ИвГУ, ф-т МиКН, курс 2

"КОМПЬЮТЕРНАЯ АЛГЕБРА"

Тема 7.

Кольца многочленов.

Неприводимые многочлены

Лектор: Н. И. Яцкин, 2014

ФАКТОРИАЛЬНЫЕ КОЛЬЦА

КОЛЬЦА МНОГОЧЛЕНОВ
(над ФК,
от одной переменной)

ЕВКЛИДОВЫ КОЛЬЦА

КОЛЬЦА МНОГОЧЛЕНОВ
(над полем,
от одной переменной)

ФК:

Любой ненулевой и необратимый элемент однозначно (с точностью до порядка сомножителей и их ассоциированности) разлагается в произведение неразложимых элементов.

ЕК:

Заданы евклидова норма и алгоритм Евклида.

В примерах: **кольца**

$$\mathbb{Z}[x]$$

и

$$\mathbb{Q}[x]$$

Стиль записи многочленов (по возрастанию степеней):

$$f(x) = \sum_{i=0}^{n} f_i x^i =$$

$$= f_0 + f_1 x + \cdots + f_{n-1} x^{n-1} + f_n x^n;\ f_n \neq 0.$$

Функция-степень:

$$f(x) \longmapsto \deg\big(f(x)\big) = n$$

определена как ***над полем P***, так и ***над кольцом L***,

но роль ***евклидовой нормы*** играет лишь в случае ***поля***.

Обратимые многочлены суть ***обратимые скаляры***, т. е.

над полем P:

все ***ненулевые*** константы $c \in P^* = P \setminus \{0\}$;

над кольцом L:

обратимые константы $c \in L^*$.

Многочлены **ассоциированы** $\equiv$

отличаются ***обратимым множителем***.

В частном случае $L = \mathbb{Z}$:

ассоциированы $\equiv$ равны или отличаются знаком.

Нормализованный многочлен ≡

старший коэффициент равен **1**.

Над полем: любой многочлен можно ***нормализовать***

(заменить на ассоциированный нормализованный);

над кольцом – не любой.

В частном случае $L = \mathbb{Z}$: $2x \nsim x$.

Содержание многочлена (***над кольцом***):

$$\mathbf{cont}(f) \in \text{НОД}(f_0, f_1, \dots, f_n);$$

этот элемент определен ***с точностью до ассоциированности***.

В частном случае $L = \mathbb{Z}$: **содержание**

$$\mathbf{cont}(f) = (f_0, f_1, \dots, f_n)$$

определено ***однозначно*** (является натуральным числом).

Примитивный многочлен $\equiv$ содержание

является ***обратимым*** элементом (ассоциировано с **1**).

В частном случае $L = \mathbb{Z}$:

многочлен $f(x)$ примитивен $\Leftrightarrow \mathbf{cont}(f) = 1$.

Всякий многочлен представляется в виде:

$$f(x) = c\,\tilde{f}(x),$$

где $c = \mathrm{cont}(f)$, $\tilde{f}(x)$ - ***примитивный*** многочлен.

Теорема 1 (лемма Гаусса).

Произведение двух примитивных многочленов является примитивным многочленом.

Доказательство (для случая $L = \mathbb{Z}$).

От противного: пусть

$$f(x) = \sum_{i=0}^{n} f_i x^i \ (f_n \neq 0)$$

и

$$g(x) = \sum_{j=0}^{m} g_j x^j \ (g_m \neq 0)$$

- ***примитивны***, т. е. коэффициенты каждого из них взаимно просты.

Рассмотрим произведение

$$h(x) = f(x)g(x) = \sum_{k=0}^{n+m} h_k x^k,$$

где старший коэффициент

$$h_{n+m} = f_n g_m .$$

Если $h(x)$ ***не примитивен***, то существует ***простое*** натуральное число p, делящее все h_k.

По предположению, p не может делить все f_i и все g_j; так что существует ***крайние слева*** коэффициенты f_{i_0} и g_{j_0}, ***не делящиеся*** на p. Вычислим коэффициент h_{k_0}, где $k_0 = i_0 + j_0$:

$$h_{k_0} = \sum_{i=0}^{i_0-1} f_i g_{k_0-i} + f_{i_0} g_{j_0} + \sum_{i=i_0+1}^{k_0} f_i g_{k_0-i}.$$

По предположению, все коэффициенты f_i $(i < i_0)$, все коэффициенты g_{k_0-i} $(i > i_0)$, а также h_{k_0} делятся на p; значит, делится на p произведение $f_{i_0} g_{j_0}$, что, в силу простоты p, приводит к противоречию: хотя бы один из коэффициентов, f_{i_0} или g_{j_0}, делится на p. ■

Теорема 2 (свойство содержания).

Содержание произведения двух многочленов равно произведению содержаний сомножителей:

$$\mathbf{cont}(f \cdot g) = \mathbf{cont}(f) \cdot \mathbf{cont}(g) .$$

Доказательство (для случая $L = \mathbb{Z}$). Перемножив равенства $f(x) = c\,\tilde{f}(x)$, и $g(x) = d\,\tilde{g}(x)$, где $c = \mathbf{cont}(f)$, $d = \mathbf{cont}(g)$, а $\tilde{f}(x)$ и $\tilde{g}(x)$ - ***примитивны***, получим $f(x)g(x) = cd\,\tilde{f}(x)\tilde{g}(x)$.

В силу ***леммы Гаусса***, многочлен $\tilde{f}(x)\tilde{g}(x)$ – также ***примитивен*** и, следовательно, $\mathbf{cont}(fg) = cd$. ■

Задача 1. Представить процедуру вычисления ***содержания*** $c = \mathbf{cont}(f)$ и ***примитивной части*** $\tilde{f} = \mathbf{prim}(f)$ для целочисленного многочлена $f(x) = c\,\tilde{f}(x)$.

```
> ContPrim:=proc(f::polynom(integer),x::name)
```

Можно использовать функции:

igcd(a) – возвращает **НОД** последовательности **a** целых чисел;

coeff(f,x,i) – возвращает коэффициент при **i**-ой степени **x** в многочлене **f**.

Решение.

```
> ContPrim:=proc(f::polynom(integer),x::name)
  local cl,cf,prf;
if f=0 then
  RETURN(NULL);
else
  cl:=seq(coeff(f,x,i),i=0..degree(f,x));
  cf:=igcd(cl);
  prf:=sort(simplify(f/cf),x);
  RETURN(cf,prf);
end if;
end proc;
```

Примеры применения.

```
> ContPrim(-3,x);
ContPrim(4*x^10+2*x^4-6,x);
ContPrim(5*x^4-3*x^2+2*x+2,x);
ContPrim((1/2)*x^100-1,x);
```

$$3, -1$$

$$2, 2\,x^{10} + x^4 - 3$$

$$1, 5\,x^4 - 3\,x^2 + 2\,x + 2$$

```
Error, invalid input: ContPrim expects its 1st argument, f,
to be of type polynom(integer), but received 1/2*x^100-1
```

Факториальность колец многочленов влечет тот факт, что

ПЭ ⇔ НЭ.

Напоминание:

НЭ (*неразложимый* элемент a):

$$[a = b \cdot c] \Rightarrow [(b \text{ обратим}) \vee (c \text{ обратим})]$$

ПЭ (*простой* элемент a):

$$[a \mid b \cdot c] \Rightarrow [(a \mid b) \vee (a \mid c)]$$

Многочлен $f(x)$ ***неразложим*** в кольце многочленов ⇔ его нельзя представить в виде произведения двух ***необратимых*** многочленов.

Общий случай многочленов над полем.

- Все многочлены ***нулевой*** степени (ненулевые константы) ***обратимы***.

- Многочлен ***положительной*** степени ***неразложим*** ⇔ не представляется в виде произведения двух многочленов ***меньшей*** степени. Такие многочлены называются ***неприводимыми.***

- Многочлены степени **1** ***неприводимы*** (над любым полем).

Конкретно **над полем** $\mathbb{C}$ (или, вообще, - над любым ***алгебраически замкнутым*** полем):

неприводимы только многочлены степени **1**.

Конкретно **над полем** $\mathbb{R}$:

неприводимы:

(1) многочлены степени **1**;

(2) многочлены степени **2** с отрицательным дискриминантом.

Конкретно **над полем** $\mathbb{Q}$:

неприводимые многочлены имеются в любой положительной степени. (*Доказательство см. ниже.*)

Случай многочленов над (факториальным) кольцом.

- Не все многочлены нулевой степени обратимы. Среди ***необратимых*** констант имеются ***неразложимые***. Всякая (ненулевая и необратимая) константа является произведением неразложимых констант.

- Многочлен ***положительной*** степени представляется в виде $f(x) = c\,\tilde{f}(x)$, где $c = \mathbf{cont}(f)$, а $\tilde{f}(x)$ – ***примитивен***.

$f(x)$ **неразложим**	$\Leftrightarrow$	**содержание** c **является обратимой константой, а примитивная часть** $\tilde{f}(x)$ **неразложима**

Неприводимыми многочленами (над **кольцом**) считаются многочлены положительной степени, не представимые в виде произведения двух многочленов ***меньшей степени***. При таком подходе ***неприводимость*** не влечет ***неразложимость*** (нужна еще ***примитивность***).

Конкретно над **кольцом** $\mathbb{Z}$: ***неразложимыми*** элементами кольца $\mathbb{Z}[x]$ являются:

(1) ***простые*** целые числа (константы);

(2) ***примитивные неприводимые*** многочлены положительной степени.

Например, многочлен $2x+3$ неразложим, а многочлен $2x+2=2(x+1)$ разложим (он неприводим, но не является примитивным).

(Ниже будет доказано, что в любой степени существуют неприводимые примитивные многочлены над $\mathbb{Z}$*.)*

Переход к полю частных

Поле частных F целостного **кольца** L состоит из классов эквивалентности ***несократимых*** дробей $\frac{a}{b}$, где $a, b \in L; b \neq 0$, а ***эквивалентность*** понимается следующим образом:

$$\left[\frac{a}{b} \sim \frac{c}{d}\right] \Leftrightarrow [ad = bc].$$

Всякий многочлен над L можно рассматривать над F.

Всякий многочлен над F представляется в виде произведения некоторой константы, принадлежащей F, и некоторого многочлена (причем – ***примитивного***) с коэффициентами из L.

Установим связь понятий ***неприводимости*** для ***примитивного*** многочлена $f(x) \in L[x]$:

над **кольцом** L

и

над **полем** F.

Изложение (для простоты) ведется в простейшем случае:

$$L = \mathbb{Z}; F = \mathbb{Q},$$

это позволяет считать содержание и примитивную часть однозначно определенными.

С каждым ***рациональным*** многочленом ассоциирован некоторый примитивный ***целочисленный*** многочлен $f(x) \in \mathbb{Q}[x]$, который представляется в виде

$$f(x) = \frac{1}{d}\tilde{f}(x) = \frac{c}{d}\tilde{\tilde{f}}(x),$$

где

d – ***наименьший общий знаменатель*** коэффициентов $f(x)$,

$\tilde{f}(x)$ – многочлен с целыми коэффициентами,

$c = \mathrm{cont}(\tilde{f})$ – ***содержание*** этого многочлена,

$\tilde{\tilde{f}}(x)$ – ***примитивный*** многочлен с целыми коэффициентами.

Рациональное число $\frac{c}{d}$ будем называть ***рациональным содержанием*** многочлена $f(x)$.

Неприводимость

$$\overset{?}{(\text{над } \mathbf{Z}) \Leftrightarrow (\text{над } \mathbf{Q})}$$

В сторону $\Leftarrow$ утверждение очевидно: если $f(x)$ многочлен положительной степени, приводим над $\mathbb{Z}$, то он приводим и над $\mathbb{Q}$; значит, неприводимость над $\mathbb{Q}$ влечет неприводимость над $\mathbb{Z}$.

В сторону $\Rightarrow$.

Пусть $f(x) \in \mathbb{Z}[x]$ ***примитивен*** и ***приводим*** над $\mathbb{Q}$,

т. е. разлагается на два необратимых множителя в кольце $\mathbb{Q}[x]$:

$$f(x) = g(x)h(x).$$

В каждом из множителей выделим ***рациональное содержание*** и ***примитивную*** целочисленную часть:

$$f(x) = \frac{c_1}{d_1}\frac{c_2}{d_2}\widetilde{g}(x)\widetilde{h}(x).$$

Произведение примитивных многочленов "с волнами" также является примитивным многочленом над $\mathbb{Z}$. Избавляясь от знаменателей, получим:

$$d_1 d_2 f(x) = c_1 c_2 \widetilde{g}(x)\widetilde{h}(x),$$

что, с учетом примитивности $f(x)$, влечет два равенства: $d_1 d_2 = c_1 c_2$ и $f(x) = \widetilde{g}(x)\widetilde{h}(x)$. Значит, данный многочлен ***приводим*** над $\mathbb{Z}$; ***неприводимость*** над $\mathbb{Z}$ влечет ***неприводимость*** над $\mathbb{Q}$.

Таким образом, доказана

Теорема 3.

Примитивный целочисленный многочлен неприводим над $\mathbb{Z}$ тогда и только тогда, когда он неприводим над $\mathbb{Q}$. ■

Замечание 1. *По ходу доказательства выше дополнительно выяснилось, что исследование любого многочлена с **рациональными** коэффициентами на **неприводимость** сводится к исследованию соответствующего ему **целочисленного** многочлена.*

Задача 2. Представить процедуру вычисления *рационального содержания* $c = \mathbf{cont}(f)$ и *примитивной части* $\tilde{f} = \mathbf{prim}(f)$ для многочлена с рациональными коэффициентами $f(x) = c\,\tilde{f}(x)$.

```
> RatContPrim:=proc(f::polynom(rational),x::name)
```

Решение.

```
> RatContPrim:=proc(f::polynom(rational),x::name)
  local cl,dcl,b,ncl,a,rcf,prf;
if f=0 then
  RETURN(NULL);
else
  cl:=[seq(coeff(f,x,i),i=0..degree(f,x))];
  dcl:=map(z->denom(z),cl);
  b:=ilcm(dcl[]);
  ncl:=map(z->z*b,cl);
  a:=igcd(ncl[]);
  rcf:=a/b;
  prf:=sort(simplify(f/rcf),x);
  RETURN(rcf,prf);
end if;
end proc;
```

Примеры применения.

```
> f,g,h:=(4/3)*x^10+(2/5)*x^4-6/5,
   (5/9)*x^4-(15/2)*x^2+10*x+25/3,
   (1/21)*x^100-(2/33)*x+5;
```

$$f, g, h := \frac{4}{3}x^{10} + \frac{2}{5}x^4 - \frac{6}{5}, \frac{5}{9}x^4 - \frac{15}{2}x^2 + 10x + \frac{25}{3}, \frac{1}{21}x^{100} - \frac{2}{33}x + 5$$

```
> map(expr->[RatContPrim(expr,x)],[f,g,h]);
```

$$\left[\left[\frac{2}{15}, 10x^{10} + 3x^4 - 9\right], \left[\frac{5}{18}, 2x^4 - 27x^2 + 36x + 30\right], \left[\frac{1}{231}, 11x^{100} - 14x + 1155\right]\right]$$

ПРИЗНАКИ НЕПРИВОДИМОСТИ

(для многочленов с целыми коэффициентами,
допускают перенос на "абстрактный" случай)

Признак Эйзенштейна.

Теорема 4 (Эйзенштейн). *Пусть*

$$f(x) = f_0 + f_1 x + \cdots + f_{n-1} x^{n-1} + f_n x^n \in \mathbb{Z}[x]$$

многочлен положительной степени n.

Если существует простое натуральное число p, *делящее все коэффициенты многочлена, кроме старшего, причем свободный член не делится на* p^2, *то* $f(x)$ *неприводим*.

Доказательство. Предположим противное:

$$f(x) = g(x)h(x); \qquad (*)$$

$$g(x) = g_0 + gx + \cdots + g_m x^m;\ g_m \neq 0;$$

$$h(x) = h_0 + h_1 x + \cdots + h_l x^l;\ h_l \neq 0;$$

$$m, l > 0;\ m + l = n.$$

Приравняем ***свободные члены*** в **(*)**:

$$f_0 = g_0 h_0.$$

Имеем: $p | f_0$ и $p^2 \nmid f_0$; следовательно, справедлива ***одна и только одна*** из делимостей: $p | g_0$ или $p | h_0$. Пусть, для определенности, $p | g_0$ и $p \nmid h_0$.

Приравняем теперь ***старшие коэффициенты*** в **(*)**:

$$f_n = g_m h_l.$$

Имеем: $p \nmid f_n$ и, следовательно, $p \nmid g_m$ и $p \nmid h_l$.

Итак, p не может делить все коэффициенты $g(x)$; пусть g_{j_0} – крайний слева из не делящихся на p коэффициентов $g(x)$.

Приравняем в (*) коэффициенты при x^{j_0}:

$$f_{j_0} = g_0 h_{j_0} + g_1 h_{j_0-1} + \cdots + g_{j_0-1} h_1 + g_{j_0} h_0 .$$

Левая часть делится на p (т. к. $j_0 \leqslant m < n$); в правой части все слагаемые, кроме последнего, также делятся на p.

В силу *простоты* p, последнее слагаемое не может делиться на p. Противоречие. ■

Следствие 1. Всякий ***двучлен*** $f(x) = x^n + pa$ (где n - натуральное, a - целое, p - ***простое, не делящее*** a) ***неприводим*** над $\mathbb{Z}$.

Следствие 2. Для любого натурального n существует неприводимый целочисленный многочлен степени n.

(*Автоматически над* $\mathbb{Q}$ *оказывается справедливым аналогичный факт.*)

Пример 1. Многочлен $f(x) = x^4 + 4$ ***приводим*** над $\mathbb{Z}$:

$$f(x) = x^4 + 4x^2 + 4 - 4x^2 = (x^2 + 2)^2 - (2x)^2 =$$
$$= (x^2 - 2x + 2)(x^2 + 2x + 2),$$

где оба квадратных трехчлена имеют дискриминант (-4) и поэтому ***неприводимы*** не только над ***кольцом*** $\mathbb{Z}$ и ***полем*** $\mathbb{Q}$, но и над ***полем*** $\mathbb{R}$; над ***полем*** $\mathbb{C}$ они ***приводимы***, многочлен $f(x)$ имеет четыре комплексных ***корня*** $x_{1,2,3,4} = \pm 1 \pm i$ и следующее разложение на ***линейные*** множители:

$$f(x) = (x - (1 + i))(x - (1 - i))(x - (-1 + i))(x - (-1 - i)).$$

Пример 2. Многочлен $f(x) = x^4 + 2$ ***неприводим*** над $\mathbb{Z}$ и над $\mathbb{Q}$ в силу ***признака Эйзенштейна***. Однако, если поле $\mathbb{Q}$ ***расширить***, присоединив к нему элемент $\alpha = \sqrt[4]{2}$, то $f(x)$ окажется ***приводимым***:

$$f(x) = x^4 + 2\sqrt{2}x^2 + 2 - 2\sqrt{2}x^2 = \left(x^2 + 2^{1/2}\right)^2 - \left(2^{3/4}x\right)^2 =$$

$$= \left(x^2 + \alpha^2\right)^2 - \left(\alpha^3 x\right)^2 = \left(x^2 - \alpha^3 x + \alpha^2\right)\left(x^2 + \alpha^3 x + \alpha^2\right),$$

где снова оба квадратных трехчлена имеют отрицательный дискриминант $\alpha^6 - 4\alpha^2 = \alpha^6 - \alpha^{10} = \alpha^6(1 - \alpha^4) = -\alpha^6$ и поэтому ***неприводимы*** над $\mathbb{Q}$ (и над $\mathbb{R}$).

Полное разложение $\boldsymbol{f(x)}$ будет достигнуто, если к полю $\mathbb{Q}$ добавить два элемента $\{\boldsymbol{\alpha, i}\}$, после чего $\boldsymbol{f(x)}$ будет иметь четыре корня

$$\boldsymbol{x_{1,2,3,4} = \frac{\alpha^3}{2}(\pm 1 \pm i)}$$

и разложение:

$$\boldsymbol{f(x) = \left(x - \frac{\alpha^3}{2}(1+i)\right)\left(x - \frac{\alpha^3}{2}(1-i)\right)\left(x - \frac{\alpha^3}{2}(-1+i)\right)\left(x - \frac{\alpha^3}{2}(-1-i)\right).}$$

Замечание 2. *Ключевая идея теории полей: поля* ***расширяются*** *присоединением к ним* ***корней неприводимых многочленов****. Если к данному полю присоединить корни* ***всех*** *неприводимых многочленов над ним, то получится* ***алгебраическое замыкание*** *данного поля. Алгебраическим замыканием поля* $\mathbb{Q}$ *является поле*

$$\mathbb{A} = \overline{\mathbb{Q}}$$

так называемых ***алгебраических чисел*** *(являющихся корнями всевозможных многочленов с целыми коэффициентами).*

Известный с первого семестра пример алгебраического замыкания:

$$\mathbb{C} = \overline{\mathbb{R}}.$$

Замечание 3. *Не все целочисленные многочлены могут быть исследованы на* ***неприводимость*** *с помощью* ***признака Эйзенштейна****. Используются другие, более сильные признаки.*

Однофамильцы известного французского математика

Алекса́ндр Дюма́ (отец) (фр. *Alexandre Dumas, père*; **1802 —1870**) — французский писатель, чьи приключенческие романы сделали его одним из самых читаемых французских авторов в мире.

Алекса́ндр Дюма́ (сын) (фр. *Alexandre Dumas fils*, **1824 —1895**) — французский драматург и прозаик

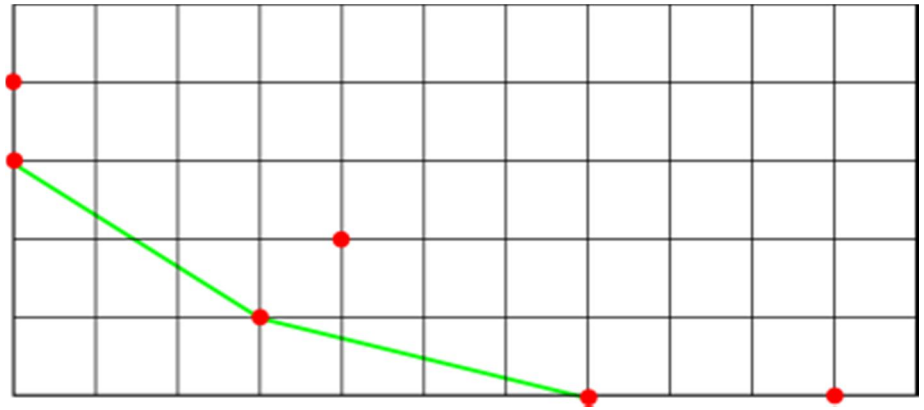
JOURNAL DE MATHÉMATIQUES
PURES ET APPLIQUÉES

"Геометрический"
признак Г. Дюма *(1906),*
использует так
называемые
многоугольники Ньютона.

G. DUMAS

Sur quelques cas d'irréductibilité des polynomes à coefficients rationnels

Journal de mathématiques pures et appliquées 6^e série, tome 2 (1906), p. 191-258.
<http://portail.mathdoc.fr/JMPA/afficher_notice.php?id=JMPA_1906_6_2_A5_0>



Теорема 5 (Основная теорема алгебры многочленов).

Кольцо многочленов над факториальным кольцом само является факториальным, т. е. всякий ненулевой многочлен над факториальным кольцом однозначно (с точностью до порядка сомножителей и их ассоциированности) разлагается на неразложимые множители (среди которых могут присутствовать неразложимые константы и неприводимые примитивные многочлены положительной степени).

Доказательство см., например, в пособии *Н. И. Яцкин.* ***Алгебра: Теоремы и алгоритмы****. Иваново: ИвГУ, 2006* (с 427-428).

В следующей теме будет рассмотрен ***тест Кронекера*** на ***неприводимость*** целочисленного многочлена и ***алгоритм Кронекера факторизации*** (разложения на неприводимые множители) в кольце $\mathbb{Z}[x]$.

Леопо́льд Кро́некер (нем. *Leopold Kronecker*; **1823 — 1891**) — немецкий математик. Был сторонником ***"арифметизации" математики***, которая по его мнению, должна быть сведена к арифметике целых чисел; только последняя, как он утверждал, обладает подлинной реальностью.

Защищая эти взгляды, вёл упорную дискуссию с принципами ***теоретико-функциональной*** школы **К. Вейерштрасса** и ***теоретико-множественной*** школы **Г. Кантора**.

Следующее выражение Кронекера стало знаменитым:

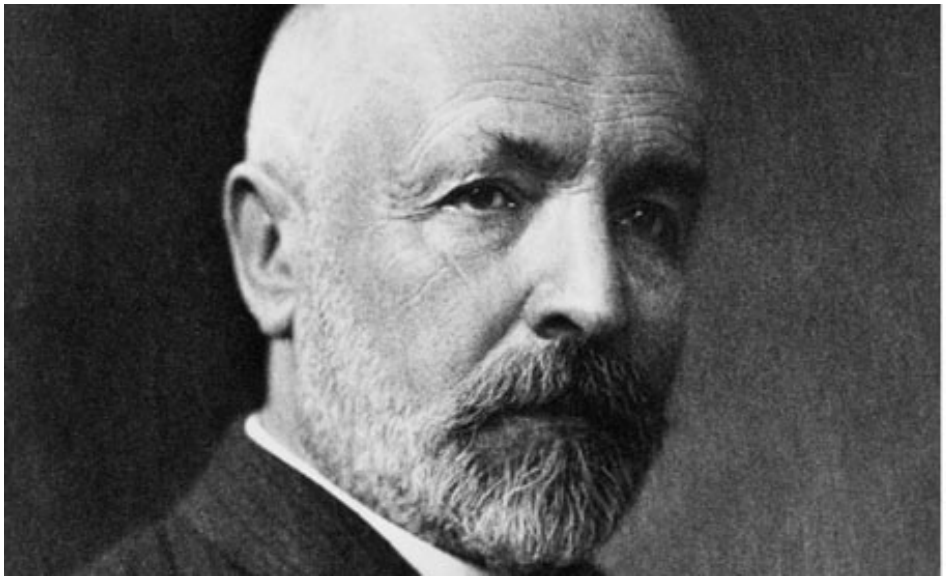
Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.

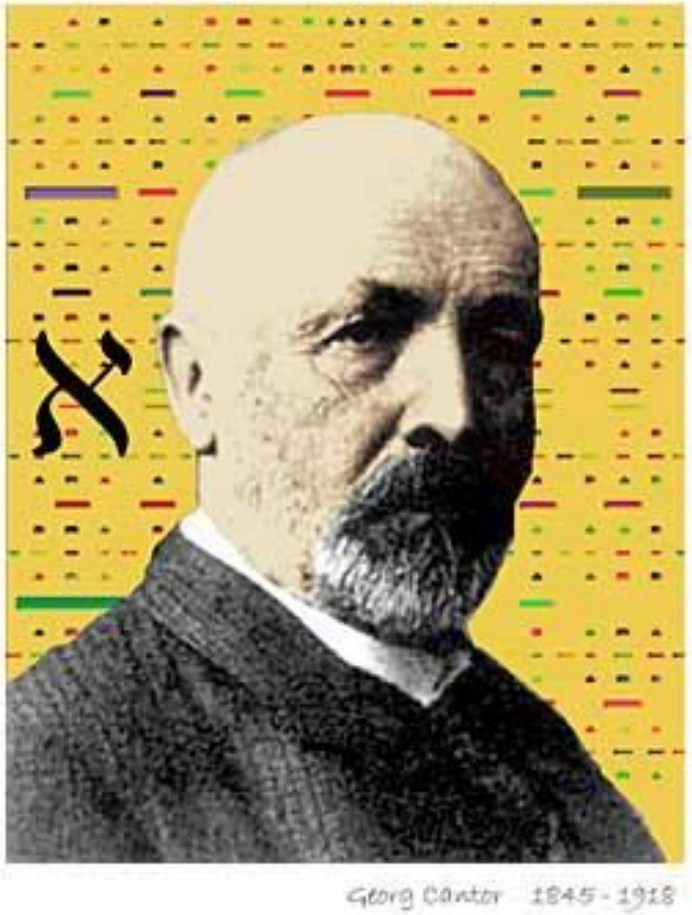
Бог создал целые числа,
всё остальное — дело рук человека.

$\aleph_0$

Гео́рг Ка́нтор (нем. *Georg Ferdinand Ludwig Philipp Cantor*, **1845**, **Санкт-Петербург** — **1918**) — немецкий математик. Наиболее известен как создатель ***теории множеств***, ставшей краеугольным камнем в математике.

Критика его трудов была порой очень агрессивна: так, **Пуанкаре** называл его идеи ***"тяжёлой болезнью"***, поражающей математическую науку; а в публичных заявлениях и личных выпадах **Кронекера** в адрес **Кантора** мелькали иногда такие эпитеты, как ***"научный шарлатан"***, ***"отступник"*** и ***"развратитель молодёжи"***.




Georg Cantor 1845 - 1918