Z})$ и a и b взаимно просты, то a делит c.*

б) *Если a и b взаимно просты и делят c, то их произведение ab также делит c.*

Доказательство. Умножая на c равенство $ax + by = 1$, получаем $c = acx + bcy$. Правая часть этого равенства делится на a при bc делящемся на a, и делится на ab при c делящемся и на a и на b (т. е. при $c = ar = bs$).

3.6.2. Предложение. *$\mathbb{Z}/p\mathbb{Z}$ тогда и только тогда является полем, когда p — простое число.*

Доказательство. Если $n = n_1n_2 \in \mathbb{N}$ — не простое (т. е. $n_1 \neq n$ и $n_2 \neq n$), то в $\mathbb{Z}/n\mathbb{Z}$ имеем $[n_1][n_2] = [n] = [0]$, т. е. $[n_1]$ и $[n_2]$ — делители нуля, что невозможно в поле.

Наоборот, если $n = p \in \mathbb{N}$ — простое, то $\forall [m] \neq [0]$ число m будет взаимно просто с p, а стало быть $mx + py = 1$ для некоторых целых x и y. Но тогда $[m][x] = [mx] = [1 - py] = [1]$ и $[m]$ обратим. Предложение доказано.

3.7. Простые и максимальные идеалы. Для того, чтобы в случае произвольного кольца A уметь выяснять, является ли фактор $A/\mathfrak{p}$ по данному идеалу $\mathfrak{p}$ полем, можно попытаться сформулировать условие "p — простое число" в терминах свойств идеала (p). Поскольку число p просто тогда и только тогда, когда оно взаимно просто с любым числом не лежащем в (p), идею для нужной нам переформулировки можно взять из Пр.3.6.1.

А именно, идеал $\mathfrak{p} \in A$ в произвольном коммутативном кольце A называется *простым*, если $\forall a, b \in A$ из $ab \in \mathfrak{p}$ и $a \notin \mathfrak{p}$ следует, что $b \in \mathfrak{p}$.

Задача 2.19. Докажите, что $(p) \subset \mathbb{Z}$ прост тогда и только тогда, когда p — простое число.

3.7.1. Предложение. *Фактор кольцо $A/\mathfrak{p}$ тогда и только тогда является целостным, когда $\mathfrak{p}$ — простой идеал.*

Доказательство. Отсутствие делителей нуля в $A/\mathfrak{p}$ равносильно тому, что $\forall a, b \in A$ равенство $[a][b] = [ab] = [0] = \mathfrak{p}$ при условии $[a] \neq [0]$ влечет за собой $[b] = [0] = \mathfrak{p}$. Но это и означает, что из $ab \in \mathfrak{p}$ и $a \notin \mathfrak{p}$ следует $b \in \mathfrak{p}$. Предложение доказано.

Однако, не всякое целостное кольцо — поле, и в частности, фактор по простому идеалу может и не быть полем.

Задача 2.20. Проверьте, что главный идеал $(x^2 - y) \subset \mathbb{C}[x, y]$ прост, и найдите в факторе по нему необратимые элементы.

Идеал $\mathfrak{m}$ называется *максимальным*, если он не содержится ни в каком другом нетривиальном идеале. Это условие равносильно тому, что в факторе $A/\mathfrak{m}$ нетривиальных идеалов нет вообще. Действительно, если $\mathfrak{I} \subset A/\mathfrak{m}$ — такой нетривиальный идеал, то подмножество $\tilde{\mathfrak{I}} = \{a \in A \mid [a]_{\mathfrak{m}} \in \mathfrak{I}\} \subset A$ составит нетривиальный идеал в A, строго содержащий $\mathfrak{m}$.

Задача 2.21. Проверьте последнее утверждение.

Задача 2.22. Докажите, что всякий максимальный идеал прост.

Задача 2.23. Докажите, что $A/\mathfrak{m}$ — поле тогда и только тогда, когда $\mathfrak{m}$ — максимальный идеал.

§4. Примеры гомоморфизмов

Гомоморфизм колец $f: A \longrightarrow B$ определяется дословно также, как и гомоморфизм полей: это такое отображение, при котором $\forall a_1, a_2 \in A$ в кольце B выполнены соотношения:

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

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

Задача 2.24. Докажите, что если $f: A \longrightarrow B$ — гомоморфизм, то $f(0) = 0$ и $f(-a) = -f(a)$.

Рассмотрим несколько примеров.

4.1. Гомоморфизм обратного образа, Большая часть гомоморфизмов между кольцами, встречающимися в анализе, геометрии и топологии, строится по следующей схеме. Пусть X и Y — два множества, A — кольцо, и A^X, A^Y — кольца функций на X и Y со значениями в A. Тогда для любого отображения множеств

$$\varphi: X \longrightarrow Y$$

возникает гомоморфизм колец
$$\varphi^*: A^Y \longrightarrow A^X$$
называемый *гомоморфизмом обратного образа* или *поднятия* (обратите внимание, что он действует в направлении, противоположном φ).

По определению, для каждой функции F на Y функцмя $\varphi^*(F)$ на X действует на элементы $x \in X$ по правилу: $\varphi^*(F)(x) = F\big(\varphi(x)\big)$, т. е. является композицией исходной функции F и отображения φ.

Задача 2.25. Убедитесь, что φ^* действительно гомоморфизм.

Оказывается, что алгебраические свойства гомоморфизма φ^* на *структурное подкольцо* в A^Y (в ТФКП таковым служит кольцо голоморфных функций, в дифференциальной геометрии и топологии — кольцо гладких или непрерывных функций, в алгебраической геометрии — кольцо полиномиальных функций) очень хорошо отражают геометрические свойства как самого отображения φб так и пространств X и Y.

4.2. Гомоморфизмы вычисления. Рассмотрим предыдущую конструкцию в случае, когда $X = \{p\}$ состоит из одной точки и $\varphi: \{p\} \hookrightarrow Y$ отождествляет эту точку с некоторой точкой $y \in Y$. Здесь $A^X = A$ и гомоморфизм поднятия будет действовать из A^Y в A, сопоставляя функции $F \in A^Y$ её значение $F(y)$ в точке y. В такой ситуации он называется *гомоморфизмом вычисления значения* функций на Y в точке $y \in Y$ и обозначается
$$\mathrm{ev}_y: A^Y \longrightarrow A.$$

Другие гомоморфизмы вычисления встречаются в анализе. Например, для некоторых формальных рядов из $\mathbb{C}[[t]]$ (называемых *сходящимися*) можно определить их значение в точке $z \in \mathbb{C}$. Эта конструкция не алгебраическая, ибо результат подстановки числа в формальный ряд определяется не как результат конечного числа алгебраических действий, а при помощи перехода к пределу. В этом случае свойство ev_y быть гомоморфизмом перестаёт быть тривиальным и превращается в содержательную теорему из анализа. Алгебраическое значение этой теоремы состоит в том, что все формальные тождества между рядами в кольце $\mathbb{C}[[t]]$ при применении к сходящимся рядам влекут за собой соответствующие тождества между числами в $\mathbb{C}$ или между функциями в $\mathbb{C}^{\mathbb{C}}$.

4.3. Гомоморфизм факторизации. Отображение $\pi_n: \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, при котором $m \mapsto [m]_n$ является (по определению операций в $\mathbb{Z}/n\mathbb{Z}$) гомоморфизмом. Он называется *редукцией по модулю* n. Этот гомоморфизм *сюрьективен*, т. е. у любого $x \in \mathbb{Z}/n\mathbb{Z}$ имеется прообраз[4].

Аналогично, для любого идеала $\mathfrak{I}$ в произвольном кольце A имеется эпиморфизм $\pi_{\mathfrak{I}}$: $A \longrightarrow A/\mathfrak{I}$ редукции по модулю этого идеала.

4.4. Простое подполе и характеристика. Пусть k — любое поле, $1 \in k$ — единица в этом поле. Определим отображение $f: \mathbb{Z} \longrightarrow k$, полагая:
$$\begin{aligned} f(0) &= 0 \\ f(n) &= \underbrace{1 + 1 + \cdots + 1}_{n} \\ f(-n) &= \underbrace{-1 - 1 - \cdots - 1}_{n}, \end{aligned}$$
где n — любое натуралюное число. Очевидно, что f — это гомоморфизм кольца $\mathbb{Z}$ в поле k.

[4]Сюрьективные гомоморфизмы называют также *эпиморфизмами*.

Если f является вложением, говорят, что поле k имееит *характеристику нуль*, и пишут: $\mathrm{char}(k) = 0$. В этом случае f однозначно продолжается по формуле $f(m/n) = f(m)/f(n)$ до вложения полей $\mathbb{Q} \longrightarrow k$, так что k содержит канонически определенное подполе, изоморфное $\mathbb{Q}$.

Если f не является вложением, скажем $f(m) = f(s)$ для некоторых $m, s \in \mathbb{Z}$, и, скажем, $m > s$, то $f(m - s) = f(m) - f(s) = 0$. Значит, имеется натуральное n, такое что

$$f(n) = \underbrace{1 + 1 + \cdots + 1}_{n} = 0.$$

Наименьшее такое n называется *характеристикой* поля k и обозначается $\mathrm{char}(k)$. При этом говорят, что поле *имеет положительную характеристику* (в отличие от случая нулевой характеристики).

Задача 2.26. Убедитесь, что $\mathrm{char}(\mathbb{Z}/p\mathbb{Z}) = p$ (где $p \in \mathbb{N}$ — простое).

Ясно, что и в общем случае $\mathrm{char}(k)$ — простое число. Действительно, если $\mathrm{char}(k) = n = sr$, где $s < n$ и $r < n$ (так что $f(s)$ и $f(r)$ ненулевые в k), то

$$0 = \underbrace{1 + 1 + \cdots + 1}_{n} = \underbrace{(1 + 1 + \cdots + 1)}_{r}\underbrace{(1 + 1 + \cdots + 1)}_{s} = f(r)f(s),$$

что невозможно, ибо в поле нет делителей нуля.

При $\mathrm{char}(k) = p > 0$ *образ* гомоморфизма f (т. е. $f(\mathbb{Z}) \subset k$) составляет подполе в k, изоморфное полю $\mathbb{Z}/p\mathbb{Z}$. Действительно, этот образ будет подкольцом в k, которое можно рассматривать как фактор кольца $\mathbb{Z}$ по разбиению, объединяющему в один класс все числа, имеющие одинаковый образ в k. Но мы видели, что такое кольцо должно быть фактором $\mathbb{Z}$ по идеалу, состоящему из всех чисел n, для которых $f(n) = 0$. Наименьшее такое число —p, и значит идеал этот совпадает с (p), а $f(\mathbb{Z})$ есть $\mathbb{Z}/p\mathbb{Z}$.

Итак, в любом поле k можно *канонически* выделить наименьшее подполе, содержащее 0 и 1. Это подполе называется *простым подполем*. Оно изоморфно $\mathbb{Q}$ при $\mathrm{char}(k) = 0$ и изоморфно $\mathbb{Z}/p\mathbb{Z}$ при $\mathrm{char}(k) = p > 0$. Смысл эпитета “канонически” призвана прояснить следующая

Задача 2.27. Докажите, что все элементы простого подполя остаются на месте при любом ненулевом гомоморфизме из k в k.

4.5. Гомоморфизм Фробениуса. Если $\mathrm{char}(k) = p$, то отображение $F\colon x \mapsto x^p$ является *гомоморфизмом* из поля k в себя (он называется *гомоморфизмом Фробениуса*).

Действительно, $(xy)^p = x^p y^p$. Раскрывая скобки в $(x + y)^p$ по обычным правилам, мы получим сумму, состоящую из слагаемых вида $x^k y^{p-k}$. Как объяснялось на стр.12, всего членов, равных фиксированному $x^\nu y^{p-\nu}$, будет $\binom{p}{\nu}$, т. е. коэффициент при $x^\nu y^{p-\nu}$ будет равен

$$\underbrace{1 + 1 + \cdots + 1}_{\binom{p}{\nu}} = f\left(\frac{p!}{\nu!(p-\nu)!}\right)$$

(где f — гомоморфизм из предыдущего пункта). Но $\frac{p!}{\nu!(p-\nu)!} = 1$ при $\nu = 0$ и $\nu = p$, а во всех остальных случаях делится на p, ибо числитель дроби делится на p, а знаменатель взаимно прост с p при простом p. Поэтому все слагаемые в разложении $(x + y)^p$, кроме x^p и y^p сократятся, и $(x + y)^p = x^p + y^p$.

4.5.1. Предложение. (Малая теорема Ферма.) *Если p — простое число, то $\forall a \in \mathbb{Z}$ выполнено сравнение $a^p \equiv a \pmod{p}$. Если же a не делится на p, то $a^{p-1} \equiv 1 \pmod{p}$.*

Доказательство. Гомоморфизм Фробениуса тождественно действует на $\mathbb{Z}/p\mathbb{Z}$ (оно есть простое подполе самого себя), и значит, $[a^p] = [a]^p = [a]\ \forall a \in \mathbb{Z}$, то есть $a \equiv a \pmod p$.

Если же a не делится на p, то $[a]$ обратим в $\mathbb{Z}/p\mathbb{Z}$, и умножая на $[a]^{-1}$ равенство $[a^p] = [a]$, получим $[a^{p-1}] = [1]$, т. е. $a^{p-1} \equiv 1 \pmod p$.

4.6. Строение гомоморфизмов. Предыдущие примеры показывают, что гомоморфизмы колец (в отличие от гомоморфизмов полей) могут не быть вложениями. Тем не менее, их строение может быть детально описано.

4.7. Определение. *Пусть $f\colon A \longrightarrow B$ — гомоморфизм колец. Подмножество*

$$\ker(f) = \{a \in A \mid f(a) = 0\} \subset A$$

называется ядром гомоморфизма f, а подмножество

$$\operatorname{im}(f) = \{b \in B \mid \exists a \in A\colon f(a) = b\} \subset B$$

называется образом гомоморфизма f.

4.7.1. Предложение. *Образ гомоморфизма $f\colon A \longrightarrow B$ является подкольцом в B, а ядро — идеалом в A. При этом существует канонический изоморфизм*

$$\tilde{f}\colon\ A/\ker(f) \xrightarrow{\sim} \operatorname{im}(f),$$

при котором классу $[a]$ по модулю $\ker(f)$ соответствует $f(a) \in \operatorname{im}(f)$.

Доказательство. Если $a, \tilde{a} \in \ker(f)$, то $f(a - \tilde{a}) = f(a) - f(\tilde{a}) = 0 - 0 = 0$, так что $a - \tilde{a} \in \ker(f)$. Аналогично, если $a \in ker(F)$, и $b \in A$ — любой, то $f(ab) = f(a)f(b) = 0 \cdot f(b) = 0$, так что $ab \in \ker(f)$. Следовательно, $\ker(f)$ — идеал.

Пусть $\tilde{A} = A/\ker(f)$ — соответствующий фактор. Отображение $\tilde{f}\colon [a] \mapsto f(a)$ действует из $\tilde{A}$ в $\operatorname{im}(f)$. Оно определено корректно, поскольку $\forall \tilde{a} : [\tilde{a}] = [a]$ имеем $\tilde{a} = a + r$ (где $r \in ker(f)$), и $f(\tilde{a}) = f(a) + f(r) = f(a)$. Это отображение является гомоморфизмом (ибо f — гомоморфизм) и взаимно-однозначно, поскольку у каждого $b = f(a) \in \operatorname{im}(f)$ есть прообраз $[a] \in \tilde{A}$, причем ровно один, т.к. $b = f(a) = f(\tilde{a})$ означает, что $f(a - \tilde{a}) = f(a) - f(\tilde{a}) = 0$, откуда $a - \tilde{a} \in \ker(f)$ и $[a] = [\tilde{a}]$.

Таким образом, $\tilde{f}$ и в самом деле отождествляет $\tilde{A}$ с $\operatorname{im}(f)$ с сохранением операций, в частности, $\operatorname{im}(f)$ — подкольцо в B.

□

4.7.2. Следствие. *Произвольный гомоморфизм $f\colon A \longrightarrow B$ может быть разложен в композицию эпиморфизма редукции A по модулю идеала $\ker(f)$, изоморфизма*

$$\tilde{f}\colon\ A/ker(f) \xrightarrow{\sim} \operatorname{im}(f)$$

и вложения подкольца $\operatorname{im}(f)$ в B.

□

Схематически это изображается *коммутативной диаграммой*:

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle \pi_{\ker(f)}}\big\downarrow & & \big\uparrow \\ A/\ker(f) & \xrightarrow{\tilde{f}} & \operatorname{im}(f) \end{array}$$

Эпитет “коммутативный” означает, что результат переноса любого элемента $a \in A$ в B по стрелкам не зависит от выбора пути (в данном случае таких путей 2).

4.8. Прямые суммы колец. В заключение лекции приведем еще одну часто встречающуюся конструкцию с кольцами. Пусть A_1, A_2, ..., A_n — n колец.

4.9. Определение. *Прямой суммой*

$$\bigoplus_{\nu=1}^{n} A_\nu = A_1 \oplus A_2 \oplus \cdots \oplus A_n$$

называется кольцо, элементами которого служат наборы:

$$a = (a_1, a_2, \ldots, a_n), \qquad \text{где } \ a_\nu \in A_\nu,$$

а операции определяются покомпонентно: если $a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n)$, *то*

$$a + b = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$
$$ab = (a_1b_1, a_2b_2, \ldots, a_nb_n)$$

Нулем относительно этих операций будет набор $(0, 0, \ldots, 0)$, а единицей — набор $(1, 1, \ldots, 1)$.

Задача 2.28. Докажите, что $A_1 \oplus A_2 \oplus \cdots \oplus A_n$ — кольцо (проверьте аксиомы).

Прямая сумма по своим свойствам дальше отстоит от поля, чем слагаемые. Например, в ней всегда есть делители нуля: $(0, 1)(1, 0) = (0, 0)$. В частности, прямая сумма полей есть кольцо, но не поле.

Задача 2.29. Убедитесь, что в кольце

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

всего имеется ровно $n_1n_2 \cdots n_k$ элементов.

В качестве примера, иллюстрирующего все конструкции этой лекции, укажем “научное” доказательство одной известной теоремы арифметики. Тем, кто знает ее “элементарное” доказательство, поучительно будет сравнить его с нашим и отметить для себя те алгебраические пружины, которые им движут.

4.9.1. Предложение. (Китайская теорема об остатках.) *Пусть* $(n_1, n_2, \ldots, n_k)$ *— набор попарно взаимно простых чисел. Тогда для любого набора* $(r_1, r_2, \ldots, r_k)$ *остатков от деления на* n_1, n_2, ..., n_k *соответственно можно подобрать такое целое число* a, *которое довало бы остаток* r_1 *от деления на* n_1, *остаток* r_2 *от деления на* n_2, *и так далее.*

Более того, если $\tilde{a}$ *— другое такое число, то разность* $a - \tilde{a}$ *делится на произведение* $n_1n_2 \cdots n_k$.

Доказательство. Пусть $N = n_1n_2 \cdots n_k$. Кольца

$$A = \mathbb{Z}/N\mathbb{Z} \qquad \text{и} \qquad B = \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$$

состоят из одинакового числа элементов. Отображение $f\colon\ A \longrightarrow B$, переводящее класс $[a]_N$ в набор классов $([a]_{n_1}, [a]_{n_2}, \ldots, [a]_{n_2})$ корректно определено, т. е. не зависит от выбора представителя $a \in [a]_N$, и является гомоморфизмом.

Его ядро состоит из таких классов $[a]_N$, что a делится на каждое из чисел n_ν. Но так как числа n_ν попарно взаимно просты, то каждое такое a будет делиться и на их произведение N (почему?), а сало быть $[a]_N = [0]_N$ и $\ker(f) = \{0\}$.

Образ $\mathrm{im}(f)$ изоморфен $A/ker(f) = A$. В частности, он состоит из того же количества элементов, что и A, а поэтому совпадает с B.

Итак, f — изоморфизм. Но это в точности и составляет утверждение теоремы.