Алгебра. Сентябрь 2010.

Введение.

Эти записки лекций, прочитанных в сентябре. Все определения и теоремы, необходимые для освоения курса, здесь содержатся, возможно, в виде задач. Не все определения выделены в отдельную формулировку и предваряются словом "определение", но все впервые определяемые термины выделены курсивом. Все задачи, не отмеченные звездочкой, важны для понимания дальнейшего: в них, как правило, содержатся результаты, существенно используемые впоследствии, или же вводятся важные примеры. Большинство задач повторяет с незначительными вариациями задачи из листочков; нумерация,однако, может быть иной.

Оглавление

1. Арифметика.

Элементарная арифметика целых чисел, в основном, известна из школьного курса. Напомним, однако, некоторые основные понятия. Говорят, что целое число b *является делителем* целого числа a, или что целое число a *делится* на целое число b, если $a = bc$, где число c также целое. Этот факт мы будем обозначать следующим образом: $b \mid a$ (читается: «b является делителем a», или «a делится на b»). Натуральное число $p > 1$ называется простым, если оно не имеет натуральных делителей, отличных от 1 и самого себя. Известно, что любое натуральное число, большее единицы, можно разложить в произведение простых сомножителей, причем это разложение однозначно с точностью до порядка сомножителей; этот факт называется «основной теоремой арифметики» и, вообще говоря, требует доказательства, которое мы здесь не приводим.

Пусть даны два целых числа a и b, тогда их *наибольшим общим делителем* называется, такое наибольшее натуральное число d, что $d \mid a$ и $d \mid b$. Обозначение: $d = \text{НОД}(a, b)$; часто его сокращают до $d = (a, b)$. Аналогично, *наименьшим общим кратным* чисел a и b называется такое наименьшее натуральное число f, что $a \mid f$ и $b \mid f$. Обозначение: $f = \text{НОК}(a, b)$.

Задача 1.1. *Доказать, что* $\text{НОК}(a, b)\text{НОД}(a, b) = |ab|$.

Два целых числа a и b называются *взаимно простыми*, если они не имеют общих делителей, отличных от 1 и -1, то есть если НОД$(a,b) = 1$. Часто в доказательствах удобно ссылаться на следующее очевидное утверждение:

Лемма 1.1. *Пусть a, b и c — целые числа, причем a и b взаимно просты (то есть* НОД$(a,b) = 1$*) и $a \mid bc$. Тогда $a \mid c$.*

Еще один важный инструмент при работе с целыми числами — это деление с остатком. Разделить с остатком целое число a на натуральное число n — это значит представить число a в виде $a = ns + r$, где s и r — целые числа, причем $0 \le r < n$. Очевидно, такое представление всегда возможно и определено однозначно; при этом s называется неполным частным (и редко бывает зачем-нибудь полезным), а r — остатком (он-то, как правило, и важен). Заметим еще, что для положительного числа a деление с остатком на n равносильно разложению дроби $\frac{a}{n}$ в сумму ее целой части s и правильной дроби $\frac{r}{n}$: деля равенство $a = ns + r$ на n, получаем $\frac{a}{n} = s + \frac{r}{n}$. Обратите внимание на деление с остатком отрицательных чисел: остаток, например, от деления числа -11 на 5 равен 4 ($-11 = (-3)5 + 4$).

1.1. Неопределенные уравнения.

Мы будем искать целочисленные решения уравнений вида

$$ax + by = c, \tag{1.1}$$

где x и y — неизвестные, а a,b и c — фиксированные целые числа; заменяя при необходимости x на $-x$ или y на $-y$, можно считать числа a,b и c натуральными.

Начнем со случая $c = 1$, т. е. будем исследовать уравнение вида

$$ax + by = 1. \tag{1.2}$$

Предположим, что уравнение (1.2) имеет решения, и предположим, что числа a и b делятся на некоторое натуральное число d . Тогда выражение $ax + by$ также должно делиться на это число d, что невозможно, поскольку $ax + by = 1$. Следовательно, для того, чтобы уравнение (1.2) имело целые решения, необходимо, чтобы числа a и b были взаимно просты, т.е. НОД$(a,b) = 1$. Оказывается, это же условие является и достаточным. Докажем это. Предположим, что НОД$(a,b) = 1$, перепишем уравнение (1.2) в виде $ax = -by + 1$ и попробуем искать его решения подбором, подставляя вместо y последовательно числа 0, 1, 2, 3, ... и так далее до тех пор, пока by не будет давать при делении на a остаток 1. Как только это произойдет, число $-by + 1$ будет нацело делиться на a, поэтому $x = \frac{-by+1}{a}$ будет искомым целочисленным решением уравнения (1.2). Осталось только понять, почему это вообще когда-нибудь должно произойти, и сколько значений y нам перед этим придется перепробовать. Оказывается, нам потребуется не более a проб; мы сейчас докажем, что остатки от деления a чисел $b \cdot 0$, $b \cdot 1$, $b \cdot 2$, ..., $b \cdot (a-1)$ на a должны быть все различны. Тогда, поскольку всего существует только a возможных остатков от деления на a, один из них обязательно окажется равным 1, что и даст нам искомое решение уравнения 1.2.

Итак, рассмотрим числа $b \cdot 0, b \cdot 1, b \cdot 2, \ldots, b \cdot (a-1)$; предположим, что какие-нибудь два из них, например $b \cdot p$ и $b \cdot q$, дают при делении на a один и тот же остаток r , т. е. $bp = au + r$ и $bq = av + r$, $p, q \in \{0, 1, 2, \ldots, a-1\}$, $0 \le r < a$. Пусть, например, $p > q$, тогда, вычитая второе равенство из первого, получим, что $b(p-q) = a(u-v)$, то есть $b(p-q)$ делится на a . Применяя теперь лемму 1.1, заключаем, что $a \mid (p-q)$, что невозможно, поскольку числа p и q заключены между 0 и $a-1$, так что и $0 < p - q < a$. Полученное противоречие доказывает, что остатки от деления чисел $b \cdot 0, b \cdot 1, b \cdot 2, \ldots, b \cdot (a-1)$ на a действительно все различны, поэтому существует целочисленное решение $(x_0; y_0)$ уравнения (1.2) с $0 < y_0 < a$.

Заметим теперь, что более общий, на первый взгляд, вопрос о существовании решений уравнения (1.1) сразу сводится к уже разобранному случаю. Действительно, для существования решений

уравнения (1.1) необходимо, чтобы всякий общий делитель чисел a и b являлся бы одновременно и делителем c, тогда, сокращая обе части уравнения на общие делители всех его коэффициентов, мы опять приходим к условию НОД$(a,b)=1$. Легко видеть, что это условие является также и достаточным: если $(x_0;y_0)$ — какое-нибудь решение уравнения (1.2), то $(cx_0;cy_0)$ является, очевидно, решением уравнения (1.1).

Вопрос о перечислении всех решений уравнения (1.1) или (1.2) также решается очень просто: если $(x_1;y_1)$ и $(x_2;y_2)$ — два решения уравнения (1.1), то, вычитая равенство $ax_1+by_1=c$ из равенства $ax_2+by_2=c$, получаем $a(x_1-x_2)+b(y_1-y_2)=0$. Но поскольку коэффициенты a и b взаимно просты, из леммы 1.1 следует, что $a \mid (y_1-y_2)$, т.е. $y_1-y_2=ka$, где k — целое число, и, значит, $x_1-x_2=-kb$. Следовательно, любое решение уравнения (1.1) имеет вид $x=x_0-kb, y=y_0+ka, k\in\mathbb{Z}$. Сформулируем полученные результаты в виде теоремы.

Теорема 1.1. *Пусть a,b и c — целые числа,*

$$ax+by = 1 \tag{1.3}$$
$$ax+by = c \tag{1.4}$$

— диофантовы уравнения. Тогда
1) уравнение (1.3) имеет целые решения тогда и только тогда, когда a и b взаимно просты (то есть НОД$(a,b)=1$*);*
2) если $(x_0;y_0)$ — какое-нибудь решение (1.2), то все остальные решения (1.3) получаются по формулам $x=x_0-kb;\quad y=y_0+ka;\quad k\in\mathbb{Z}$;
3) уравнение (1.4) имеет целые решения $\Longleftrightarrow$ c делится на НОД(a,b)*; в этом случае сокращение уравнения на* НОД(a,b) *сводит его решение к случаю* НОД$(a,b)=1$.
4) если НОД$(a,b)=1$ *и $(x_0;y_0)$ — какое-нибудь решение (1.3), то все остальные решения (1.4) получаются по формулам $x=cx_0-kb;\quad y=cy_0+ka;\quad k\in\mathbb{Z}$.*

Задача 1.2. *Докажите, не используя доказанные нами результаты о неопределенных уравнениях, что если* НОД$(a,b)=1$*, то наименьшее натуральное число, представимое в виде $ax+by$ $x,y\in\mathbb{Z}$, равно 1. (Это дает другое доказательство теоремы 1.1.)*

Задача 1.3. *Обобщите первое утверждение теоремы 1.1 на уравнение с $n>2$ неизвестными.*

Мы привели два доказательства существования решения уравнения (1.3). Между ними имеется принципиальная разница: в то время как подход, предложенный в задаче 1.2, на первый взгляд, дает чистое доказательство существования решения без указания того, как его найти, наше первое доказательство все-таки позволяет указать некоторый алгоритм нахождения решения, хотя и очень примитивный: гарантируется, что решение можно найти прямым перебором не более чем за $\max(a,b)$ шагов. Существует, однако, намного более экономный алгоритм нахождения решения, использующий цепные дроби.

1.2. Цепные дроби и алгоритм Евклида.

Цепной дробью называется выражение следующего вида:

$$2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{5+\cfrac{1}{3}}}}. \tag{1.5}$$

Нетрудно сосчитать, что здесь написано число 165/73. Преобразование обыкновенной дроби в цепную получается последовательным выделением целой части:

$$\frac{165}{73} = 2 + \frac{19}{73} = 2 + \frac{1}{73/19} = 2 + \frac{1}{3 + \frac{16}{19}} = 2 + \frac{1}{3 + \frac{1}{19/16}} =$$

$$= 2 + \frac{1}{3 + \frac{1}{1 + \frac{3}{16}}} = 2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{16/3}}} = 2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{5 + \frac{1}{3}}}}. \quad (1.6)$$

Предположим, что мы хотим найти решение уравнения

$$73x + 165y = 1. \quad (1.7)$$

Оказывается, для этого надо проделать вычисление (1.6), а затем следующее таинственное вычисление:

$$2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{5}}} = 2 + \frac{1}{3 + \frac{5}{6}} = 2 + \frac{6}{23} = \frac{52}{23} \quad (1.8)$$

Ответ готов: $x = 52,\ y = -23$.

Задача 1.4. *Сформулируйте алгоритм в общем виде и обоснуйте его.*

Решение этой задачи, как и многие другие важные результаты о цепных дробях, можно найти, например, в книге Хинчина "Цепные дроби".

Разложение в цепную дробь на самом деле является просто одной из форм записи алгоритма Евклида. Он был изобретен античными математиками для решения задачи о нахождении общей меры двух отрезков, т.е. для нахождения такого отрезка, который укладывался бы в двух данных отрезках целое число раз. Именно с помощью этого алгоритма и было тогда же доказано, что эта задача не всегда разрешима, т.е. что существуют несоизмеримые отрезки. Опишем действие алгоритма Евклида.

Пусть a_0 и a_1 — длины двух отрезков. Отложив отрезок a_1 максимально возможное целое число раз в отрезке a_0, получим деление с остатком a_0 на a_1

$$a_0 = s_0 a_1 + a_2, \quad (1.9)$$

где неполное частное s_0 — натуральное число, а остаток a_2 удовлетворяет неравенству $0 \le a_2 < a_1$. Если на самом деле имеет место равенство $a_2 = 0$, то задача решена и сам отрезок a_1 может служить искомой общей мерой, а если $a_2 > 0$, то для решения задачи достаточно найти общую меру отрезков a_1 и a_2. Для этого, конечно, надо сделать то же самое — разделить с остатком a_1 на a_2:

$$a_1 = s_1 a_2 + a_3, \quad (1.10)$$

где неполное частное s_1 — натуральное число, а остаток a_3 удовлетворяет неравенству $0 \le a_3 < a_2$. После k таких шагов у нас появится k аналогичных равенств:

$$a_{i-1} = s_{i-1} a_i + a_{i+1}, \qquad i = 1, \dots k. \quad (1.11)$$

Из каждого из этих равенств можно выразить отношение a_{i-1}/a_i, поделив i-ое равенство на a_i:

$$\frac{a_{i-1}}{a_i} = s_{i-1} + \frac{a_{i+1}}{a_i}, \qquad i = 1, \dots k, \quad (1.12)$$

а затем переписать то же самое в виде

$$\frac{a_{i-1}}{a_i} = s_{i-1} + \cfrac{1}{\cfrac{a_i}{a_i+1}}, \qquad i = 1, \dots k. \tag{1.13}$$

Получили цепочку равенств:

$$\begin{aligned}
\frac{a_0}{a_1} &= s_0 + \cfrac{1}{\cfrac{a_1}{a_2}},\\
\frac{a_1}{a_2} &= s_1 + \cfrac{1}{\cfrac{a_2}{a_3}},\\
\frac{a_2}{a_3} &= s_2 + \cfrac{1}{\cfrac{a_3}{a_4}},\\
&\dots\\
\frac{a_{k-1}}{a_k} &= s_{k-1} + \cfrac{1}{\cfrac{a_{k+1}}{a_k}}.
\end{aligned} \tag{1.14}$$

Подставляя теперь каждую следующую дробь в предыдущую, получим цепную дробь:

$$\frac{a_0}{a_1} = s_0 + \cfrac{1}{s_1 + \cfrac{1}{s_2 + \cfrac{1}{\dots + \cfrac{1}{s_{k-1} + \cfrac{a_{k+1}}{a_k}}}}} \tag{1.15}$$

1.3. Арифметика остатков.

В вопросах про целые числа также очень существенную роль играют рассуждения "по модулю n". Напомним, что два целых числа называются *сравнимыми по модулю* n, если они дают одинаковые остатки при делении на n (или, что равносильно, их разность делится на n). Этот факт стандартно записывается так: $a \equiv b \pmod n$. Зафиксируем натуральное число $n > 1$. Если нас при вычислениях интересует не сам ответ, а только остаток от деления его на n, то и при вычислениях мы также можем оперировать не с самими числами, а только с их остатками от деления на n. Этот общеизвестный прием основывается на следующей простой лемме:

Лемма 1.2. *Пусть* $a \equiv a' \pmod n$ *и* $b \equiv b' \pmod n$. *Тогда* $a + b \equiv a' + b' \pmod n$ *и* $ab \equiv a'b' \pmod n$.

Задача 1.5. *Докажите эту лемму.*

Следовательно, операции сложения и умножения можно естественно определить на множестве всех возможных остатков от деления на фиксированное натуральное число n. Это множество мы будем обозначать $\mathbb{Z}_n$; иногда удобно обозначать остатки числами с чертой сверху, чтобы отличать их от целых чисел:

$$\mathbb{Z}_n = \{\bar 0, \bar 1, \bar 2, \dots, \overline{n-1}\}. \tag{1.16}$$

Приведем для полноты формальное определение сложения и умножения элементов $\mathbb{Z}_n$: суммой двух остатков $\bar a, \bar b \in \mathbb{Z}_n$ (a, b — целые числа от нуля до $n-1$) называется остаток от деления натурального числа $a + b$ на n; произведением — остаток от деления натурального числа ab на n.

Выпишем очевидные свойства операций сложения и умножения остатков. Здесь $x, b, c \in \mathbb{Z}_n$.

$$\begin{array}{ll} 1) & x+(y+z)=(x+y)+z; \\ 2) & x+y=y+x \\ 3) & x+\bar{0}=\bar{0}+x=x \\ 7) & x(y+z)=xz+xz; \end{array} \qquad \begin{array}{ll} 4) & x(yz)=(xy)z \\ 5) & xy=yx \\ 6) & x\bar{1}=\bar{1}+x=x \end{array} \tag{1.17}$$

Задача 1.6. *Докажите все эти свойства.*[1]

Задача 1.7. *Выпишите и рассмотрите внимательно таблицы сложения и умножения в $\mathbb{Z}_n$, для $n = 2,\ 3,\ 4,\ 5,\ 6,\ 7$ и 8.*

Сразу заметно, что арифметика в $\mathbb{Z}_n$ существенно отличается от привычной арифметики целых чисел. Отметим некоторые наиболее существенные отличия.

Всякий остаток, будучи сложенным сам с собой несколько раз, дает $\bar{0}$. Например, в $\mathbb{Z}_2$ уже $\bar{1}+\bar{1}=\bar{0}$, а, скажем, в $\mathbb{Z}_6$ $\bar{4}+\bar{4}+\bar{4}=\bar{0}$. Наименьшее число раз, которое нужно сложить данный остаток $x \in \mathbb{Z}_n$ с собой, чтобы получить $\bar{0}$, называется его *порядком по сложению*. Таким образом, порядок по сложению остатка $\bar{1} \in \mathbb{Z}_2$ равен 2, а порядок по сложению остатка $\bar{4} \in \mathbb{Z}_6$ равен 3.

Задача 1.8. *Придумайте формулу для вычисления порядка по сложению остатка $\bar{a} \in \mathbb{Z}_n$. (Кроме знаков арифметических действий, можно еще использовать функции* НОК *и* НОД.*)*

Умножение доставляет еще более непривычные ситуации. Во-первых, произведение двух ненулевых остатков иногда оказывается нулем. (Найдите такие примеры в выписанных таблицах умножения!) Такие остатки называются *делителями нуля*.

Задача 1.9. *При каких значениях n в $\mathbb{Z}_n$ встречаются делители нуля? Как узнать, является ли $\bar{a} \in \mathbb{Z}_n$ делителе нуля?*

Некоторые остатки при возведении в некоторую степень дают нуль. (Конечно, это значит, что они являются делителями нуля.) Такие остатки называют *нильпотентными*. (Найдите такие примеры в выписанных таблицах умножения!)

Задача 1.10. *При каких значениях n в $\mathbb{Z}_n$ встречаются нильпотентные элементы? Как узнать, является ли $\bar{a} \in \mathbb{Z}_n$ нильпотентным? Как перечислить все нильпотентные элементы в данном $\mathbb{Z}_n$?*

Задача 1.11. *Докажите, что сумма нильпотентных остатков снова является нильпотентным.*

Некоторые отличные от $\bar{0}$ и $\bar{1}$ остатки при возведении в квадрат не меняются. Такие остатки называют *идемпотентными*. (Найдите такие примеры в выписанных таблицах умножения!)

Задача 1.12. *Докажите, что идемпотентные остатки всегда являются делителями нуля.*

Задача 1.13. *Докажите, что если $x \in \mathbb{Z}_n$ является идемпотентным, то $\bar{1}-x$ тоже.*

Задача 1.14. *При каких значениях n в $\mathbb{Z}_n$ встречаются идемпотентные элементы? Как перечислить все идемпотентные элементы в данном $\mathbb{Z}_n$?*

Теперь давайте обсудим, как в арифметике остатков обстоит дело с двумя остальными арифметическими операциями: вычитанием и делением. Легко понять, что возможность выполнения вычитания равносильна существованию для любого элемента $x \in \mathbb{Z}_n$ противоположного элемента (т.е. такого $y \in \mathbb{Z}_n$, что $x+y=\bar{0}$), а возможность деления — существованию обратного, т.е. такого $z \in \mathbb{Z}_n$, что $xz=\bar{1}$.

---

[1] На всякий случай приведем доказательство ассоциативности сложения. Если $\bar{a}, \bar{b}, \bar{c}$ — три элемента $\mathbb{Z}_n$ (a, b, c — целые числа от нуля до $n-1$) , то остатком при делении на n суммы целых чисел $b+c$ будет по определению остаток $\bar{b}+\bar{c}$, тогда на основании леммы 1.2 остатком от деления на n суммы $a+(b+c)$ будет остаток $\bar{a}+(\bar{b}+\bar{c})$ Аналогично, остатком от деления суммы целых чисел $(a+b)+c$ будет остаток $(\bar{a}+\bar{b})+\bar{c}$. Но поскольку мы знаем, что сложение целых чисел ассоциативно, $a+(b+c)=(a+b)+c$, так что и остатки от деления будут тоже равны.

Задача 1.15. *Пусть $\bar{a} \in \mathbb{Z}_n$, где a — целое число от 0 до $n-1$. Укажите формулу для остатка, противоположного к $\bar{a}$.*

А вот с существованием обратных элементов дело обстоит намного сложнее. Нетрудно понять, что, например, у делителей нуля обратных остатков точно быть не может. (Действительно, если x — делитель нуля x, то существует такой ненулевой остаток y, что $xy = \bar{0}$, и если бы при этом существовал такой z, что $xz = \bar{1}$, то домножив предыдущее равенство на этот остаток z, мы бы получили, что $z(xy) = z\bar{0} = \bar{0}$, но при этом $z(xy) = (zx)y = \bar{1}y = y$. Противоречие, так как y был ненулевым.) Однако рассмотрение таблиц показывает, что в некоторых случаях дело обстоит благополучно.

Пусть $\bar{a} \in \mathbb{Z}_n$, где a — целое число от 0 до $n-1$. Если $z = \bar{t}$ обратный остаток для $\bar{a}$ в $\mathbb{Z}_n$, то $\bar{a}\bar{t} = \bar{1}$ в $\mathbb{Z}_n$, что по определению означает, что натуральное число at дает при делении на n остаток 1. А это в свою очередь по определению деления с остатком означает, что $at = ns + 1$ (здесь s — неполное частное, 1 — остаток). Другими словами, неопределенное уравнение $at - ns = 1$ имеет целочисленные решения, что, согласно теореме 1.1, равносильно тому, что числа a и n взаимно просты. Полученный важный результат мы сформулируем в виде теоремы.

Теорема 1.2. *Остаток $\bar{a} \in \mathbb{Z}_n$ обратим тогда и только тогда, когда целые числа a и n взаимно просты.*

Следствие 1.1. *Если p — простое число, то все ненулевые остатки в $\mathbb{Z}_p$ обратимы.*

Следствие показывает, что при простом p арифметика остатков наиболее похожа на привычную нам арифметику: в $\mathbb{Z}_p$ определены все четыре привычные нам арифметические действия. Мы подробно обсудим значение этого обстоятельства в следующем разделе.

Задача 1.16. *Докажите, что при простом p в $\mathbb{Z}_p$ любое уравнение первой степени $\alpha x + \beta = \bar{0}$ при ненулевом α имеет единственное решение.*

Задача 1.17. *Покажите, что если число n не простое, то уравнение $\alpha x + \beta = \bar{0}$ при ненулевом α может как не иметь решений, так и иметь несколько решений. Как по $\alpha = \bar{a}$, $\beta = \bar{b}$ и n указать число решений этого уравнения?*

Рассмотрим простейшее квадратное уравнение $x^2 = \bar{1}$.

Задача 1.18. *Докажите, что при простом p это уравнение имеет ровно два решения в $\mathbb{Z}_p$.*

Задача 1.19. *Докажите, что при $n = 2^k$, $k > 2$, это уравнение имеет ровно четыре решения в $\mathbb{Z}_n$.*

Задача 1.20. *Докажите, что для любого натурального N существует такое n, что это уравнение имеет в $\mathbb{Z}_n$ не менее N решений.*

А как обстоит дело с извлечением корня? Напомним, что в обычной арифметике действительных чисел квадратный корень можно извлекать только из положительных чисел. В арифметике остатков по простому модулю ситуация похожая: корни извлекаются ровно из половины ненулевых остатков, хотя, в отличие от действительных чисел, эта половина не имеет простого описания.

Задача 1.21. *Докажите, что при простом $p \neq 2$ ровно половина ненулевых остатков в $\mathbb{Z}_p$ является квадратами.*

Задача 1.22. *При каких простых p остаток $-\bar{1}$ является квадратом в $\mathbb{Z}_p$?*

Задача 1.23. *а) Докажите, что при простом p любое квадратное уравнение с коэффициентами из $\mathbb{Z}_p$ имеет в $\mathbb{Z}_p$ не более двух корней.*
б) Объясните, в каком месте доказательство из предыдущего пункта перестает быть верным при не простом p.
в) Верна ли теорема Виета для квадратных уравнений с коэффициентами в $\mathbb{Z}_n$?
г) Объясните, как и в какой мере можно пользоваться в $\mathbb{Z}_n$ школьными формулами для корней квадратного уравнения.

Задача 1.24. *Придумайте алгебраическое уравнение вида* $x^k + a_1 x^{k-1} + \ldots a_{k-1}x + a_k = 0$ *наименьшей возможной степени* k *с коэффициентами из* $\mathbb{Z}_n$*, которое имело бы в* $\mathbb{Z}_n$ *ровно* n *различных корней,*
а) для $n = 101$*;* *б) для* $n = 111$*;* *в) для* $n = 121$.

Задача 1.25. *1) Верно ли, что если сумма квадратов двух целых чисел делится на 7, то каждое из этих чисел делится на 7?*

2) Верно ли, что если сумма квадратов двух целых чисел делится на 13, то каждое из этих чисел делится на 13?

3) Верно ли, что если сумма кубов трех целых чисел делится на 7, то хоть одно из этих чисел делится на 7?

Задача 1.26. *Докажите теорему Вильсона: при простом* p $(p-1)! \equiv -1 \pmod{p}$.

Задача 1.27. *а) Вычислите произведение всех ненулевых остатков в в* $\mathbb{Z}_p$ *при простом* p.
б) Вычислите произведение всех обратимых остатков в* $\mathbb{Z}_n$.

Как узнать число обратимых остатков в $\mathbb{Z}_n$? Ответ называется функцией Эйлера и обозначается $\varphi(n)$. Как следует из теоремы 1.2,

$$\varphi(n) = \text{количество натуральных чисел, меньших } n \text{ и взаимно простых с } n. \tag{1.18}$$

Если n — простое число, то $\varphi(n) = n - 1$.

Задача 1.28. *Вычислите* $\varphi(n)$ *для* $n = 2, 3, 4, \ldots, 10$.

Задача 1.29. *Вычислите* $\varphi(2^m)$.

Задача 1.30. *Вычислите* $\varphi(p^m)$*, где* p *— простое число.*

Задача 1.31. *Докажите, что если числа* k *и* m *взаимно просты, то* $\varphi(km) = \varphi(k)\varphi(m)$.

Задача 1.32. *Докажите, что если остаток обратим в* $\mathbb{Z}_n$*, то некоторая его степень дает единицу.*

Наименьшая положительная степень, при возведении в которую остаток дает единицу, называется его *порядком по умножению.*

Задача 1.33. *Докажите, что если обратимый остаток в некоторой степени дает единицу, то эта степень делится на его порядок по умножению.*

Задача 1.34. *Какие порядки по умножению могут иметь ненулевые остатки в* $\mathbb{Z}_p$ *при простом* p*?*

Задача 1.35. *Какие порядки по умножению могут иметь обратимые остатки в* $\mathbb{Z}_n$*?*

Задача 1.36. *Докажите Малую теорему Ферма: при простом* p *и* $(a, p) = 1$, $a^{p-1} \equiv 1 \pmod{p}$.

Задача 1.37. *Докажите, что если* $(a, p) = 1$*, то* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Задача 1.38. *1) Найдите остаток от деления* $2^{2010} + 3^{2010}$ *на* 13.

2) Докажите, что $2^{100} + 3^{100}$ *делится на* 97.

3) Найдите остаток от деления $2007^{2008^{2009}}$ *на* 11.

2. Поля и кольца. Знакомство.

В школе изучались, в основном, действительные числа. Для алгебраических задач было существенно, что с ними можно выполнять четыре основные действия арифметики: сложение, вычитание, умножение и деление. В некоторых задачах необходимо было работать с целыми числами, и сложность этих задач часто оказывалась связанной с тем, что там не определена операция деления. (Точнее сказать, что операция деления определена на большем множестве рациональных чисел, и отношение двух целых чисел может оказаться не целым числом[2].) В школе встречались и другие математические объекты, для которых были определены некоторые из четырех действий арифметики. Например, векторы можно складывать и вычитать, но для них не определялось операции умножения (скалярное произведение на роль такого умножения не подходит, потому что скалярное произведение двух векторов — это уже объект другой природы: не вектор, а действительное число). Также можно было складывать, вычитать и умножать функции, но с делением возникали проблемы, если функция где-то обращалась в нуль. В прошлом разделе появился еще один пример такого рода — множества остатков $\mathbb{Z}_n$. Как мы видели, остатки можно складывать, вычитать и умножать, а при простом n еще и делить.

Для единообразного обсуждения таких случаев нужно дать единое определение, под которое подходили бы интересующие нас случаи. Оптимальной представляется ситуация, когда можно выполнять все четыре действия арифметики, поскольку этом случае все привычные со школы приемы работы с алгебраическими выражениями. Соответствующее понятие называется *полем*. Однако часто необходимо рассматривать ситуацию, когда определены сложение, вычитание и умножение. Для этого вводится понятие *кольца*.

2.1. Бинарные операции.

Однако перед тем, как давать формальное определение поля и кольца, следует уточнить еще один термин, который мы уже употребляли, апеллируя к его обычному значению, которое, впрочем, вполне соответствует приводимому ниже формальному определению. Это понятие операции, или, точнее, *бинарной операции на множестве*.

Определение 2.1. *Бинарной операцией на множестве A называется любое правило, которое сопоставляет любым двум элементам a и b множества A новый элемент множества A, который называется результатом применения операции к элементам a и b.*

В наших лекциях никаких операций, кроме бинарных, не встречается, поэтому прилагательное "бинарный" мы будем опускать. Большинство доступных нам на сегодняшний день примеров бинарных операций — это операции, определенные на подмножествах множества действительных чисел $\mathbb{R}$. Так, на самом множестве $\mathbb{R}$ действительных чисел определены операции сложения, вычитания и умножения, а вот операция деления не определена (нельзя делить на ноль). Ситуацию с делением легко исправить: операция деления определена на множестве $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ ненулевых действительных чисел. На множестве целых чисел $\mathbb{Z}$ определены операции сложения, вычитания и умножения, а вот операция деления не определена, даже если перейти, как в предыдущем примере, к меньшему множеству $\mathbb{Z} \setminus \{0\}$. А вот на множестве геометрических векторов плоскости определены, как мы уже упоминали, операции сложения и вычитания, а вот скалярное произведение, с точки зрения нашего определения бинарной операцией не является, поскольку двум векторам при этом сопоставляется не вектор, как требуется в определении 2.1, а элемент совсем другого множества — действительное число.

Еще один важный пример — это множество отображений некоторого фиксированного множества X в себя с операцией композиции (т.е. подстановки функции в функцию). Напомним формальное определение: если f и g — два отображения множества X в себя, то их композицией называется отображение множества X в себя, сопоставляющее каждому $x \in X$ элемент $f(g(x))$.

[2] В таком случае говорят, что подмножество целых чисел в $\mathbb{Q}$ не замкнуто относительно операции деления.

Для операции композиции имеется стандартное обозначение: композиция f и g обозначается $f \circ g$, так что $f \circ g(x) = f(g(x))$. Обратите внимание, что тут важен порядок: если, скажем, X — это множество действительных чисел $\mathbb{R}$, f — это функция синус ($f(x) = \sin x$), а g — возведение в квадрат ($g(x) = x^2$), то $f(g(x)) = \sin(x^2)$, $g(f(x)) = \sin^2 x$ — две совершенно разные функции.

Определение 2.2. *Бинарная операция $*$ на множестве A называется коммутативной, если для любых двух элементов $a, b \in A$*

$$a * b = b * a. \tag{2.1}$$

Так, например, операции сложения и умножения на множестве целых чисел коммутативны, а операция вычитания на множестве целых чисел — нет: $a - b \neq b - a$. Как мы видели, операция композиции на множестве отображений множества действительных чисел $\mathbb{R}$ в себя не коммутативна.

Задача 2.1. *Покажите, что если множество X содержит больше одного элемента, то операция композиции на множестве отображений множества X в себя не коммутативна.*

Определение 2.3. *Бинарная операция $*$ на множестве A называется ассоциативной, если для любых трех элементов $a, b, c \in A$*

$$(a * b) * c = a * (b * c). \tag{2.2}$$

Так, например, операции сложения и умножения на множестве целых чисел ассоциативны, а операция возведения в степень на множестве натуральных чисел — нет ($(a^b)^c \neq a^{(b^c)}$).

Задача 2.2. *Придумайте коммутативную, но не ассоциативную операцию.*

Задача 2.3. *Придумайте ассоциативную, но не коммутативную операцию.*

Отметим, что только благодаря тому, что операции сложения и умножения ассоциативны, мы можем говорить о сумме и произведении трех слагаемых или сомножителей, не уточняя, в каком порядке выполняются операции. (А вот про разность трех чисел никто никогда не говорит...) А если бы операция была не ассоциативна, то выражения $(a*b)*c$ и $a*(b*c)$, которые, вообще говоря, не обязаны быть равными, с равным правом могли бы претендовать на роль "произведения" трех сомножителей. А для "произведения" четырех сомножителей уже имеется целых пять вариантов: $((a * b) * c) * d$, $(a * (b * c)) * d$, $a * ((b * c) * d)$, $a * (b * (c * d))$ и $(a * b) * (c * d)$.

Задача 2.4. * *Сколькими различными способами можно расставить $n - 2$ пары скобок в произведении $a_1 * a_2 * \ldots a_n$, так чтобы порядок выполнения действий был определен однозначно? (Менять порядок сомножителей нельзя!)*

Задача 2.5. *Докажите, что если операция ассоциативна, то все различные способы расстановки скобок в произведении $a_1 * a_2 * \ldots a_n$ дают один и тот же результат. (Менять порядок сомножителей по-прежнему нельзя!)*

Определение 2.4. *Элемент $\varepsilon \in A$ называется нейтральным элементом для заданной на множестве A бинарной операции $*$, если для любого $a \in A$*

$$a * \varepsilon = \varepsilon * a = a. \tag{2.3}$$

Для определенной на каком-нибудь числовом множестве операции сложения нейтральным элементом всегда является нуль, для умножения — единица; для многих операций (например, для вычитания) нейтрального элемента не существует.

Задача 2.6. *Докажите, что в любом множестве с бинарной операцией имеется не более одного нейтрального элемента.*

Задача 2.7. *Существует ли нейтральный элемент для следующих операций на множествах:*

1) *Операция композиции на множестве отображений множества X в себя;*

2) *Операция* $\max(a,b)$ *на множестве неотрицательных действительных чисел* $[0;+\infty)$*;*

3) *Операция* $\max(a,b)$ *на множестве всех действительных чисел* $\mathbb{R}$*;*

4) *Операция* НОД(a,b) *на множестве натуральных чисел* $\mathbb{N}$*;*

5) *Операция* НОК(a,b) *на множестве натуральных чисел* $\mathbb{N}$*;*

6) *Операция умножения на множестве всех периодических функций из* $\mathbb{R}$ *в* $\mathbb{R}$*, имеющих период* 2π*;*

7) *Операция объединения множеств на множестве*[3] $\mathcal{B}(\Omega)$*;*

8) *Операция пересечения множеств на множестве* $\mathcal{B}(\Omega)$*;*

9) *Операция симметрической разности множеств* $(A \oplus B = (A \setminus B) \cup (B \setminus A))$ *на множестве* $\mathcal{B}(\Omega)$*.*

2.2. Поля.

Теперь, наконец, мы дадим давно обещанное определение поля.

Определение 2.5. *Множество* $\mathbb{K}$ *вместе с введенными на нем операциями сложения* $(+)$ *и умножения* $(\cdot)$ *называется* **полем***, если эти операции коммутативны, ассоциативны, обладают нейтральными элементами, которые называются* 0 *и* 1*, причем* $0 \neq 1$*, и, кроме того, выполняются следующие три свойства:*

Дистрибутивность умножения $\forall a,b,c \in \mathbb{K} \quad a(b+c) = ab + ac$*;*

Существование противоположного элемента для сложения $\forall a \in \mathbb{K}\ \exists -a \in \mathbb{K}$ *такой что* $a + (-a) = 0$*;*

Существование обратного элемента для умножения $\forall a \in \mathbb{K}, a \neq 0,\ \exists a^{-1} \in \mathbb{K}$ *такой что* $aa^{-1} = 1$*.*

Нетрудно понять, что в это определение заложены именно те свойства, которые позволяют в поле производить все алгебраические выкладки, к которым мы привыкли в школе.

Задача 2.8. *1) Докажите, что в произвольном поле* $(-a)b = -ab$*. В частности,* $(-1)a = -a$*.*
2) Докажите, что в произвольном поле если $ab = 0$*, то либо* $a = 0$*, либо* $b = 0$*. (Другими словами, делителей нуля, с которыми мы столкнулись при знакомстве с арифметикой остатков, в поле не бывает.)*
3) Докажите, что в произвольном поле умножение на ноль всегда дает ноль: $a0 = 0$*.*

Собственно, в школе более или менее подробно рассматривались два важных примера полей: поле рациональных чисел $\mathbb{Q}$ и поле действительных чисел $\mathbb{R}$. При этом одно из этих полей является подмножеством другого; для таких случаев имеется понятие *подполя*.

Определение 2.6. *Подмножество* $\mathbb{L}$ *поля* $\mathbb{K}$ *называется подполем если оно само является полем относительно тех же операций, что и* $\mathbb{K}$ *(и, следовательно, содержит ноль и единицу поля* $\mathbb{K}$*).*

Задача 2.9. *Докажите, что в* $\mathbb{Q}$ *нет меньших подполей.*

Зато в $\mathbb{R}$ имеется много разных подполей.

[3] Через $\mathcal{B}(\Omega)$ здесь и далее обозначается множество всех подмножеств данного множества Ω.

Задача 2.10. *1) Докажите, что множество действительных чисел вида $a+b\sqrt{2}$, $a,b\in\mathbb{Q}$ является подполем в $\mathbb{R}$.*
2) Является ли множество действительных чисел вида $a+b\sqrt[3]{2}$, $a,b\in\mathbb{Q}$ подполем в $\mathbb{R}$? Как описать наименьшее подполе в $\mathbb{R}$, содержащее все такие числа?
3) Описать наименьшее подполе в $\mathbb{R}$, содержащее $\sqrt{2}$ и $\sqrt{3}$.
4) Найдите все подполя поля из п. 3.

В поле действительных чисел имеются и существенно большие подполя. Сейчас мы опишем подполе, которое в честь Евклида обозначим E. Рассмотрим евклидову плоскость и зафиксируем на ней единичный отрезок. Множество E будет состоять из длин всех отрезков, которые можно построить циркулем и линейкой, нуля и всех противоположных им чисел.

Задача 2.11. *1) Докажите, что E является подполем в $\mathbb{R}$.*
2) Докажите, что если $x\in E$, $x>0$, то $\sqrt{x}\in E$.
**3) Докажите, что $E\neq\mathbb{R}$.*

Отметим, что одно из решений последнего пункта предыдущей задачи дается классической теоремой о невозможности удвоения куба циркулем и линейкой (т.е. $\sqrt[3]{2}\notin E$). Намного труднее доказывается невозможность квадратуры круга (т.е. утверждение, что $\sqrt{\pi}\notin E$).

Нельзя не упомянуть о еще большем подполе в $\mathbb{R}$, которое называется *полем вещественных алгебраических чисел*. Оно состоит из всех действительных корней всех возможных алгебраических уравнений с целыми коэффициентами. Обозначим его $\overline{\mathbb{Q}}_{\mathbb{R}}$.

Задача 2.12. *1) Докажите, что $\overline{\mathbb{Q}}_{\mathbb{R}}$ является подполем в $\mathbb{R}$.*
2) Докажите, что E является подполем в $\overline{\mathbb{Q}}_{\mathbb{R}}$.
**3) Докажите, что $\overline{\mathbb{Q}}_{\mathbb{R}}\neq\mathbb{R}$.*

Отметим, что, в то время как, очевидно, $\sqrt[3]{2}\overline{\mathbb{Q}}_{\mathbb{R}}$, $\sqrt{\pi}\notin\overline{\mathbb{Q}}_{\mathbb{R}}$ и $\pi\notin\overline{\mathbb{Q}}_{\mathbb{R}}$; такие числа называются трансцендентными.

Кроме подполей $\mathbb{R}$, у нас имеется еще одна серия примеров совсем другого рода. Это множества $\mathbb{Z}_p$ остатков по простому модулю p с введенными в прошлом разделе операциями сложения и умножения.

Задача 2.13. *Укажите, где в прошлом разделе доказано, что при простом p $\mathbb{Z}_p$ является полем.*

Для этих полей имеется другое общепринятое обозначение $\mathbb{F}_p$, которое мы будем использовать чаще, чем $\mathbb{Z}_p$.

Поля $\mathbb{Q}$ и $\mathbb{F}_p$ называют *простыми полями* по следующей причине.

Задача 2.14. *Докажите, что в $\mathbb{Q}$ и $\mathbb{F}_p$ нет меньших подполей.*

С другой стороны, нетрудно понять, что любое поле содержит в качестве подполя одно из простых полей. Для того, чтобы точно сформулировать это утверждение, нам нужно дать еще одно определение: надо объяснить, какие поля мы будем считать одинаковыми.

Определение 2.7. *Поле $\mathbb{L}$ называется изоморфным полю $\mathbb{K}$, если существует взаимно-однозначное отображение $\varphi:\mathbb{L}\to\mathbb{K}$, согласованное с операциями сложения и умножения, т.е. такое, что $\varphi(a+b)=\varphi(a)+\varphi(b)$ и $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$. Само взаимно-однозначное отображение φ при этом называется изоморфизмом между полями $\mathbb{L}$ и $\mathbb{K}$.*

Задача 2.15. *Докажите, что при изоморфизме полей $\varphi(-a)=-\varphi(a)$, $\varphi(0)=0$ и $\varphi(1)=1$.*

Давайте теперь докажем, что всякое поле содержит подполе, изоморфное $\mathbb{Q}$ и $\mathbb{F}_p$ при какомнибудь p. Возьмем произвольное поле $\mathbb{K}$, согласно определению, оно содержит ненулевой элемент **1**. Обратите внимание, что это не действительное число 1, а обозначаемый тем же символом элемент поля $\mathbb{K}$, и чтобы подчеркнуть эту разницу, мы в этом рассуждении будем единичный элемент

поля $\mathbb{K}$ (а заодно и нулевой) обозначать жирным шрифтом, а число 1 (и число ноль) — обычным шрифтом. Любое подполе в $\mathbb{K}$ должно содержать элемент $\mathbf{1}$, и, следовательно, все его кратности, а также противоположные к ним элементы. Далее, в любом подполе должны еще содержаться всевозможные отношения этих кратностей (конечно, только с ненулевым знаменателем!). Собственно, это та самая программа, по которой в начальной школе от натуральных чисел переходили к целым и затем к рациональным. В нашей чуть более общей ситуации нужно просмотреть каждый шаг более внимательно.

Итак, рассмотрим в поле $\mathbb{K}$ последовательность элементов

$$\begin{array}{l} \mathbf{0} \\ \mathbf{1} \\ \mathbf{1}+\mathbf{1} \\ \mathbf{1}+\mathbf{1}+\mathbf{1} \\ \dots \\ \mathbf{1}+\mathbf{1}+\dots+\mathbf{1} \\ \dots \end{array} \tag{2.4}$$

Отметим, что, хотя мы ничего не знаем о том, как определены операции сложения и умножения в поле $\mathbb{K}$, складывать и вычитать элементы этой последовательности мы умеем.

Задача 2.16. *Докажите, что*

$$(\underbrace{\mathbf{1}+\mathbf{1}+\dots+\mathbf{1}}_{n})+(\underbrace{\mathbf{1}+\mathbf{1}+\dots+\mathbf{1}}_{m})=\underbrace{\mathbf{1}+\mathbf{1}+\dots+\mathbf{1}}_{n+m}; \tag{2.5}$$

$$(\underbrace{\mathbf{1}+\mathbf{1}+\dots+\mathbf{1}}_{n})\cdot(\underbrace{\mathbf{1}+\mathbf{1}+\dots+\mathbf{1}}_{m})=\underbrace{\mathbf{1}+\mathbf{1}+\dots+\mathbf{1}}_{nm}. \tag{2.6}$$

Возможны два варианта: либо в последовательности (2.4) все элементы разные, либо в ней имеются повторения.

Рассмотрим сначала первый вариант: в (2.4) все элементы разные. В этом случае мы по существу нашли в нашем поле натуральный ряд, и поэтому все что делалось в начальной школе при переходе от натуральных чисел к рациональным, можно здесь повторить практически дословно. Во-первых, у каждого элемента из последовательности (2.4) имеется противоположный элемент; нетрудно проверить, что ни один из них не совпадает ни с каким элементом (2.4), так что в результате мы имеем в $\mathbb{K}$ подмножество, находящееся во взаимно-однозначном соответствии с множеством целых чисел. Осталось рассмотреть всевозможные их отношения (с ненулевым знаменателем), и проверить,[4] что множество элементов

$$\mathbb{L}=\left\{\mathbf{0},\pm(\underbrace{\mathbf{1}+\mathbf{1}+\dots+\mathbf{1}}_{n})/(\underbrace{\mathbf{1}+\mathbf{1}+\dots+\mathbf{1}}_{m}),\quad m,n\in N\right\}\subset\mathbb{K} \tag{2.7}$$

образует подполе в $\mathbb{K}$. Конечно, имеется естественный изоморфизм между полем рациональных чисел и $\mathbb{L}$. Проще всего определить взаимно-однозначное отображение $\varphi:\mathbb{Q}\to\mathbb{K}$ следующим образом. Каждое положительное рациональное число $x\in\mathbb{Q}$ можно однозначно представить в виде несократимой дроби $x=p/q$, $p,q\in\mathbb{N}$. Тогда положим

$$\varphi(x)=(\underbrace{\mathbf{1}+\mathbf{1}+\dots+\mathbf{1}}_{p})/(\underbrace{\mathbf{1}+\mathbf{1}+\dots+\mathbf{1}}_{q}). \tag{2.8}$$

Далее, положим $\varphi(0)=\mathbf{0}$ и $\varphi(x)=-\varphi(-x)$ для $x<0$.

Задача 2.17. *Докажите, что $\mathbb{L}$ является подполем поля $\mathbb{K}$, а φ — изоморфизмом между $\mathbb{Q}$ и $\mathbb{L}$.*

[4] Проверьте!

Теперь разберем второй, менее привычный случай: если в последовательности (2.4) имеются совпадения. Предположим, что первым от начала последовательности совпадением оказалось равенство $\underbrace{\mathbf{1}+\mathbf{1}+\ldots+\mathbf{1}}_{m} = \underbrace{\mathbf{1}+\mathbf{1}+\ldots+\mathbf{1}}_{m+p}$, $m \geq 0$, $p > 0$ Если бы m не равнялось нулю, то, прибавляя к обеим частям равенства один и тот же элемент $-\mathbf{1} \in \mathbb{K}$, мы бы получили более раннее равенство $\underbrace{\mathbf{1}+\mathbf{1}+\ldots+\mathbf{1}}_{m-1} = \underbrace{\mathbf{1}+\mathbf{1}+\ldots+\mathbf{1}}_{m+p-1}$, так что $m = 0$ и самое первое совпадение элементов последовательности имеет вид $\underbrace{\mathbf{1}+\mathbf{1}+\ldots+\mathbf{1}}_{p} = \mathbf{0}$, и, следовательно, предыдущие p членов последовательности (2.4) все различны. Рассмотрим теперь подмножество

$$\mathbb{L} = \left\{ \mathbf{0}, \mathbf{1}, \mathbf{1}+\mathbf{1}, \ldots, \underbrace{\mathbf{1}+\mathbf{1}+\ldots+\mathbf{1}}_{p-1} \right\} \subset \mathbb{K}. \tag{2.9}$$

Нетрудно понять, что формулы (2.5) и (2.6) задают такие же правила сложения и умножения в $\mathbb{L}$, как были в прошлом разделе определены для $\mathbb{Z}_p$. Осталось только понять, почему число p обязательно должно быть простым. Предположим, что это не так, $p = mn$, причем $m < p$ и $n < p$. Это значит, что элементы поля $\mathbb{K}$ $a = \underbrace{\mathbf{1}+\mathbf{1}+\ldots+\mathbf{1}}_{m}$ и $b = \underbrace{\mathbf{1}+\mathbf{1}+\ldots+\mathbf{1}}_{n}$ отличны от нуля (т.к. они оба содержатся в списке (2.9), но при этом по формуле (2.6) $ab = 0$ что, как мы видели в задаче 2.8, дает искомое противоречие. Следовательно, мы доказали, что число p простое, и повторение рассуждений предыдущего раздела показывает, что множество $\mathbb{L}$ (2.9) уже является полем. Теперь осталось только предъявить изоморфизм $\varphi : \mathbb{F}_p \to \mathbb{L}$. Он, конечно, задается так же, как и в предыдущем случае, даже проще, поскольку теперь мы можем не заботиться о дробях: если $\bar{m} \in \mathbb{F}_p$ (m — натуральное число от 0 до $p-1$), то

$$\varphi(\bar{m}) = \underbrace{\mathbf{1}+\mathbf{1}+\ldots+\mathbf{1}}_{m}. \tag{2.10}$$

Задача 2.18. *Докажите, что $\mathbb{L}$ — подполем $\mathbb{L}$ поля $\mathbb{K}$, а φ — изоморфизм между $\mathbb{F}_p$ и $\mathbb{L}$.*

Обратим внимание на очень важный факт: число p определяется полем $\mathbb{K}$ однозначно: это наименьшее положительное число p, такое, что $\underbrace{\mathbf{1}+\mathbf{1}+\ldots+\mathbf{1}}_{p} = \mathbf{0}$. Это число называется *характеристикой* поля $\mathbb{K}$ и обозначается $p = \operatorname{char}\mathbb{K}$; если же такого числа p не существует (т.е. имеет место первый из рассмотренных нами случаев, когда все элементы (2.4) различны), то полагают по определению $\operatorname{char}\mathbb{K} = 0$.

Задача 2.19. *Докажите, что при определении характеристики вместо единицы можно было взять любой ненулевой элемент поля. Другими словами, требуется доказать, если a — любой ненулевой элемент поля характеристики ноль, то любая его кратность отлична от нуля, а если a — любой ненулевой элемент поля характеристики $p > 0$, то $\underbrace{a+a+\ldots+a}_{m} = 0$ равносильно тому, что m кратно p.*

Задача 2.20. *Докажите, что в поле характеристики $p > 0$ $(a+b)^p = a^p + b^p$.*

Итак, характеристика поля — это либо простое число, либо ноль. Доказанный факт сформулируем в виде теоремы.

Теорема 2.1. *Любое поле характеристики ноль содержит подполе, изоморфное полю $\mathbb{Q}$, а любое поле характеристики p содержит подполе, изоморфное $\mathbb{F}_p$.*

Надо признаться, что эта теорема доказана несколько "впрок": у нас пока нет примеров полей отличных от подполей поля действительных чисел для характеристики ноль и $\mathbb{F}_p$ в характеристике p. Позже у нас появится много других важных и интересных примеров, а пока мы перейдем к следующему общему понятию, обобщающему такие случаи, как множество целых чисел или $\mathbb{Z}_n$ при непростом n.

Определение 2.8. *Множество S вместе с введенными на нем операциями сложения $(+)$ и умножения $(\cdot)$ называется* **кольцом**, *если операция сложения коммутативна, ассоциативна, обладают нейтральным элементом, который называется* 0 *и, кроме того, выполняются следующие два свойства:*

Дистрибутивность $\forall a, b, c \in \mathbb{K} \quad a(b+c) = ab + ac$ *и* $(b+c)a = ba + ca$ *;*

Существование противоположного элемента для сложения $\forall a \in \mathbb{K}\ \exists -a \in \mathbb{K}$ *такой что* $a + (-a) = 0$*;*

Как мы видим, в определении кольца намного меньше ограничений на операцию умножения, чем в определении поля. Однако часто удобнее наложить еще некоторые ограничения и работать с кольцами более специального вида.

Определение 2.9. *1) Кольцо называется* **коммутативным**, *если операция умножения в нем коммутативна.*
2) Кольцо называется **ассоциативным**, *если операция умножения в нем ассоциативна.*
3) Кольцо называется **кольцом с единицей**, *если в нем существует нейтральный элемент относительно операции умножения, который в таком случае всегда называется единицей.*

В этих лекциях будем работать **только с коммутативными ассоциативными кольцами с единицей**, которые мы будем для краткости называть просто **кольцами**; редкие отступления от этой договоренности будут оговорены особо.

Как мы уже упоминали, первые примеры колец — это кольцо целых чисел $\mathbb{Z}$ и кольца вычетов $\mathbb{Z}_n$.

Задача 2.21. *1) Докажите, что в произвольном кольце $(-a)b = -ab$. В частности, $(-1)a = -a$.*
2) Докажите, что в произвольном кольце умножение на ноль всегда дает ноль: $a0 = 0$.

Эта задача показывает, что в кольцах, как и в полях, тоже можно производить многие привычные алгебраические выкладки. Перестает быть верным только второй пункт задачи 2.8: из того, что $ab = 0$, может вовсе не следовать, что хоть один из сомножителей равен нулю. Ненулевой элемент кольца называется *делителем нуля*, если произведение его на какой-нибудь другой элемент кольца дает ноль. ($a \neq 0$, $b \neq 0$, но $ab = 0$.) Мы уже встречали примеры делителей нуля в кольцах вычетов $\mathbb{Z}_n$. Многие другие обсуждавшиеся на примере колец $\mathbb{Z}_n$ понятия также определяются для произвольных колец.

Определение 2.10. *Элемент кольца называется нильпотентным, если некоторая его степень равна нулю. ($a \neq 0$, но $a^n = 0$.)*

Определение 2.11. *Отличный от нуля и единицы элемент кольца называется идемпотентным, если он равен своему квадрату. ($a \neq 0, 1$, и $a^2 = a$.)*

Определение 2.12. *Ненулевой элемент кольца называется обратимым, если для него существует обратный элемент относительно умножения. ($a \neq 0$, $\exists a^{-1}$, так что $aa^{-1} = 1$.)*

Задача 2.22. *Верно ли, что*

1) *произведение двух обратимых элементов является обратимым элементом?*

2) *если произведение двух элементов является обратимым элементом, то хотя бы один сомножитель является обратимым элементом?*

3) *если произведение двух элементов является обратимым элементом, то оба сомножителя являются обратимыми элементами?*

4) *если произведение двух элементов является делителем нуля, то оба сомножителя являются делителями нуля?*

5) *если произведение двух элементов является делителем нуля, то хотя бы один сомножитель является делителем нуля?*

6) *произведение двух нильпотентных элементов является нильпотентным элементом?*

7) *если произведение двух элементов является нильпотентным, то хотя бы один сомножитель является нильпотентным?*

8) *произведение любого элемента на нильпотентный является нильпотентным?*

9) *произведение двух идемпотентных элементов, является идемпотентным?*

10) *сумма двух обратимых элементов снова является обратимым?*

11) *сумма двух делителей нуля снова является делителем нуля?*

12) *сумма двух нильпотентных элементов снова является нильпотентным?*

13) *сумма двух идемпотентных элементов снова является идемпотентным?*

Задача 2.23. *Докажите, что идемпотентные элементы всегда являются делителями нуля.*

Задача 2.24. *Докажите, что если элемент кольца x является идемпотентным, то $1-x$ тоже является идемпотентным.*

Приведем теперь несколько других примеров колец.

Задача 2.25. *Докажите, что следующие множества с заданными на них операциями сложения и умножения являются кольцами (коммутативными ассоциативными и с единицей!). Найдите в них все делители нуля, нильпотентные и идемпотентные элементы (если таковые есть).*

1) *Множество всех непрерывных функций из $\mathbb{R}$ в $\mathbb{R}$ с обычными операциями сложения и умножения функций.*

2) *Множество всех непрерывных функций из $\mathbb{R}\setminus\{0\}$ в $\mathbb{R}$ с обычными операциями сложения и умножения функций.*

3) *Множество $\mathcal{B}(\Omega)$ всех подмножеств данного множества Ω; в качестве операции сложения берется симметрическая разность двух множеств, а в качестве умножения — пересечение.*

4) *Множество всех линейных функций из $\mathbb{R}$ в $\mathbb{R}$ (т.е. всех $f(x)=kx+b$, $k,b\in\mathbb{R}$); в качестве сложения берется обычное сложение функций, а умножение определяется следующим геометрическим способом. Две линейные функции перемножаются обычным образом, получается квадратный трехчлен, графиком которого является парабола (или прямая, если один из сомножителей был константой). К полученному графику проводится касательная в точке его пересечения с осью ординат; уравнение полученной прямой виде $f(x)=kx+b$ и называется произведением двух исходных функций в этом кольце.*[5]

[5]Этот пример не является искусственным, как это может показаться на первый взгляд. Если нас интересуют только очень близкие к нулю значения переменной x, то при вычислениях естественно пренебрегать слагаемыми, в которые входит x во второй (и большей) степени. Докажите, что это приводит как раз к умножению, введенному в первой части задачи. Если же нас интересуют более точные вычисления, мы можем рассматривать квадратичные по x выражения и пренебрегать слагаемыми начиная с третьего порядка малости. Опишите получающееся таким образом кольцо.

5) *Множество векторов плоскости, на которой введена прямоугольная система координат. В качестве сложения берется обычное сложение векторов, а умножение (которое мы в этой задаче, чтобы не создавать путаницы, будем обозначать звездочкой) определяется следующим образом. Если два вектора $\vec{u}$ и $\vec{v}$ имеют координаты $\vec{u} = (a; b)$ то $\vec{v} = (c; d)$ то $\vec{u} * \vec{v} = (ac; bd)$.*

6) *Изменим в условиях предыдущей задачи закон умножения: $\vec{u} * \vec{v} = (ac - bd; ad + bc)$.*

7) *Докажите, что кольца из последних трех пунктов попарно не изоморфны друг другу.*

Как и в случае полей, для колец естественно вводится понятие изоморфизма.

Определение 2.13. *Кольцо A называется изоморфным кольцу B, если существует взаимно-однозначное отображение $\varphi : A \to B$, согласованное с операциями сложения и умножения и переводящее единицу кольца A в единицу кольца B, т.е. такое, что $\varphi(1) = 1$, $\varphi(a + b) = \varphi(a) + \varphi(b)$ и $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Само взаимно-однозначное отображение φ при этом называется изоморфизмом между кольцами A и B.*

Задача 2.26. *Докажите, что при изоморфизме колец $\varphi(-a) = -\varphi(a)$ и $\varphi(0) = 0$.*

Задача 2.27. *1) Докажите, что любое кольцо из двух элементов изоморфно $\mathbb{Z}_2$.*
2) Докажите, что любое кольцо из трех элементов изоморфно $\mathbb{Z}_3$.
3) Перечислите (с точностью до изоморфизма) все кольца, состоящие из четырех элементов.

Задача 2.28. * *Заметим, что примеры колец из п. 5 и 6 задачи 2.25 построены похожим образом. Естественно спросить, какие еще кольца можно так получить. Зафиксируем какие-нибудь действительные числа α_1, α, β_1, β, γ_1, γ, δ_1 и δ_2 и определим закон умножения на множестве векторов плоскости следующим образом: $\vec{u} * \vec{v} = (\alpha_1 ac + \beta_1 bc + \gamma_1 ad + \delta_1 bd; \alpha_2 ac + \beta_2 bc + \gamma_2 ad + \delta_2 bd)$. (Здесь, как и в 2.25, $\vec{u} = (a; b)$ то $\vec{v} = (c; d)$.) Интересно выяснить, при каких значениях α_1, α, β_1, β, γ_1, γ, δ_1 и δ_2 получится коммутативное ассоциативное кольцо с единицей. Отметим, что нужно уточнить вопрос, поскольку в кольцах из п. 5 и 6 задачи 2.25 получились разные единичные элементы. Выберем в качестве основного вариант п. 6: потребуем, чтобы единичным элементом был вектор $(1; 0)$.*

1) *При каких значениях констант α_1, α, β_1, β, γ_1, γ, δ_1 и δ_2 получится коммутативное ассоциативное кольцо, единичным элементом которого будет вектор $(1; 0)$?*

2) *Найдутся ли среди полученных колец кольца, изоморфные кольцу из п. 4 задачи 2.25?*

3) *Найдутся ли среди полученных колец кольца, изоморфные кольцу из п. 5 задачи 2.25?*

4) *Найдутся ли среди полученных колец кольца, не изоморфные кольцам из п. 4, 5 и 6 задачи 2.25?*

Как мы видим, мир колец намного богаче примерами, чем мир полей; сейчас мы еще рассмотрим несколько важных стандартных способов построения новых колец исходя из уже имеющихся.

2.3. Прямое произведение колец.

Пусть даны два кольца A и B; на прямом (декартовом) произведении множеств $A \times B$ можно ввести операции покомпонентного сложения и умножения:

$$(a; b) + (a'; b') = (a + a'; b + b'), \qquad (a; b) \cdot (a'; b') = (aa'; bb'). \tag{2.11}$$

Нетрудно проверить, что множество $A \times B$ с введенными таким образом операциями является кольцом. Это кольцо называется *прямым произведением* колец A и B. Нулем этого кольца является,

конечно, пара $(0;0)$, единицей — пара $(1;1)$. Нетрудно заметить, что прямое произведение колец всегда имеет делители нуля: $(a;0)\cdot(0;b)=(0;0)$. Более того, нетрудно указать в кольце $A\times B$ идемпотентные элементы: это $(0;1)$ $(1;0)$. Оказывается, верно и обратное: наличие идемпотентных элементов всегда свидетельствует о том, что кольцо является прямым произведением колец.

Однако для начала давайте разберем один важный пример. Рассмотрим прямое произведение колец $\mathbb{Z}_m\times\mathbb{Z}_n$ при взаимно простых m и n. Единичным элементом прямого произведения будет пара $(\bar 1;\bar 1)$,[6] обозначим ее для удобства $\mathbf{1}$. Легко видеть, что в последовательности сумм

$$\begin{aligned}&\mathbf{0}\\&\mathbf{1}\\&\mathbf{1}+\mathbf{1}\\&\mathbf{1}+\mathbf{1}+\mathbf{1}\\&\dots\\&\mathbf{1}+\mathbf{1}+\ldots+\mathbf{1}\\&\dots\end{aligned}\tag{2.12}$$

остатки в первой компоненте будут повторяться с периодом m, а во второй — с периодом n, так что первое повторение получится на mn-ом шаге. Следовательно, в (2.12) мы перечислили ровно mn различных элементов, т.е. все элементы нашего прямого произведения. Но сложение и умножение элементов вида (2.12) определено однозначно (см. задачу 2.16), и, конечно, это в точности соответствует определению операций сложения и умножения в $\mathbb{Z}_{mn}$. Это значит, что отображение $\mathbb{Z}_{mn}\to\mathbb{Z}_m\times\mathbb{Z}_n$, сопоставляющее остатку $\bar a\in\mathbb{Z}_{mn}$ сумму $\underbrace{(\bar 1;\bar 1)+(\bar 1;\bar 1)+\ldots(\bar 1;\bar 1)}_{a}$, является изоморфизмом. Это отображение, конечно, можно описать намного проще: понятно, что в первой компоненте при сложении единицы с собой a получается остаток от деления числа a на m, который мы обозначим $\bar a \pmod m$ а во второй — остаток от деления числа a на n, который мы обозначим $\bar a \pmod n$. В итоге мы получили следующее полезное утверждение:

Теорема 2.2. *Если числа m и n взаимно просты, то отображение $\bar a\mapsto(\bar a \pmod m;\bar a \pmod n)$ $(\bar a\in\mathbb{Z}_{mn})$ задает изоморфизм $\mathbb{Z}_{mn}\cong\mathbb{Z}_m\times\mathbb{Z}_n$.*

Индукцией по числу взаимно-простых сомножителей сразу получаем, что для взаимно простых чисел $n_1,n_2,\dots,n_k$ отображение из $\mathbb{Z}_{n_1n_2\dots n_k}$ в $\mathbb{Z}_{n_1}\times\mathbb{Z}_{n_2}\times\ldots\times\mathbb{Z}_{n_k}$, задаваемое формулой $\bar a\mapsto(\bar a \pmod{n_1};\bar a \pmod{n_2};\dots;\bar a \pmod{n_k})$, является изоморфизмом. Это, по существу одна из форм китайской теоремы об остатках; обычно она формулируется для целых чисел следующим образом.

Следствие 2.1. *Если числа $n_1,n_2,\dots,n_k$ взаимно просты, то для любых целых чисел $a_1,a_2,\dots,a_k$ найдется такое целое число a, что $a\equiv a_i \pmod{n_i}$, $i=1,2,\dots,k$.*

Полученный результат имеет один существенных недостаток: пока что это чистая теорема существования, не предлагающая никакого алгоритма для нахождения такого остатка $\bar a$. Другими словами, мы хотели бы иметь формулу для обратного отображения, позволяющую по паре остатков $\bar b\in\mathbb{Z}_m$, $\bar c\in\mathbb{Z}_n$ находить такой остаток $\bar a\in\mathbb{Z}_{mn}$, что $a\equiv b \pmod m$ и $a\equiv c \pmod n$. Такую формулу легко построить, зная идемпотентные элементы кольца $\mathbb{Z}_{mn}$. Поскольку мы уже знаем, что кольцо $\mathbb{Z}_{mn}$ изоморфно прямому произведению, мы можем быть уверены, что такие идемпотенты существуют, один из них соответствует паре $(\bar 1;\bar 0)$, мы обозначим его $\bar e$, тогда $\bar 1-\bar e$ соответствует паре $(\bar 0;\bar 1)$. Далее, поскольку пара $(\bar 1;\bar 0)$ имеет по сложению порядок m, это означает (если решена задача 1.8), что число e делится на n и взаимно просто с m, а число $1-e$, наоборот, делится на m и взаимно просто с n. Теперь по паре $(\bar b;\bar c)$ легко сконструировать соответствующий остаток $\bar a$: для этого надо просто положить $a=be+c(1-e)$. Действительно, поскольку e делится на n,

[6] Обратим внимание на несовершенство наших обозначений: символ $\bar 1$ в первой компоненте обозначает единичный элемент кольца $\mathbb{Z}_m$, в то время как во второй компоненте тот же самый символ $\bar 1$ обозначает единичный элемент совсем другого кольца $\mathbb{Z}_n$. Чтобы не запутаться, остаток $\bar a\in\mathbb{Z}_n$ можно было бы обозначать $\bar a \pmod n$; тогда единичный элемент прямого произведения запишется как $(\bar 1 \pmod m;\bar 1 \pmod n)\in\mathbb{Z}_m\times\mathbb{Z}_m$.

$a = be + c(1-e) = c + e(b-c) \equiv c \pmod{n}$, и, аналогично, $a = be + c(1-e) = b + (e-1)(b-c) \equiv b \pmod{n}$. Осталось научиться искать идемпотентные элементы в кольце $\mathbb{Z}_{mn}$.

Для этого достаточно решить диофантово уравнение $mx + ny = 1$. Если $(x_0; y_0)$ — какое-нибудь его решение, то, домножая обе части равенства $mx_0 + ny_0 = 1$ на mx_0, получим, что $(mx_0)^2 + mnx_0y_0 = mx_0$, что означает, что остаток от деления mx_0 на mn является искомым идемпотентом. Парный ему идемпотент — это, конечно $ny_0 \pmod{mn}$.

Пример. Рассмотрим кольцо $\mathbb{Z}_{100}$. Для нахождения идемпотентов нам нужно решить уравнение $25x + 4y = 1$. Его решения: $x_0 = 1$; $y_0 = -6$; поэтому искомыми идемпотентами являются остатки $\bar{25}$ и $-\bar{24} = \bar{76}$. Если нам надо найти число, дающее при делении на 25 остаток, скажем, 7, а при делении на 4 остаток, скажем, 2, то наша формула дает ответ $7 \cdot 76 + 2 \cdot 25 \equiv 82 \pmod{100}$.

Использование идемпотентов приводит к успеху и в общем случае.

Теорема 2.3. *Кольцо изоморфно прямому произведению колец тогда и только тогда, когда оно содержит идемпотентные элементы.*

В одну сторону мы эту теорему уже доказали. Осталось понять, как из наличия идемпотентных элементов получить представление кольца в виде прямого произведения.

Пусть дан идемпотентный элемент $e \in A$, тогда, как легко проверить прямым возведением в квадрат,[7] $1-e$ тоже является идемпотентным. Рассмотрим в кольце A все кратности элемента e: $B = \{ex\ ,\quad x \in A\}$. Заметим, что операции сложения и умножения не выводят за пределы подмножества B: $ex + ey = e(x+y) \in B$ и $ex \cdot ey = e^2xy = exy \in B$. Нулевой элемент, конечно лежит в B $(0 = e \cdot 0)$, а вот единичный гарантировано не принадлежит B: если бы 1 была кратностью e, то элемент e был бы обратим, что, как мы знаем не так, поскольку идемпотент всегда является делителем нуля $(e(1-e) = e - e^2 = e - e = 0)$. Казалось бы, из этого отрицательного результата (что $1 \notin B$) следует, что B не является кольцом (по крайней мере, кольцом с единицей), однако это утверждение преждевременно: оказывается, в B имеется собственный нейтральный элемент относительно умножения, не являющийся таковым для всего кольца A. Этот элемент, конечно, просто e: действительно, $e \cdot ex = e^2x = ex$. Остальные аксиомы кольца, очевидно, автоматически выполнены (проверьте!), так что B является ассоциативным коммутативным кольцом с единицей.[8] Аналогичное утверждение верно, конечно, и для подмножества всех кратностей второго идемпотента $1-e$: множество $C = \{(1-e)x\ ,\quad x \in A\}$ также является кольцом.

Осталось установить изоморфизм A и $B \times C$, то есть построить взаимно-однозначное отображение одного кольца на другое, согласованное с операциями. Построим для начала отображение $f : B \times C \to A$ наиболее банальным и естественным способом: паре $(b; c) \in B \times C$ сопоставим просто их сумму, т.е. элемент $b + c \in A$. Согласованность этого отображения с операцией сложения проверяется автоматически: если $f(b; c) = b + c$ и $f(b'; c') = b' + c'$, то, $(b; c) + (b'; c') = (b + b'; c + c')$, поэтому $f((b; c) + (b'; c')) = f(b + b'; c + c') = b + b' + c + c' = b + c + b' + c' = f(b; c) + f(b'; c')$. С умножением лучше начать выкладку с другого конца: $f(b; c) \cdot f(b'; c') = (b + c) \cdot (b' + c') = bb' + cc' + cb' + bc' = f(bb'; cc') + cb' + bc'$. Осталось заметить, что, поскольку $b = ex$, $b' = ex'$, $c = (1-e)y$, $c' = (1-e)y'$, оба произведения cb' и bc' на самом деле равны нулю. Единичным элементом кольца $B \times C$ является пара $(e; 1-e)$, которая при отображении f переходит в $f(e; 1-e) = e + 1 - e = 1$.

Для того, чтобы доказать, что f является взаимно-однозначным соответствием, мы предъявим для него обратное отображение. Определим отображение $g : A \to B \times C$ следующим образом: $g(a) = (ea; (1-e)a) \in B \times C$. Очевидно, $f(g(a)) = f(ea; (1-e)a) = ea + a = ea + a - ea = a$, и $g(f(b; c)) = g(b + c) = (eb + ec; (1-e)b + (1-e)c)$. Но $b = ex$ и $c = (1-e)y$, поэтому $eb = b$, $(1-e)c = c$, $ec = 0$ и $(1-e)b = 0$, так что $g(f(b; c)) = (b; c)$. Следовательно, отображение f взаимно-однозначно.

Задача 2.29. *Докажите, что если два отображения множеств $f : X \to Y$ и $g : Y \to X$ таковы, что $\forall x \in X\ g(f(x)) = x$ и $\forall y \in Y\ f(g(y)) = y$, то f и g являются взаимно-однозначными.*

---

[7] $(1-e)^2 = 1 - e - e + e^2 = 1 - e - e + e = 1 - e$.

[8] Обратите внимание, что в этой ситуации кольцо B не является с точки зрения определения подкольцом кольца A, поскольку у них разные единичные элементы!

Отметим, что в доказательстве теоремы содержится больше, чем заявлено в ее формулировке: у нас имеется явная формула для изоморфизма $A \xrightarrow{\sim} B \times C$, а также формула для обратного изоморфизма. Для применения этих формул необходимо, правда, знать идемпотентные элементы, однако, как мы видели, иногда их бывает не так уж трудно найти.

Задача 2.30. *Докажите, что если p — простое число, то кольцо $\mathbb{Z}_{p^n}$ нельзя представить в виде прямого произведения каких-нибудь колец.*

Задача 2.31. *Сколько попарно неизоморфных колец здесь выписано:*
$\mathbb{Z}_{24}$, $\mathbb{Z}_{12} \times \mathbb{Z}_2$, $\mathbb{Z}_8 \times \mathbb{Z}_3$, $\mathbb{Z}_6 \times \mathbb{Z}_4$, $\mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_2$, $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$?

Задача 2.32. *1) Докажите, что любое кольцо вида $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ изоморфно некоторому кольцу вида $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_l}$, где числа $m_1, m_2, \ldots, m_l$ таковы, что каждое следующее является делителем предыдущего, т.е. $m_{i+1} \mid m_i$, $i = 1, 2, \ldots, l-1$.*
2) Докажите, что такое представление однозначно, т.е. если $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ изоморфно $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_l}$, причем $n_{i+1} \mid n_i$, $i = 1, 2, \ldots, k-1$ и $m_{j+1} \mid m_j$, $j = 1, 2, \ldots, l-1$. то $k = l$ и $n_i = m_i$, $i = 1, 2, \ldots, k-1$.

Задача 2.33. *1) Докажите, что кольцо всех непрерывных функций из $\mathbb{R}$ в $\mathbb{R}$ нельзя представить в виде прямого произведения колец.*
2) Представьте кольцо всех непрерывных функций из $\mathbb{R} \setminus \{0\}$ в $\mathbb{R}$ в виде прямого произведения колец.

Задача 2.34. *Докажите, что элемент $(a; b) \in A \times B$ обратим тогда и только тогда, когда обратимы оба элемента $a \in A$ и $b \in B$. Выведите из этого мультипликативность функции Эйлера (задача 1.31).*

Задача 2.35. *Докажите, что элемент $(a; b) \in A \times B$ является корнем уравнения $x^2 = 1$ тогда и только тогда, когда оба элемента $a \in A$ и $b \in B$ удовлетворяют этому уравнению. Выведите из этого решение задачи 1.20.*

Задача 2.36. *Докажите, что если $\Omega = \Omega_1 \cup \Omega_2$ и $\Omega_1 \cap \Omega_2 = \varnothing$ то кольцо $\mathcal{B}(\Omega)$ (см. задачу 2.25, п. 3) изоморфно прямому произведению колец $\mathcal{B}(\Omega_1) \times \mathcal{B}(\Omega_2)$. Выведите из этого для случая конечного множества Ω изоморфизм $\mathcal{B}(\Omega) \cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{|\Omega|}$.*

Задача 2.37. *Кольцо называется* **булевым**, *если все его элементы идемпотентны (кроме 0 и 1).*
1) Докажите, что любое конечное булево кольцо изоморфно $\mathcal{B}(\Omega)$ для некоторого конечного множества Ω.
**2) Приведите пример бесконечного булева кольца, не изоморфного $\mathcal{B}(\Omega)$ ни для какого множества Ω.*

2.4. Функции, многочлены, формальные ряды.

Первая из обсуждаемых конструкций совершенно банальна: множество отображений X^A из произвольного фиксированного множества X в некоторое фиксированное кольцо A можно естественным образом превратить в кольцо, введя естественным образом операции сложения и умножения функций: если $f : X \to A$ и $g : X \to A$ — две функции, то их сумма $f + g$, конечно задается тем, что $(f + g)(x) = f(x) + g(x)$, а произведение fg — тем, что $(fg)(x) = f(x)g(x)$.

Задача 2.38. *1) Докажите, что множество X^A является кольцом относительно этих операций.*
2) Докажите, что если $X = X_1 \cup X_2$ и $X_1 \cap X_2 = \varnothing$ то кольцо X^A изоморфно прямому произведению колец $(X_1)^A \times (X_2)^A$.

Второе утверждение этой задачи показывает, что кольцо всех отображений устроено довольно неинтересно; действительно, обычно интерес представляют его подкольца, состоящие из функций, удовлетворяющих каким-нибудь специальным условиям, например, непрерывные или дифференцируемые (при подходящих X и A). Мы будем обсуждать такие кольца позже, когда в соответствующих курсах будут даны нужные определения.

Вторая конструкция также хорошо известна из школьного курса: это кольцо многочленов. Зафиксируем некоторое кольцо A и некоторый символ x. *Многочленом степени* n от переменной x с коэффициентами из кольца A называется **формальное выражение** вида

$$P(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n, \quad \text{где все } a_i \in A \text{ и } a_n \neq 0. \tag{2.13}$$

Множество всех многочленов с коэффициентами из данного кольца A стандартно обозначается $A[x]$; для степени имеется стандартное обозначение $n = \deg P(x)$. (Удобно договориться, что слагаемые с нулевыми коэффициентами не пишутся, за исключением многочлена нулевой степени, этот многочлен называется нулевым и обозначается просто 0. Договоримся также считать, что многочлен степени n имеет коэффициенты при всех степенях переменной x, но все коэффициенты $a_{n+1}, a_{n+2}, \ldots$ равны нулю.) Как обычно, коэффициент при x^n многочлена степени n называется его *старшим коэффициентом*[9].

Определим теперь операции на множестве $A[x]$: суммой многочленов $P(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$ и $Q(x) = b_0 + b_1x + \ldots + b_{m-1}x^{m-1} + b_mx^m$ **называется** многочлен $(P + Q)(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_{k-1} + b_{k-1})x^{n-1} + (a_k + b_k)x^k$, где $k = \max(m, n)$ (напомним, что участвующие в этой формуле коэффициенты, большие степени соответствующего многочлена, мы договорились считать нулевыми). Произведением многочленов P и Q **называется** многочлен $(PQ)(x) = c_0x + c_1x + \ldots + c_{k-1}x^{k-1} + c_kx^k$, где коэффициенты c_i вычисляются по обычному правилу: $c_i = a_ib_0 + a_{i-1}b_1 + \ldots + a_1b_{i-1} + a_0b_i$. (Как и в прошлой формуле коэффициенты, большие степени соответствующего многочлена, мы договорились считать нулевыми).

Мы пропускаем проверку того, что введенные таким образом операции удовлетворяют всем аксиомам кольца.[10]

Отметим важное (и очевидное) свойство умножения многочленов, доказываемое рассмотрением старшего коэффициента произведения многочленов:

Теорема 2.4. *1)* $\deg(P(x)Q(x)) \leq \deg(P(x)) + \deg(Q(x))$.
2) Если в кольце нет делителей нуля, то $\deg(P(x)Q(x)) = \deg(P(x)) + \deg(Q(x))$.

Следствие 2.2. *Если в кольце A нет делителей нуля, то в кольце многочленов $A[x]$ тоже нет делителей нуля.*

Пусть дан многочлен $P(x) = a_0+a_1x+\ldots+a_{n-1}x^{n-1}+a_nx^n \in A[X]$ и элемент кольца $\alpha \in A$. Тогда *значением многочлена $P(x)$ при $x = \alpha$* (часто говорят также о значении в точке α) **называется** элемент кольца $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} + a_n\alpha^n \in A$, который, естественно, обозначается $P(\alpha)$. Такой $\alpha \in A$, что $P(\alpha) = 0$ называется, как обычно, *корнем многочлена $P(x)$*.

Итак, каждый многочлен $P(x) \in A[x]$ определяет функцию из A в A, сопоставляющую каждому $\alpha \in A$ значение $P(\alpha)$ данного многочлена на элементе $\alpha \in A$. Тогда возникает естественный вопрос: а почему нельзя было дать обычное, школьное определение многочлена: многочленом называется функция $P : A \to A$, заданная формулой $P(x) = a_0+a_1x+\ldots+a_{n-1}x^{n-1}+a_nx^n$? Нетрудно

[9] Обратите внимание, что коэффициенты многочлена иногда удобно нумеровать в обратном порядке, "от хвоста к голове": $b_0x^n + b_1x^{n-1} + \ldots + b_{n-1}x + b_n$; тогда старшим коэффициентом оказывается, соответственно, b_0.

[10] Проверим все же ассоциативность умножения: пусть $P(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$, $Q(x) = b_0 + b_1x + \ldots + b_{m-1}x^{m-1} + b_mx^m$ и $R(x) = c_0x + c_1x + \ldots + c_{k-1}x^{k-1} + c_kx^k$ — три многочлена. Тогда $(PQ)(x) = \sum_{l=0}^{m+n}(\sum_{i=0}^{l} a_ib_{l-i})x^l$, поэтому коэффициент произведения $(PQ)R$ при x^s равен $\sum_{j=0}^{s}(\sum_{i=0}^{j} a_ib_{j-i})c_{s-j}$. Аналогично коэффициент произведения $P(QR)$ при x^s равен $\sum_{p=0}^{s} a_p(\sum_{q=0}^{s-p} b_qc_{s-p-q})$. Осталось заметить, что обе получившиеся суммы представляют собой сумму всех возможных произведений $a_ub_vc_w$ в которых $u + v + w = s$ (очевидно, что число таких ненулевых произведений конечно).

проверить, что для случая $A = \mathbb{R}$ оба определения приводят к одному и тому же понятию. Однако в общем случае это может быть уже и не так. Имеется естественное отображение $v : A[x] \to A^A$, сопоставляющее каждому многочлену ту функцию из A в A, которую он определяет. В случае поля действительных чисел это отображение является вложением (т.е. разным многочленам соответствуют разные функции), но в случае, например, конечного поля $\mathbb{F}_p$ это уже не может быть так, поскольку ${\mathbb{F}_p}^{\mathbb{F}_p}$ очевидно, конечно, а $\mathbb{F}_p[x]$, наоборот, бесконечно.

Задача 2.39. *1) Сколько элементов содержит A^A, если $|A| = n$?*
2) Докажите, что если A конечно, то $A[x]$ счетно.
**3) Докажите, что если A счетно или континуально, то $A[x]$равномощноA .*

Малая теорема Ферма доставляет многочлен, который дает тождественно нулевую функцию на всем $\mathbb{F}_p$: это многочлен $x^p - x$. Этим же свойством, очевидно, будут обладать все кратности этого многочлена; многочлены, отличающиеся на такое слагаемое будут задавать одну и ту же функцию из $\mathbb{F}_p$ в $\mathbb{F}_p$.

Задача 2.40. *1) Докажите, что любая функция из $\mathbb{F}_p$ в $\mathbb{F}_p$ задается многочленом.*
**2) Верно ли аналогичное утверждение для произвольного кольца $\mathbb{Z}_n$?*

Отметим, что мы можем без труда аналогичным образом определить и кольцо многочленов от нескольких переменных $A[x_1, \ldots, x_n]$; все сказанное о различии между многочленами и функциями (теперь уже от нескольких переменных) справедливо, конечно, и в этом случае.

Задача 2.41. *1) Докажите, что любая функция нескольких переменных (т.е. отображение из из $\mathbb{F}_p^n$ в $\mathbb{F}_p$) задается многочленом.*

Теперь необходимо коснуться двух фундаментальных результатов, так или иначе упоминавшихся в школьной программе: теоремы Виета и теоремы Безу.

Теорема Виета дает явный способ сконструировать многочлен степени n, корнями которого являются данные элементы $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$. Это, конечно, многочлен $(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) \in A[x]$. После раскрытия скобок получается многочлен, зависимость коэффициентов которого от $\alpha_1, \alpha_2, \ldots, \alpha_n$ очень важна и очень легко вычисляется. Запишем сначала результат в общем виде:

$$(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + \ldots + (-1)^{n-1}\sigma_{n-1}x + (-1)^n\sigma_n. \tag{2.14}$$

Выражения коэффициентов через $\alpha_1, \alpha_2, \ldots, \alpha_n$:

$$\begin{aligned}
&\sigma_0 = 1\\
&\sigma_1 = \alpha_1 + \alpha_2 + \ldots + \alpha_n = \sum_{i\in\{1,2,\ldots,n\}} \alpha_i\\
&\sigma_2 = \sum_{\{i,j\}\subset\{1,2,\ldots,n\}} \alpha_i\alpha_j\\
&\ldots\\
&\sigma_k = \sum_{\{i_1,i_2,\ldots,i_k\}\subset\{1,2,\ldots,n\}} \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}\\
&\ldots\\
&\sigma_n = \alpha_1\alpha_2\ldots\alpha_n.
\end{aligned} \tag{2.15}$$

Эти выражения называются *основными симметрическими многочленами.*

Число слагаемых в многочлене σ_k, очевидно, равно числу подмножеств множества $\{1, 2, \ldots, n\}$, состоящих ровно из k элементов; это число обозначается C_n^k или $\binom{n}{k}$ и называется *числом сочетаний* или *биномиальным коэффициентом.* Подставляя $\alpha_1 = \alpha_2 = \ldots = \alpha_n = -a$ получаем *бином Ньютона*:

$$(x + a)^n = x^n + C_n^1 x^{n-1}a + C_n^2 x^{n-2}a^2 + \ldots + x + C_n^{n-1}x^{n-1}a^{n-1} + a^n = \sum_{k=0}^{n} C_n^k x^{n-k}a^k. \tag{2.16}$$

Нетрудно видеть, что $C_n^k = C_n^{n-k}$ (т.к. выбрать k элементов из n можно столькими же способами, сколькими можно оставить остальные $n-k$ элементов невыбранными), при этом первые значения нетрудно посчитать:
$C_n^0 = 1$ (существует единственный способ не выбрать ни один элемент из n),
$C_n^1 = n$ (один элемент из n можно выбрать ровно n способами),
$C_n^2 = \frac{n(n-1)}{2}$ (это число пар элементов).

Задача 2.42. *Воспользуйтесь равенством $(x+a)^n(x+a) = (x+a)^{n+1}$ для доказательства основной формулы для биномиальных коэффициентов:*

$$C_n^k + C_n^{k-1} = C_{n+1}^k. \tag{2.17}$$

Задача 2.43. *Воспользуйтесь равенством $(x+a)^n(x+a) = (x+a)^{n+1}$ для доказательства основной формулы для биномиальных коэффициентов:*

$$C_n^k = \frac{n!}{k!(n-k)!}. \tag{2.18}$$

Следующий важный сюжет, связанный с многочленами, и также известный еще со школы — это деление с остатком и теорема Безу. Пусть даны два многочлена $P(x), Q(x) \in A[x]$, где A — некоторое кольцо. *Разделить многочлен $P(x)$ с остатком на многочлен $Q(x)$* — это значит представить многочлен $P(x)$ в виде $P(x) = S(x)Q(x) + R(x)$, где многочлены $S(x), R(x) \in A[x]$, причем $\deg R(x) < \deg Q(x)$. Как и в арифметике, многочлен $R(x)$ называется при этом *остатком*, а многочлен $S(x)$ — *неполным частным*.

Теорема 2.5. *1) Если старший коэффициент многочлена $Q(x)$ обратим, то любой многочлен из $A[x]$ можно разделить с остатком на $Q(x)$.*
2) Если старший коэффициент многочлена $Q(x)$ не является делителем нуля и данный многочлен можно разделить с остатком на $Q(x)$, то остаток и неполное частное определены однозначно.

Для доказательства первого утверждения запишем многочлен $Q(x)$ в виде $Q(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$; по условию элемент a_0 обратим. Рассмотрим произвольный многочлен $P(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m$; докажем индукцией по m возможность деления с остатком $P(x)$ на $Q(x)$. Это утверждение, очевидно, верно при $m < n$, поскольку в этом случае неполное частное можно положить равным нулю, а остатком будет тогда сам $P(x)$. Предположим теперь, что $m \geq n$, и предположим, что возможность деления с остатком на $Q(x)$ уже доказана для всех многочленов, имеющих степень меньше m. Возьмем произвольный многочлен $P(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m$, тогда степень многочлена $P(x) - b_0a_0^{-1}x^{m-n}Q(x)$ будет, очевидно, меньше m, поэтому его по предположению индукции можно представить в виде $P(x) - b_0a_0^{-1}x^{m-n}Q(x) = S(x)Q(x) + R(x)$, где $\deg R(x) < n$. Тогда $P(x) = (b_0a_0^{-1}x^{m-n} + S(x))Q(x) + R(x)$ будет, конечно, искомым представлением для многочлена $P(x)$.

Для доказательства второго утверждения теоремы допустим, что имеется два различных представления $P(x) = S(x)Q(x) + R(x)$ и $P(x) = S_1(x)Q(x) + R_1(x)$, где степени многочленов $R(x)$ $R_1(x)$ меньше n. Тогда, вычитая одно равенство из другого, получим, что $(S(x) - S_1(x))Q(x) = R(x) - R_1(x)$. Если многочлены $S(x)$ и $S_1(x)$ не равны, то степень многочлена в левой части не меньше n, в то время как степень правой части должна быть строго меньше n, что дает искомое противоречие.

Следствие 2.3. *Пусть $\alpha \in A$ является корнем многочлена $P(x) \in A[x]$ степени $n > 0$. Тогда многочлен $P(x)$ нацело делится на $x - \alpha$, т.е. существует представление $P(x) = (x-\alpha)S(x)$, где $S(x) \in A[x]$ и $\deg S(x) = n - 1$.*

Для доказательства достаточно заметить, что многочлен $Q(x) = x - \alpha$ удовлетворяет условию первой части теоремы 2.5, поэтому имеется представление вида $P(x) = (x - \alpha)S(x) + R(x)$, в котором степень многочлена $R(x)$ меньше 1, т.е равна нулю, что означает, что $R(x)$ является константой, т.е. $R(x) = c \in A$. Следовательно, $P(x) = (x - \alpha)S(x) + c$, и, подставляя $x = \alpha$ в обе части этого равенства, получим, что $0 = 0 + c$, откуда $c = 0$.

Следствие 2.4. *1) Любой многочлен $P(x) \in A[x]$ степени $n > 0$ можно представить в виде*

$$P(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_k)S(x), \tag{2.19}$$

где $k \leq n$, $\alpha_1, \alpha_2, \dots \alpha_k \in A$, а многочлен $S(x)$ не имеет корней в A.
2) Если в кольце A нет делителей нуля, то такое представление однозначно.

Отметим, что, вообще говоря, среди сомножителей $(x-\alpha_i)$ в представлении (2.19) могут встретиться одинаковые скобки; число сомножителей $(x - \alpha_i)$ в этом представлении называется *кратностью* корня α_i.

Следствие 2.5. *Если в кольце нет делителей нуля, то многочлен степени n имеет не более n различных корней, считая с кратностями (т.е сумма кратностей всех корней не превосходит n).*

Отметим, что требование отсутствия делителей нуля является здесь весьма существенным: например, над кольцом $\mathbb{Z}_8$ многочлен $x^2 - \bar{1}$ имеет четыре корня и два представления в виде (2.19): $x^2 - \bar{1} = (x - \bar{1})(x + \bar{1}) = (x - \bar{3})(x + \bar{3})$.

Следующий пример — кольцо формальных степенных рядов. *Формальным степенным рядом* от переменной x с коэффициентами из кольца A называется **формальное выражение** вида

$$P(x) = a_0 + a_1 x + a_2 x^2 + \dots, \tag{2.20}$$

где $a_0, a_1, a_2, \dots$ — некоторая бесконечная последовательность элементов кольца A.

Множество всех формальных степенных рядов с коэффициентами из данного кольца A стандартно обозначается $A[[x]]$.

Операции сложения и умножения на множестве $A[[x]]$ определяются ровно по тем же формулам, что и для кольца многочленов: суммой формальных степенных рядов $P(x) = a_0 + a_1 x + a_2 x^2 + \dots$ и $Q(x) = b_0 + b_1 x + b_2 x^2 + \dots$ **называется** формальный степенной ряд $(P + Q)(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots$.

Произведением формальных степенных рядов P и Q **называется** формальный степенной ряд $(PQ)(x) = c_0 x + c_1 x + c_2 x^2 + \dots$, где коэффициенты c_i вычисляются по обычному правилу: $c_i = a_i b_0 + a_{i-1} b_1 + \dots + a_1 b_{i-1} + a_0 b_i$.

Теперь, конечно, надо проверить, что введенные таким образом операции на $A[[x]]$ удовлетворяют всем аксиомам кольца — мы оставляем это в качестве обязательной задачи.

Как связано кольцо формальных степенных рядов с предыдущими двумя примерами? Ясно, что любой многочлен можно рассматривать как формальный степенной ряд, у которого все коэффициенты, начиная с некоторого, равны нулю. Это значит, что кольцо многочленов $A[x]$ является подкольцом кольца формальных степенных рядов $A[[x]]$. А вот установить какую-нибудь очевидную связь кольца формальных степенных рядов с кольцом функций из A в A в общем случае не удается.[11]

Есть ли в кольце формальных степенных рядов делители нуля? Ответ такой же, как для многочленов.

Теорема 2.6. *Если в кольце A нет делителей нуля, то в кольце $A[[x]]$ тоже их нет.*

Повторить доказательство, данное нами для многочленов, в этой ситуации нельзя: у степенного ряда нет ни степени, ни старшего коэффициента. Но зато для каждого ненулевого степенного ряда можно указать наименьшую степень переменной, при которой стоит ненулевой коэффициент. Обозначим эту степень через k; это значит, что наш ряд можно представить в виде $P(x) = a_k x^k +$

[11] Если A — поле действительных чисел, то такая связь существует для некоторых рядов, называемых *сходящимися*, и для некоторых, достаточно хороших функций, называемых *аналитическими*. Открытие этой связи, собственно, и дало начало математическому анализу, а изучение разложения функций в ряд до сих пор составляет весьма существенную его часть.

$a_{k+1}x^{k+1}+\ldots$, где $a_k\neq 0$. Если другой ряд представлен в виде $Q(x)=b_mx^m+b_{m+1}x^{m+1}+\ldots$, где $b_m\neq 0$, то $PQ(x)=a_kb_mx^{k+m}+(a_kb_{m+1}+a_{k+m+1}b_m)x^{k+m+1}+\ldots$, причем $a_kb_m\neq 0$, поскольку в кольце A нет делителей нуля.

Следующий естественный вопрос: какие элементы в кольце формальных степенных рядов обратимы. В этом отношении кольцо $A[[x]]$ представляет собой полную противоположность кольцу многочленов, в котором обратимых элементов очень мало: в кольце многочленов обратимыми могут быть, конечно, только многочлены степени нуль, то есть константы, причем только те, которые являются обратимыми элементами кольца A. В кольце формальных степенных рядов, как показывает следующая теорема, обратимых элементов, наоборот, очень много.

Теорема 2.7. *Формальный степенной ряд $P(x)=a_0+a_1x+a_2x^2+\ldots$ обратим тогда и только тогда, когда a_0 является обратимым элементом кольца A.*

Докажем, что существует такая последовательность элементов кольца $b_0,b_1,b_2,\ldots$, что ряд $Q(x)=b_0+b_1x+b_2x^2+\ldots$ обладает тем свойством, что $PQ(x)=1$. По определению, коэффициенты ряда $(PQ)(x)=c_0x+c_1x+c_2x^2+\ldots$ вычисляются по формуле $c_i=a_ib_0+a_{i-1}b_1+\ldots+a_1b_{i-1}+a_0b_i$. Мы хотим подобрать такие $b_0,b_1,b_2,\ldots$, что $c_0=1$, а $0=c_1=c_2=\ldots$. Первому равенству удовлетворить легко: надо положить $b_0=a_0^{-1}$. Далее, $c_1=a_0b_1+a_1b_0$, поэтому, чтобы сделать $c_1=0$ достаточно положить $b_1=-a_0^{-1}a_1b_0$. Напомним, что b_0 мы только что вычислили: $b_0=a_0^{-1}$, так что мы можем выразить b_1 только через коэффициенты ряда $P(x)$: $b_1=-a_0^{-2}a_1$. Далее, нетрудно видеть, что из условия $c_2=0$ мы можем найти формулу для вычисления коэффициента b_2 через известные коэффициенты a_0,a_1 и a_2 (выпишите это выражение!) и так далее. Отметим, что для доказательства теоремы нам нет необходимости искать явный вид выражения b_n $a_0,a_1,a_2,\ldots a_n$; достаточно доказать, что такая формула существует. Это очень легко сделать по индукции: предположим, что мы нашли формулы для выражения каждого из коэффициентов $b_0,b_1,b_2,\ldots,b_n$ через коэффициенты $a_0,a_1,a_2,\ldots a_n$, которые дают $c_0=1$ и $c_1=c_2=\ldots=c_n=0$. Докажем, что можно выразить b_{n+1} через $a_0,a_1,a_2,\ldots a_n,a_{n+1}$ таким образом, чтобы c_{n+1} было бы нулем. Для этого достаточно выразить b_{n+1} из равенства $c_{n+1}=0$:

$$0=a_0b_{n+1}+a_1b_n+\ldots+a_nb_1+a_{n+1}b_0\quad\Rightarrow b_{n+1}=-a_0^{-1}(a_1b_n+a_2b_{n-1}+\ldots+a_nb_1+a_{n+1}b_0),$$

и, подставляя в правые части последнего равенства выражения для $b_0,b_1,b_2,\ldots,b_n$, которые существуют по предположению индукции, мы получим искомое выражение для b_{n+1}.

Отметим, что частный случай этой теоремы хорошо известен в школьном курсе под названием суммы бесконечно-убывающей геометрической прогрессии:

$$\frac{1}{1-x}=1+x+x^2+x^3+\ldots=\sum_{n=0}^{\infty}x^n. \tag{2.21}$$

Наше утверждение даже намного проще: в школьном курсе нам необходимо было доказать, что последовательность сумм конечных геометрических прогрессий $1+x+x^2+x^3+\ldots+x^n$ имеет предел, и что этот предел равен в точности $\frac{1}{1-x}$, причем это все имело смысл только для действительных чисел x, по абсолютной величине меньших единицы.[12] Мы же теперь можем сформулировать и доказать это равенство над любым кольцом как равенство формальных степенных рядов: для доказательства достаточно лишь заметить, что у произведения двух степенных рядов $1-x$ и $1+x+x^2+x^3+\ldots$ все коэффициенты, кроме нулевого, равны нулю.

[12]На этом примере очень хорошо видны все трудности, которые возникают в математическом анализе при попытке интерпретировать степенной ряд как функцию, или, наоборот, представить функцию степенным рядом. В приведенном примере видно, что в степенной ряд $1+x+x^2+x^3+\ldots$ над полем действительных чисел вместо x можно подставлять значения, но не любые, а только по модулю меньшие единицы. Другими словами, действительную функцию $f(x)=\frac{1}{1-x}$ можно представить степенным рядом, но только на интервале $(-1;1)$. Мы оставляем обсуждение всех возникающих здесь трудностей и путей их преодоления до курса математического анализа.

2.5. Поле частных.

Как мы видели, очень многие результаты, верные для полей, верны также для колец без делителей нуля. Формально говоря, это обстоятельство объясняется очень просто: в кольце без делителей нуля, как и в поле из равенства $ab = 0$ следует, что либо $a = 0$, либо $b = 0$, а это рассуждение и является решающим в очень многих доказательствах. Однако имеется и более глубокая причина: всякое кольцо без делителей нуля является на самом деле подкольцом некоторого поля, которое однозначно задается данным кольцом и называется его *полем частных*. Способ построения этого поля ничем не отличается от того, которым в курсе математики 5 класса вводятся рациональные числа исходя из целых; здесь мы просто воспроизведем эти рассуждения на чуть более формальном уровне.

Пусть дано некоторое кольцо A, не имеющее делителей нуля. Мы хотим дать точное описание множеству "всех дробей", числитель и знаменатель которых брался бы из кольца A, и ввести на этом множестве операции сложения и умножения, которые бы превратили это множество в поле,содержащее наше исходное кольцо A. Первая сложность, которую мы сразу замечаем, рассматривая наш основной пример, состоит в том, что рациональное число представляется дробью не однозначно: при умножении числителя и знаменателя на одно и тоже ненулевое целое число получается другая дробь, представляющая то же самое рациональное число. При работе с рациональными числами эта неоднозначность не очень мешала, поскольку ввиду однозначности разложения целых чисел на простые множители мы могли выбрать наиболее экономное представление данного рационального числа — несократимую дробь. В произвольном кольце у нас такой теоремы об однозначном разложении на множители у нас нет, поэтому нам и не удастся ввести понятие несократимой дроби. С другой стороны, очень легко сформулировать условие того, когда две дроби a/b и a'/b' представляют одно и то же рациональное число, причем это условие записывается только при помощи операции сложения: это равенство $ab' = a'b$.

Теперь мы готовы дать формальное определение: рассмотрим прямое произведение множеств A и $A \setminus \{0\}$. Пары $(a; b) \in A \times (A \setminus \{0\})$ мы и будем называть "дробями"; введем на $A \times (A \setminus \{0\})$ отношение эквивалентности $\sim$ следующим образом: $(a; b) \sim (a'; b')$, если $ab' = a'b$. Конечно, надо сначала доказать, что это действительно отношение эквивалентности. Его симметричность ($x \sim y \Leftrightarrow y \sim x$) и рефлексивность ($x \sim x$) очевидны; надо только проверить транзитивность, т.е. что если $(a; b) \sim (a'; b')$ и $(a'; b') \sim (a''; b'')$, то $(a; b) \sim (a''; b'')$. Запишем соответствующие равенства: $ab' = a'b$ и $a'b'' = a''b'$. Домножим второе равенство на b: $ba'b'' = ba''b'$ и заменим в левой части равенства ba' на ab': $ab'b'' = ba''b'$. Перенесем все в левую часть равенства и вынесем b' за скобки: $(ab'' - ba'')b' = 0$. Теперь, наконец, воспользуемся тем, что в кольце нет делителей нуля: из того, что $b' \neq 0$, следует, что $ab'' - ba'' = 0$, т.е. $(a; b) \sim (a''; b'')$.

Теперь, конечно, надо рассмотреть множество K классов эквивалентности: класс эквивалентности, содержащий пару $(a; b)$ удобнее, конечно, обозначать "дробью" a/b.

Осталось ввести на множестве K операции сложения и умножения, и доказать, что относительно введенных операций K, действительно, является полем. Определение операций, конечно, такое же, как в 5 классе: суммой "дробей" a/b и c/d **называется** дробь $(ad + bc)/(bd)$, а произведением "дробей" a/b и c/d **называется** дробь $(ac)/(bd)$. Эти определения при всей своей привычности требуют большой подготовительной работы: сначала надо доказать их корректность. Дело в том, что дробью мы назвали целый класс эквивалентности, содержащий много различных пар, а операции определили формулами, в которых участвуют какие-то произвольно выбранные представители своих классов эквивалентности. Для того, чтобы этим определением можно было пользоваться, необходимо доказать, что если мы выберем две пары $(a; b)$ и $(a'; b')$ из одного и того же класса (т.е. $ab' = a'b$) и еще две пары $(c; d)$ и $(c'; d')$ из какого-то другого класса (т.е. $cd' = c'd$), то результаты применения только что определенных нами операций к парам $(a; b)$ и $(c; d)$ будут эквивалентны результатам применения этих же операций к парам $(a'; b')$ и $(c'; d')$. Проверим это, скажем для сложения. Мы хотим доказать, что $(ad+bc; bd) \sim (a'd'+b'c'; b'd')$, то есть, что $(ad+bc)b'd' = (a'd'+b'c')bd$. Для этого достаточно отдельно доказать равенства $adb'd' = a'd'bd$ и $bcb'd' = b'c'bd$, а потом их сложить. Но первое из этих равенств получается домножением равенства $ab' = a'b$ на dd', а второе

— домножением равенства $cd' = c'd$ на bb'. Для умножения проверка еще проще; мы оставляем ее читателю.

Только теперь, доказав корректность определений сложения и умножения на множестве K, мы можем начать доказывать, что введенные таким образом операции удовлетворяют всем аксиомам поля. Коммутативность обеих операций очевидна ввиду симметричности формул, которыми мы их определили; проверим ассоциативность, скажем, для сложения. Имеем три "дроби" a/b, c/d и e/f. Нам надо доказать, что $(a/b + c/d) + e/f = a/b + (c/d + e/f)$. Выписываем, что дает определение для левой части равенства: $(a/b + c/d) + e/f = (ad + bc)/bd + +e/f = ((ad + bc)f + ebd)/bdf = (adf + bcf + ebd)/bdf$ (Мы свободно пользуемся ассоциативностью отдельно в числителе и отдельно в знаменателе, поскольку там мы работаем с элементами кольца A). Теперь уже нетрудно проверить, что правая часть искомого равенства преобразуется к тому же самому выражению. Мы опускаем это вычисление, а также аналогичную проверку ассоциативности умножения. Также мы опустим и проверку дистрибутивности, выполняемую совершенно аналогично.

Нулем для операции сложения будет, очевидно, класс, состоящий из пар вида $(0; x)$. (Проверьте, что они, действительно, составляют отдельный класс эквивалентности!) В самом деле: согласно определению, $(a; b) + (0; x) = (ax + b0; bx) = (ax; bx) \sim (a; b)$. Аналогично, единицей для умножения будет класс $(x; x)$: $(a; b) \cdot (x; x) = (ax; bx) \sim (a; b)$.

Парой, противоположной паре $(a; b)$ будет, конечно, пара $(-a; b)$: $(a; b)+(-a; b) = ((ab+(-a)b; b^2) = (0; b^2)$. Обратной по умножению для пары $(a; b)$ будет, конечно, пара $(b; a)$ (конечно, только при $b \neq 0$): $(a; b) \cdot (b; a) = (ab; ab)$.

Итак, множество K с введенными на нем операциями, действительно, является полем, осталось найти в K подкольцо, изоморфное исходному кольцу A. Это будут, конечно, "дроби" со знаменателем, равным единице, т.е. классы эквивалентности, содержащие пары вида $(a; 1)$. Естественно отождествить это подкольцо в K с A, тогда можно сказать, что мы построили поле, содержащее наше исходное кольцо A в качестве подкольца.

Нетрудно понять, что это K является наименьшим полем, содержащим A, то есть K меньших подполей, содержащих A. Наоборот, если A является подкольцом какого-нибудь поля L, то наименьшее подполе в L, содержащее A, изоморфно построенному нами полю K. Это поле K и называется *полем частных* кольца A.

Рассмотрим несколько примеров. Первый — это кольцо многочленов $\mathbb{K}[x]$ над некоторым полем $\mathbb{K}$. Его поле частных называется полем рациональных функций[13] от переменной x и состоит из выражений вида $\frac{P(x)}{Q(x)}$, где $P(x)$ и $Q(x)$ некоторые многочлены (причем $Q(x)$ ненулевой). Это поле обычно обозначается $\mathbb{K}(x)$. Поскольку (мы этого еще не доказывали) каждый многочлен над полем можно однозначно разложить на неприводимые сомножители, элементы поля рациональных функций, как и рациональные числа, имеют стандартное несократимое представление в виде такой дроби, у которой многочлены в числителе и знаменателе не имеют общих множителей положительной степени, а многочлен, стоящий в знаменателе, имеет старшим коэффициентом единицу.

Рассмотрим другой, более простой пример, в котором, однако, найти стандартное представление элементов поля частных чуть-чуть труднее. Рассмотрим встречавшееся в одной из предыдущих задач кольцо, состоящее из действительных чисел вида $a + b\sqrt{2}$, где a и b — целые числа. Поскольку оно является подкольцом поля действительных чисел, в нем, конечно, нет делителей нуля. Поле частных, конечно, состоит из действительных чисел вида $\frac{a+b\sqrt{2}}{c+d\sqrt{2}}$, но такое представление, конечно, очень неоднозначно. Стандартное представление здесь получается чуть-чуть по-другому: нетрудно проверить, что любой элемент поля частных представляется в виде $\alpha + \beta\sqrt{2}$, где числа α и β надо теперь брать уже не обязательно целыми, а рациональными: $\alpha, \beta \in \mathbb{Q}$. Очевидно, что все числа такого вида должны принадлежать полю частных; для доказательства того, что это и есть поле частных достаточно доказать, что числа такого вида действительно образуют поле. Очевидно, это множество замкнуто относительно сложения, вычитания и умножения и образует, поэтому, по крайней мере подкольцо в поле действительных чисел. Наличие у каждого элемента

[13]Это традиционное название, как это часто бывает, формально не очень удачно, поскольку применение здесь термина "функция" в общем случае может оказаться так же некорректно, как и в случае многочленов.

обратного элемента проверяется при помощи школьного приема "избавления от иррациональности в знаменателе": $\frac{1}{\alpha+\beta\sqrt{2}} = \frac{\alpha-\beta\sqrt{2}}{(\alpha+\beta\sqrt{2})(\alpha-\beta\sqrt{2})} = \frac{\alpha-\beta\sqrt{2}}{\alpha^2-2\beta^2} = \frac{\alpha}{\alpha^2-2\beta^2} - \frac{\beta}{\alpha^2-2\beta^2}\sqrt{2}$. Знаменатель здесь, конечно, никогда не равен нулю, поскольку, как мы знаем, не существует рационального числа, квадрат которого был бы равен двум.

И последний в этом разделе, новый для нас пример — поле частных кольца формальных степенных рядов $\mathbb{K}[[x]]$ над некоторым полем $\mathbb{K}$. Как мы видели, ряд $a_0 + a_1x + a_2x^2 + \ldots$ обратим тогда и только тогда, когда $a_0 \neq 0$. Это значит, что если у некоторого ряда $f(x)$ наименьший ненулевой коэффициент имеет номер k, т.е. $f(x) = b_kx^k + b_{k+1}x^{k+1} + b_{k+2}x^{k+2} + \ldots$ где $b_k \neq 0$, то ряд $f(x)$ можно представить в виде $f(x) = x^k(b_k + b_{k+1}x + b_{k+2}x^2 + \ldots)$, где второй сомножитель обратим. Другими словами, единственными, с точностью до обратимого сомножителя, необратимыми элементами кольца формальных степенных рядов являются степени x, поэтому любой элемент поля частных можно представить в виде $\frac{a_0+a_1x+a_2x^2+\ldots}{x^k}$, где $k \geq 0$. Учитывая, что числитель тоже может делиться на некоторую неотрицательную степень x, и используя степени x с любым целым показателем, это выражение можно переписать в виде $f(x) = x^k(b_0 + b_1x + b_2x^2 + \ldots)$, где K — любое целое число, положительное или отрицательное, а $b_0 \neq 0$. Удобно также записать это выражение в следующем виде: сдвинем нумерацию коэффициентов, положив $C_i = b_{i+k}$, и раскроем скобки. Получится: $f(x) = c_kx^k +_{k+1} x^{k+1} + c_{k+2}x^{k+2} + \ldots = \sum_{n=k}^{\infty} c_nx^n$ где k — любое целое число, положительное или отрицательное. Поле частных кольца формальных степенных рядов обозначается $\mathbb{K}((x))$ и называется полем *формальных степенных рядов Лорана.*