Закон взаимности Вейля: от теоремы Виета до квадратичного закона взаимности

Н. С. Калинин, М. И. Магин

> Алгебра — это предложение, которое дьявол делает математику. Дьявол говорит: «Я дам тебе эту мощную машину, она ответит на любой твой вопрос. Всё, что тебе нужно сделать — это отдать мне свою душу: откажись от геометрии, и ты получишь эту чудесную машину».
>
> *сэр Майкл Атья*, 2002

§ 1. Введение

Закон взаимности Вейля для многочленов

Рассмотрим два приведённых (т. е. со старшим коэффициентом один) многочлена f и g степеней n и m соответственно и предположим, что f имеет ровно n различных вещественных корней, а g — ровно m. Подсчитаем произведение значений f в корнях g и произведение значений g в корнях f.

Если

$$f(x) = (x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n),$$
$$g(x) = (x-\beta_1)\cdot\ldots\cdot(x-\beta_m),$$

Исследование М. И. Магина выполнено в Санкт-Петербургском международном математическом институте имени Леонарда Эйлера при финансовой поддержке Министерства науки и высшего образования Российской Федерации (соглашение № 075-15-2022-287 от 06.04.2022).

то
$$\prod_{j=1}^{m} f(\beta_j) = \prod_{i,j=1}^{n,m} (\beta_j - \alpha_i), \quad \prod_{i=1}^{n} g(\alpha_i) = \prod_{i,j=1}^{n,m} (\alpha_i - \beta_j). \tag{1}$$

Мы получили *закон взаимности Вейля* в простейшей форме: произведение значений f в корнях g и произведение значений g в корнях f равны или отличаются знаком (если nm нечётно).

Упражнение 1. а) Каким будет выражение, если многочлены не приведённые, т. е. коэффициент при старшей степени x не равен 1?

б) Покажите, что возникающая поправка равна пределу отношения f^m/g^n при x стремящемся к бесконечности.

Упражнение 2. Используя предыдущее упражнение, вычислите поправку в общем случае, т. е. когда многочлены f и g могут иметь кратные и общие корни. *Подсказка*: поведение $f(x)$ в окрестности нуля похоже на поведение $f(1/x)$ при $x \to \infty$.

Настоящая заметка посвящена связи закона взаимности Вейля с *квадратичным законом взаимности*.

Напомним, что для целого a и нечётного простого p *символ Лежандра* $\left(\frac{a}{p}\right)$ равен нулю, если a делится на p, и ± 1 соответственно тому, разрешимо сравнение $a \equiv x^2 \pmod{p}$ или нет.

Теорема 1 (квадратичный закон взаимности). *Пусть p и q — различные нечётные простые числа. Тогда*
$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Обнаружил этот закон Леонард Эйлер, затем Лежандр доказал несколько частных случаев, а первое полноценное доказательство дал Гаусс (впоследствии нашедший ещё семь доказательств, см. [GW86]). Сейчас известно великое множество самых разных доказательств. Одно из самых коротких и элегантных из них предложил в 1872 году русский математик Егор Иванович Золотарёв. Оно изложено, например, в [Го13].

Квадратичный закон взаимности существует не только для целых чисел, но и для *многочленов по модулю p*. Он был сформулирован Рихардом Дедекиндом в 1857 году в работе [Ded57] (всего через 2 года после смерти Гаусса) и впервые доказан Эмилем Артином в 1924 году в работе [Art24]. Отметим, что утверждение, называемое теперь законом взаимности Вейля, сформулировано как вспомогательный пример в письме Эмилю Артину от Андре Вейля 10 июля 1942.

Итак, оказывается, что кольца $\mathbb{Z}$ и $\mathbb{F}_p[x]$ похожи, а простые числа в $\mathbb{Z}$ похожи на неприводимые многочлены в $\mathbb{F}_p[x]$. Символ Лежандра для элементов $\mathbb{F}_p[x]$ определяется аналогично случаю целых чисел и при этом там также выполняется критерий Эйлера. Более того, формулировка закона взаимности практически дословно повторяет формулировку для целых чисел: для неприводимых $f, g \in \mathbb{F}_p[x]$ выполнено равенство

$$\left(\frac{f}{g}\right)\left(\frac{g}{f}\right) = (-1)^{\deg f \cdot \deg g \cdot \frac{p-1}{2}}.$$

В настоящей заметке мы покажем, что квадратичный закон взаимности для неприводимых $f, g \in \mathbb{F}_p[x]$ — это в точности утверждение о равенстве произведения значений f по корням g и произведения значений g по корням f.

Случай алгебраически незамкнутого поля

В рассуждении в самом начале заметки мы существенно пользовались тем, что все корни многочленов вещественные. Возникает вопрос — что делать, если у многочлена степени n менее n вещественных корней?

Можно поступить двояко: сказать, что мы работаем над $\mathbb{C}$, и применить такой же аргумент, или попробовать получить аналог тождества, но уже над $\mathbb{R}$. Рассмотрим минимальный интересный пример.

Пример 1. Пусть $f(x) = (x - \alpha_1)(x - \alpha_2)$, где α_i — вещественные, а $g(x) = x^2 + \beta$, $\beta > 0$. Тогда, раскладывая f на линейные одночлены с комплексными коэффициентами, мы получаем тождество

$$g(\alpha_1)g(\alpha_2) = f\left(i\sqrt{\beta}\right)f\left(-i\sqrt{\beta}\right).$$

С другой стороны, группируя скобки с сопряжёнными корнями g, можно записать правую часть вполне «вещественным» способом:

$$\left(i\sqrt{\beta} - \alpha_1\right)\left(-i\sqrt{\beta} - \alpha_1\right) = \left|\alpha_1 + i\sqrt{\beta}\right|^2.$$

Из этого примера видно, что если многочлен g, раскладывающийся на линейные множители, домножить на «неприводимый над $\mathbb{R}$ кусок» $x^2 + \beta$ с $\beta > 0$, то произведение значений f по вещественным корням g должно домножиться на $\prod_j |\alpha_j + i\sqrt{\beta}|^2$ (где α_j — все вещественные корни многочлена f).

Упражнение 3. Покажите, что произведение значений многочлена f по (возможно) комплексным корням g выражается как функция от коэффициентов g и f (можете предположить для простоты, что корни f и g различны).

Найденный только что вид поправки в тождестве может показаться странным, но в § 3 станет ясно, почему тождество над алгебраически незамкнутым полем должно быть именно таким; более того, мы научимся записывать такое тождество над произвольным полем, а не только над $\mathbb{R}$.

Упражнение 4. Доведите предыдущее рассуждение до конца и получите общий вид формулы для двух произвольных ненулевых многочленов над $\mathbb{R}$.

Римановы поверхности и мероморфные функции

Определение 1. Пусть U — открытое подмножество в $\mathbb{C}$. Функция $f\colon U \to \mathbb{C}$ называется *голоморфной*, если у каждой точки $z_0 \in U$ существует окрестность, в которой она раскладывается в сходящийся поточечно степенной ряд:

$$\forall\, z_0 \in U \;\; \exists\, r > 0\colon \forall\, z \in B_r(z_0) \quad f(z) = \sum_{k=0}^{\infty} a_k (z - z_0)^k.$$

Эквивалентное определение: функция голоморфна, если ряд Тейлора функции f определён и поточечно сходится к f в окрестности каждой точки z_0:

$$f(z) = f(z_0) + f'(z_0)(z - z_0) + \frac{f''(z_0)}{2}(z - z_0)^2 + \ldots + \frac{f^{(k)}(z_0)}{k!}(z - z_0)^k + \ldots$$

Пример 2. Многочлен или экспонента — голоморфные функции во всей комплексной плоскости.

К сожалению, голоморфных функций не слишком много, поэтому мы рассмотрим более широкий класс функций.

Определение 2. Функция $f\colon U \to \mathbb{C}$ называется *мероморфной*, если в окрестности каждой точки U она раскладывается в степенной ряд, но для дискретного множества точек из U этот ряд может начинаться с отрицательной степени, т. е. иметь вид

$$f(z) = \frac{a_{-k}}{(z - z_0)^k} + \frac{a_{-k+1}}{(z - z_0)^{k-1}} + \ldots + \frac{a_{-1}}{(z - z_0)} + a_0 + a_1 z + \ldots$$

для некоторого натурального k. Такая точка z_0 называется *полюсом* функции f, а число k — *порядком* или *кратностью* полюса.

Если же ряд начинается с положительной степени $a_k(z-z_0)^k$, $k>0$, то f имеет ноль в точке k. В этом случае число k называют *кратностью нуля*.

Заметим, что мероморфная функция f имеет полюс порядка k в точке z_0 тогда и только тогда, когда $1/f$ имеет в этой точке ноль порядка k.

Пример 3. Мероморфными являются рациональные функции, т. е. функции вида $f(z)=p(z)/q(z)$, где p и q — многочлены, причём q не равен нулю тождественно.

Для дальнейших обобщений нам также понадобится рассматривать функции не только на прямой (вещественной или комплексной), но и на кривых и поверхностях. Напомним соответствующие определения.

Двумерную ориентируемую хаусдорфову поверхность S называют *римановой поверхностью*, если у каждой точки $p\in S$ есть окрестность $U\subset S$, отождествлённая с единичным диском

$$\mathbb{D}=\{z\in\mathbb{C},\ |z|<1\}\subset\mathbb{C}$$

взаимно однозначным отображением[1] $\varphi_U\colon U\to\mathbb{D}$. Причём, если у нас есть две пересекающиеся окрестности U и V, которые отождествляются с диском при помощи взаимно однозначных отображений φ_U и φ_V, то мы требуем, чтобы отображение $\varphi_U\varphi_V^{-1}$ было голоморфным (там, где оно определено, т. е. на $U\cap V$).

Простейшим компактным примером римановой поверхности является *комплексная проективная прямая* $\mathbb{C}P^1$, она же *сфера Римана*, она же *расширенная комплексная плоскость* $\widehat{\mathbb{C}}=\mathbb{C}\cup\infty$. Топологически $\mathbb{C}P^1$ представляет собой обычную двумерную сферу, а добавление точки $\{\infty\}$ — это одноточечная компактификация комплексной плоскости $\mathbb{C}$.

Так как риманова поверхность локально устроена как единичный диск в комплексной плоскости, мы можем говорить о голоморфных и мероморфных функциях на ней. В маленькой окрестности каждой точки p римановой поверхности S мы можем выбрать локальную координату z и разложить функцию f в ряд

$$f(z)=a_0z^k+a_1z^{k+1}+\ldots$$

[1] Мы также будем требовать, чтобы при этом отождествлении точка p переходила в $0\in\mathbb{D}$. Это отождествление мы будем называть *локальным параметром* или *локальной координатой* в окрестности точки p.

Наименьшую степень k в этом разложении мы будем называть *порядком* функции f в точке p и обозначать $\mathrm{ord}_p f$. Для мероморфной функции на римановой поверхности порядок функции в точке p *не зависит от выбора локального параметра*.

Если p — нуль функции f, то $\mathrm{ord}_p f$ — кратность нуля, а если p — полюс функции f, то $\mathrm{ord}_p f$ — это кратность полюса со знаком минус. Если же p — не ноль и не полюс, то $\mathrm{ord}_p f = 0$.

Пример 4. Так как мероморфная функция на римановой поверхности S — это голоморфная функция, которой на некотором дискретном множестве разрешили принимать значение ∞, все мероморфные функции $S \to \mathbb{C}$ — это просто голоморфные функции из S в $\mathbb{C}P^1$.

Например, непостоянные многочлены являются мероморфными функциями на $\mathbb{C}P^1$ с единственным полюсом в точке ∞. Более того, любая мероморфная функция на $\mathbb{C}P^1$ рациональна, т. е. представляется в виде частного двух многочленов.

Для двух многочленов

$$f(z) = a_0 + a_1 z + \ldots + a_n z^n \quad \text{и} \quad g = b_0 + b_1 z + \ldots + b_m z^m$$

без общих нулей определим *символ Вейля* в точке $p \in \mathbb{C}P^1$ как

$$[f, g]_p = (-1)^{\mathrm{ord}_p f \cdot \mathrm{ord}_p g} \cdot \frac{f(p)^{\mathrm{ord}_p g}}{g(p)^{\mathrm{ord}_p f}}, \quad [f, g]_\infty = \frac{a_n^m}{b_m^n}.$$

В этих терминах формула (1) переписывается таким образом:

$$\prod_{p \in \mathbb{C}P^1} [f, g]_p = 1.$$

Оказывается, что закон взаимности Вейля выполняется не только для пары многочленов на $\mathbb{C}P^1$, но и для произвольной пары ненулевых мероморфных функций на компактной римановой поверхности.

В § 2 мы обсуждаем закон взаимности Вейля для произвольных мероморфных функций на компактной римановой поверхности, его связь с теоремами Карно и Менелая из планиметрии, а также «комбинаторный» способ его доказывать. В § 3 мы изучим прямую связь между законом взаимности Вейля и квадратичным законом взаимности для многочленов над конечным полем. Эти параграфы можно читать параллельно. В § 4 мы немного поговорим о законах взаимности в общем и о локально-глобальном принципе в арифметике и алгебраической геометрии.

Закон взаимности Вейля является яркой иллюстрацией математического стиля и вкуса Андре Вейля, в работах которого переплетения арифметики, алгебры и геометрии приводят к поразительным открытиям.

§ 2. В направлении закона взаимности Вейля

Теоремы Менелая и Карно и теорема Виета

Оказывается, теорема Вейля связана с классическими теоремами Менелая и Карно. Теорема Менелая утверждает, что если прямая ℓ пересекает стороны AB, BC, AC треугольника ABC в точках C', A', B', то выполняется равенство

$$\frac{|AC'|}{|C'B|} \cdot \frac{|BA'|}{|A'C|} \cdot \frac{|CB'|}{|B'A|} = 1.$$

Её естественным обобщением является теорема Лазаря Карно, которая утверждает, что если коника пересекает стороны AB, BC, AC треугольника ABC в точках C'_1, C'_2, A'_1, A'_2, B'_1, B'_2, то выполнено равенство

$$\frac{|AC'_1| \cdot |AC'_2|}{|C'_1B| \cdot |C'_2B|} \cdot \frac{|BA'_1| \cdot |BA'_2|}{|A'_1C| \cdot |A'_2C|} \cdot \frac{|CB'_1| \cdot |CB'_2|}{|B'_1A| \cdot |B'_2A|} = 1.$$

Существует множество различных геометрических доказательств теоремы Карно. Например, проективным преобразованием переведём конику в окружность, тогда искомая формула получается выписыванием степеней точек A, B и C. Остаётся заметить, что искомая формула — тождество на двойные отношения, которые не изменяются при проективных преобразованиях.

Оказывается, что простая алгебраическая техника позволяет получить обобщение этой теоремы на кривые *произвольной* степени.

Определение 3. *Плоская вещественная алгебраическая кривая степени d* — это кривая в $\mathbb{R}^2$, заданная уравнением

$$F(x, y) = \sum_{i+j \leqslant d,\, 0 \leqslant i, j} a_{ij} x^i y^j = 0,$$

причём $a_{ij} \neq 0$ хотя бы для одной пары индексов с суммой d.

Пример 5. Коники — это плоские алгебраические кривые степени 2.

Итак, предположим, что плоская алгебраическая кривая $F(x, y) = 0$ пересекает стороны AB, BC, AC треугольника ABC в точках $C_1', \ldots C_d'$, $A_1', \ldots, A_d'$, $B_1', \ldots, B_d'$; для простоты мы предполагаем, что все эти точки различны и не совпадают с вершинами треугольника.

Прямую (AB) в координатах зададим как $A + tv$, где $t \in \mathbb{R}$, а v — единичный вектор, сонаправленный со стороной AB. Подставим уравнение прямой (AB) в уравнение, задающее кривую, и запишем его в виде многочлена от t:

$$F(A + tv) = a_0 + a_1 t + \ldots + a_d t^d = 0.$$

Заметим, что произведение корней F равно в точности

$$|AC_1'| \cdot |AC_2'| \cdot \ldots \cdot |AC_d'|.$$

С другой стороны, по теореме Виета оно равно $(-1)^d \frac{a_d}{a_0}$. Очевидно, что $a_0 = F(A)$, вычислим коэффициент a_d. Разобьём многочлен $F(x, y)$ в сумму «однородных компонент»:

$$F(x, y) = F_0(x, y) + F_1(x, y) + \ldots + F_d(x, y),$$

в F_k входят только мономы степени k.

Так как a_d — коэффициент при старшей степени t, он может получаться только из мономов старшей степени, т. е. $a_d = F_d(v)$. Таким образом, мы получаем

$$|AC_1'| \cdot |AC_2'| \cdot \ldots \cdot |AC_d'| = (-1)^d \frac{F(A)}{F_d(v)}.$$

Выписывая аналогичную формулу для произведения

$$|BC_1'| \cdot |BC_2'| \cdot \ldots \cdot |BC_d'|$$

и вершины B, мы получаем

$$\frac{|AC_1'| \cdot |AC_2'| \cdot \ldots \cdot |AC_d'|}{|BC_1'| \cdot |BC_2'| \cdot \ldots \cdot |BC_d'|} = \frac{F(A)}{F(B)}.$$

Проделав так для каждой стороны треугольника ABC, получаем обобщение теоремы Карно для произвольной плоской кривой степени d.

При рассмотрении кривых в $\mathbb{R}^2$ могут возникать разные неприятности (например, в рассуждении выше нам приходилось требовать, чтобы кривая пересекала каждую сторону треугольника в d точках, а это далеко не всегда так). Этих неприятностей можно избежать, если рассматривать кривые в комплексной проективной плоскости $\mathbb{C}P^2$.

Определение 4. *Комплексная проективная плоскость* $\mathbb{C}P^2$ — это множество комплексных прямых в $\mathbb{C}^3$, проходящих через начало координат, иными словами,

$$\mathbb{C}P^2 = \{(x, y, z) \neq 0 \mid (x, y, z) \sim (\lambda x, \lambda y, \lambda z)\}.$$

Каждой плоской алгебраической кривой $F(x, y) = 0$ сопоставим алгебраическую кривую $F(x, y, z) = 0$ в $\mathbb{C}P^2$ при помощи гомогенизации многочлена:

$$F(x, y) = \sum_{i+j\leqslant d} a_{ij} x^i y^j \rightsquigarrow F(x, y, z) = \sum_{i+j\leqslant d} a_{ij} x^i y^j z^{d-i-j}.$$

В дальнейшем под словами «комплексная алгебраическая кривая» в этом параграфе мы понимаем именно кривую в $\mathbb{C}P^2$.

Отметим, что топологически комплексная алгебраическая кривая представляет собой непрерывный образ компактной римановой поверхности (у плоской кривой могут быть точки самопересечения, поэтому она не обязательно гомеоморфна римановой поверхности). С другой стороны, если у кривой нет особенностей, то она реализуется как компактная риманова поверхность (действительно, из теоремы о неявной функции следует, что локально она устроена как комплексный диск).

Верно и обратное: на любой компактной римановой поверхности S существуют три мероморфные функции f, g, h такие, что образ $(f, g, h)\colon S \to \mathbb{C}P^2$ — алгебраическая кривая в $\mathbb{C}P^2$ и отображение инъективно всюду, кроме конечного числа точек. Это обстоятельство позволяет каждому читателю иметь в виду то, что ему нравится — ориентируемые поверхности (т. е. сферы с ручками) или нули однородных многочленов.

Теперь мы можем дать формулировку закона взаимности Вейля для произвольной компактной римановой поверхности.

Теорема 2 (Андре Вейль, 1942). *Пусть f и g — мероморфные функции на компактной римановой поверхности S без общих нулей и полюсов. Тогда*

$$\prod_{p\in S} f(p)^{\operatorname{ord}_p g} = \prod_{p\in S} g(p)^{\operatorname{ord}_p f}.$$

Так как на компактной римановой поверхности мероморфная функция имеет лишь конечное число нулей и полюсов, в обеих частях равенства лишь конечное число сомножителей не равно единице.

Замечание 1. Вообще говоря, закон взаимности Вейля можно понимать как весьма далёкое обобщение теоремы Виета, так как в случае $S=\mathbb{C}P^1$ и $f(z)=z$, $g(z)=\sum_{k=0}^{n}a_kz^k$ мы имеем

$$\prod_{p\in\mathbb{C}} f(p)^{\mathrm{ord}_p g}=\frac{a_0}{a_n},$$

ведь это просто произведение корней g с учётом кратности.

Оригинальное доказательство Вейля практически в точности повторяет рассуждение, которое мы использовали при доказательстве теоремы Карно. Вейль рассматривал кривую C в $\mathbb{C}P^1\times\mathbb{C}P^1$, заданную образом отображения $z\mapsto(f(z),g(z))$, и её пересечения с четырьмя координатными осями $\mathbb{C}P^1\times\mathbb{C}P^1$ ($\{0\}\times\mathbb{C}P^1$, $\mathbb{C}P^1\times\{0\}$, $\{\infty\}\times\mathbb{C}P^1$, $\mathbb{C}P^1\times\{\infty\}$), так как нас интересуют значения в нулях и полюсах.

Отметим (обобщая таким образом упражнения 1 и 2), что с наличием у функций общих нулей и полюсов несложно справиться, добавляя соответствующие поправки.

Определение 5. Для пары мероморфных функций f, g на комплексной алгебраической кривой C определим *символ Вейля* $[f,g]_p$ как

$$[f,g]_p\overset{\mathrm{def}}{=}(-1)^{nm}\cdot\frac{a_n^m}{b_m^n},$$

где $f(z)=a_nz^n+\ldots$, $g(z)=b_mz^m+\ldots$ — разложения в ряд Тейлора в малой окрестности точки $p\in S$.

Тогда закон взаимности Вейля мы можем переписать в виде *формулы произведения*:

$$\prod_{p\in S}[f,g]_p=1 \tag{2}$$

и в такой формулировке функции f и g уже могут иметь общие нули. Как мы увидим в § 4, такая форма записи (в виде произведения по всем точкам кривой) является стандартной для законов взаимности.

Комбинаторное доказательство закона Вейля

Как мы уже отмечали, компактная риманова поверхность топологически представляет собой сферу с g ручками. Её можно разрезать на «элементарные» кусочки — пары штанов. Каждую пару штанов, в свою очередь, можно разрезать[2)] на три цилиндра. Можно ли доказать закон Вейля отдельно на каждом кусочке, а потом всё склеить?

[2)] При разрезании появятся «углы», но нам здесь это несущественно.

Дело в том, что для поверхности с краем S (коей является цилиндр) закон взаимности Вейля может не выполняться, так что заведём для поправки в формуле следующее обозначение:

$$\mathrm{WP}(S, f, g) \stackrel{\text{def}}{=} \frac{\prod_{p\in S} f(p)^{\mathrm{ord}_p g}}{\prod_{p\in S} g(p)^{\mathrm{ord}_p f}}.$$

Рассмотрим комплексный цилиндр $C = \{z \in \mathbb{C} \mid R_1 < z < R_2\}$, и пусть S_2 и S_1 — его внешняя и внутренняя граничные окружности соответственно. Предположим, что они ориентированы стандартным образом (внешняя — против часовой стрелки, внутренняя — по часовой стрелке).

Упражнение 5. Докажите, что произведение Вейля на цилиндре вычисляется следующим образом:

$$\mathrm{WP}(C, f, g) = \frac{\varphi(S_2)}{\varphi(S_1)},$$

где

$$\varphi(S_i) = \varphi(f, g, S_i) = \exp\left(\frac{1}{2\pi i}\int_{S_i} \log(f)\,\frac{dg}{g}\right).$$

Упражнение 6. Пользуясь формулой из упражнения 5, изучите, что происходит с произведением Вейля при склейке двух цилиндров по граничной окружности.

Упражнение 7. Выведите из предыдущих двух упражнений закон взаимности Вейля (теорема 2).

Это доказательство вдохновлено идеями из *тропической геометрии* и появилось при изучении авторами тропического аналога закона взаимности Вейля. Ознакомиться с ним можно в работе [KM24].

§ 3. В направлении квадратичного закона взаимности

Попробуем вывести из закона взаимности Вейля аналог квадратичного закона взаимности для неприводимых многочленов над конечным полем $\mathbb{F}_p$.

Рассмотрим два многочлена

$$f = a_0 + a_1 x + \ldots + x^n \quad \text{и} \quad g = b_0 + b_1 x + \ldots + x^m$$

над алгебраически замкнутым полем $\Bbbk$ и предположим, что они не имеют общих корней. Разложим их на множители:

$$f(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n),$$
$$g(x) = (x - \beta_1) \cdot \ldots \cdot (x - \beta_m).$$

Тогда, как мы уже видели в 1,

$$\prod_{j=1}^{m} f(\beta_j) = \prod_{i=1}^{n} g(\alpha_i) \cdot (-1)^{mn}, \tag{3}$$

ведь в рассуждении для многочленов мы пользовались только тем, что многочлены раскладываются на линейные сомножители.

Чтобы подобраться к квадратичному закону взаимности, логично было бы посмотреть на это тождество над конечным полем $\mathbb{F}_p$. Соответственно, для начала попробуем установить, как выглядит аналог тождества (3) для не замкнутого поля $\Bbbk$. Для этого нам понадобится немного *теории Галуа*. Для понимания дальнейшего материала достаточно знакомства с определением группы Галуа расширения, см. классические учебники [Че34], [По63] или [Ар16].

Определение 6. Пусть L — конечное расширение поля K. Тогда мы можем рассматривать L как конечномерное векторное пространство над K и каждый элемент $\alpha \in L$ задаёт линейное отображение

$$m_\alpha \colon L \to L, \quad m_\alpha x = \alpha \cdot x.$$

Нормой элемента α называется

$$\mathrm{N}_{L/K}(\alpha) \stackrel{\text{def}}{=} \det(m_\alpha).$$

Пример 6. Если мы рассматриваем $\mathbb{C}$ как расширение поля вещественных чисел, то с каждым комплексным числом $z = a + bi$ связано линейное отображение $m_z(w) = z \cdot w$. Матрица этого линейного отображения в базисе $\{1, i\}$ имеет вид

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Её часто называют *матричной формой* комплексного числа z. В этом случае норма z равна $a^2 + b^2$, т. е. квадрату модуля z.

Пример 7. Рассмотрим расширение $\mathbb{Q}$ присоединением $\sqrt{d}$, где d — целое число, свободное от квадратов и не равное 0 или 1, т. е. множество

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

Числа такого вида образуют поле. Тогда для $\alpha = a + b\sqrt{d}$ матрица линейного отображения m_α в базисе $\{1, \sqrt{d}\}$ имеет вид

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix},$$

откуда получаем

$$\mathrm{N}(\alpha) = \det\begin{pmatrix} a & bd \\ b & a \end{pmatrix} = a^2 - db^2.$$

Это определение удобно в работе со вполне конкретными расширениями маленькой степени, но для наших целей оно не подходит, так как неочевидна его связь с корнями каких-либо многочленов.

Оказывается, что теорема Виета подсказывает более удобное для нас определение[3]. А именно, пусть L/K — расширение Галуа[4], $\alpha \in L$. Тогда все корни минимального многочлена элемента α над алгебраическим замыканием поля K, содержащим L, — это в точности набор $\{\sigma\alpha\}_{\sigma \in \mathrm{Gal}(L/K)}$ и норма вычисляется как

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma\alpha.$$

Пример 8. Обратимся ещё раз к примеру 7.

Группа Галуа $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ — циклическая группа из двух элементов id и $\sigma\colon \sqrt{d} \mapsto -\sqrt{d}$, откуда сразу же видно, что норма элемента $\alpha = a + b\sqrt{d}$ равна

$$\mathrm{N}(\alpha) = \alpha \cdot \bar{\alpha} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$

Посмотрим на это немного иначе. Реализуем расширение $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ как факторкольцо[5] $\mathbb{Q}[x]/(x^2 - d)$ и посмотрим на элементы из $\mathbb{Q}(\sqrt{d})$ как на классы многочленов из $\mathbb{Q}[x]$. Тогда для

$$\alpha = f(\sqrt{d}) = f \pmod{x^2 - d},$$

где $f = bx + a \in \mathbb{Q}[x]$, мы имеем

$$\mathrm{N}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})} \sigma(f(\sqrt{d})) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})} f(\sigma(\sqrt{d})) = f(\sqrt{d}) \cdot f(-\sqrt{d}).$$

В первом равенстве мы пользуемся тем, что σ — гомоморфизм полей, оставляющий на месте элементы поля $\mathbb{Q}$. То есть, при таком взгляде на расширение, норма элемента есть *произведение значений одного многочлена в корнях другого*!

---

[3] Достаточно найти связь между минимальным многочленом элемента α и характеристическим многочленом матрицы m_α и выразить определитель как произведение собственных чисел.

[4] То есть сепарабельное и нормальное расширение. В дальнейшем мы будем применять этот аппарат только к конечным расширениям конечных полей, которые всегда обладают такими свойствами, так что это ограничение не слишком существенно.

[5] Для этого достаточно рассмотреть сюръективный гомоморфизм

$$\mathbb{Q}[x] \to \mathbb{Q}(\sqrt{d}), \quad x \mapsto \sqrt{d}$$

с ядром $(x^2 - d)$.

Именно такое определение нормы элемента и будет удобным для нас. Отметим, что понятие нормы является фундаментальным в теории полей и алгебраической теории чисел и имеет великое множество приложений. Более подробно с этой темой (в особенности с приложениями этого понятия) читатель может ознакомиться в любом классическом учебнике по теории полей, например в [Mil22, с. 82] или [Ле65, с. 239].

Вернёмся теперь к нашему контексту. Предположим, что поле $\Bbbk$ не алгебраически замкнуто. Чтобы выкладки приняли более приятный вид, предположим, что f и g приведённые.

Тогда мы не можем разложить f и g в произведение линейных, но всегда можем разложить в произведение неприводимых многочленов со старшим коэффициентом 1:

$$f(x) = r_1(x) \cdot \ldots \cdot r_d(x),$$
$$g(x) = s_1(x) \cdot \ldots \cdot s_c(x).$$

Воспользуемся соображениями из примера 8 и рассмотрим расширения $K_i = \Bbbk[x]/r_i(x)$ и $L_j = \Bbbk[x]/s_j(x)$, порождённые корнями r_i и s_j. Тогда аналогом тождества (3) будет тождество

$$\prod_{j=1}^{m} \mathrm{N}_{L_j/\Bbbk}(f \bmod s_j) = \prod_{i=1}^{n} \mathrm{N}_{K_i/\Bbbk}(g \bmod r_i) \cdot (-1)^{mn}, \tag{4}$$

где под $(f \bmod s_j)$ мы подразумеваем класс $\bar{f} \in L_j = \Bbbk[x]/s_j(x)$. Доказательство: так как L_j получается присоединением корней s_j, сомножитель $\mathrm{N}_{L_j/\Bbbk}(f \bmod s_j)$ равен произведению значений многочлена f в корнях s_j и мы получаем тождество (4), просто записывая (3) над алгебраическим замыканием $\Bbbk^{\mathrm{alg}}$ поля $\Bbbk$ и группируя сомножители по неприводимым кусочкам.

Квадратичный закон взаимности для неприводимых многочленов над $\mathbb{F}_p$

Теперь перейдём наконец поближе к квадратичному закону взаимности и рассмотрим в качестве базового поля $\Bbbk = \mathbb{F}_p$ (p — нечётное простое). В этом случае наши расширения K_i и L_j устроены совсем несложно:

$$K_i = \mathbb{F}_p[x]/(r_i) = \mathbb{F}_{p^{\deg r_i}}, \quad L_j = \mathbb{F}_p[x]/(s_j) = \mathbb{F}_{p^{\deg s_j}}.$$

Посмотрим, что представляет собой норма для расширения вида $\mathbb{F}_{p^n}/\mathbb{F}_p$. Группа Галуа такого расширения — циклическая группа из n

элементов, порождённая автоморфизмом Фробениуса $\mathrm{Fr}_p(x) = x^p$, откуда

$$\mathrm{N}(\alpha) = \prod_{j=0}^{n-1} \mathrm{Fr}_p^j(\alpha) = \prod_{j=0}^{n-1} \alpha^{p^j} = \alpha^{1+p+p^2+\ldots+p^{n-1}} = \alpha^{\frac{p^n-1}{p-1}}.$$

Если же многочлены f и g неприводимы, тождество (4) приобретёт немного более простой вид

$$(f \bmod g)^{\frac{p^m-1}{p-1}} = (g \bmod f)^{\frac{p^n-1}{p-1}}(-1)^{mn}. \tag{5}$$

Возведём равенство в степень $(p-1)/2$:

$$(f \bmod g)^{(p^m-1)/2} = (g \bmod f)^{(p^n-1)/2} \cdot (-1)^{mn\cdot(p-1)/2}. \tag{6}$$

Это равенство уже должно напоминать читателю что-то знакомое, ведь *критерий Эйлера* говорит, что для $a \in \mathbb{Z}$ справедливо сравнение

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Тут мы понимаем a как элемент $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, а в нашей ситуации $f \bmod g \in \mathbb{F}_{p^{\deg g}} = \mathbb{F}_p[x]/(g)$, так что нужно некоторым образом обобщить критерий Эйлера.

Сначала сделаем простое наблюдение: если $\pi \in \mathbb{F}_p[x]$ — неприводимый многочлен, то количество ненулевых элементов (то есть порядок мультипликативной группы) поля $\mathbb{F}_p[x]/(\pi) = \mathbb{F}_{p^{\deg\pi}}$ равно $p^{\deg\pi} - 1$. Значит, любой ненулевой элемент этого поля при возведении в степень $p^{\deg\pi} - 1$ даёт единицу, откуда

$$f^{p^{\deg\pi}-1} \equiv 1 \pmod \pi \quad\Rightarrow\quad f^{(p^{\deg\pi}-1)/2} \equiv \pm1 \pmod \pi.$$

Знак в этом сравнении определяет, является $f \in \mathbb{F}_p[x]$ квадратом по модулю π или нет.

Предложение 1. *Пусть* $f \in \mathbb{F}_p[x]$ *— ненулевой многочлен,* $\pi \in \mathbb{F}_p[x]$ *— неприводимый. Тогда* $f^{(p^{\deg\pi}-1)/2} \equiv 1 \pmod \pi$ *в том и только том случае, когда* $f \bmod \pi$ *— квадрат в* $\mathbb{F}_p[x]/(\pi) = \mathbb{F}_{p^{\deg\pi}}$.

Доказательство этого утверждения практически полностью повторяет доказательство критерия Эйлера. В самом деле, если $f \equiv h^2 \pmod \pi$, то

$$f^{(p^{\deg\pi}-1)/2} \equiv h^{p^{\deg\pi}-1} \equiv 1 \pmod \pi.$$

Значит, любой квадрат в поле $\mathbb{F}_p[x]/(\pi) = \mathbb{F}_{p^{\deg\pi}}$ является корнем многочлена $t^{(p^{\deg\pi}-1)/2} - 1$. С одной стороны, так как мы работаем в поле, у этого многочлена не более $(p^{\deg\pi} - 1)/2$ корней, а с другой —

$(p^{\deg\pi}-1)/2$ квадратов в $\mathbb{F}_{p^{\deg\pi}}$ получаются возведением в квадрат всех элементов поля. Значит, корни этого многочлена — в точности все ненулевые квадраты в поле $\mathbb{F}_p[x]/(\pi)$. □

Пусть $\pi\in\mathbb{F}_p[x]$ — неприводимый многочлен. Тогда для $f\not\equiv 0 \pmod{\pi}$ мы можем определить *символ Лежандра* так же, как для целых чисел:

$$\left(\frac{f}{\pi}\right) \overset{\text{def}}{=} \begin{cases} 1, & \text{если сравнение } f\equiv h^2 \pmod{\pi} \text{ имеет решение,} \\ -1 & \text{в противном случае.} \end{cases}$$

В этих терминах мы можем переформулировать предложение 1 так:

$$f^{(p^{\deg\pi}-1)/2} \equiv \left(\frac{f}{\pi}\right) \pmod{\pi}.$$

Теперь остаётся лишь применить наше наблюдение к формуле (6): так как f и g неприводимы, мы имеем

$$\left(\frac{f}{g}\right) = (-1)^{\deg g\cdot\deg f\cdot(p-1)/2}\left(\frac{g}{f}\right). \tag{7}$$

Таким образом, от закона взаимности Вейля мы пришли к квадратичному закону взаимности для неприводимых многочленов над $\mathbb{F}_p$.

Упражнение 8. Какая поправка возникает в формуле (7), если многочлен f имеет старший коэффициент A, а g имеет старший коэффициент B?

Замечание 2. Для многочленов из $\mathbb{F}_p[x]$ так же, как и для целых чисел, определяется символ Лежандра и символ Якоби. Формула (4) (без перехода к неприводимым f и g, а только с разложением их на неприводимые сомножители) даёт закон взаимности для символа Якоби.

Закона взаимности для многочленов f, g над конечным полем можно получить, рассматривая результант f и g (см. заметку [Me] в настоящем сборнике). Закон взаимности Вейля на произвольной римановой поверхности тоже может быть выведен из рассмотрения некоторых более сложных результантов [Pre91].

§ 4. Законы взаимности и локально-глобальный принцип

Законом взаимности обычно называют утверждение такого типа:

Произведение (или сумма) значений какого-то выражения (например, символа Лежандра), вычисляемого локально, по всем точкам чего-то глобального (например, алгебраической кривой) равно единице (или нулю).

Утверждения такого типа также являются частными случаями локально-глобального принципа в арифметике или алгебраической геометрии. Для первого и обстоятельного знакомства с локально-глобальным принципом в арифметике мы рекомендуем заметку [Па08]. Ниже мы, опуская детали, поговорим о законах взаимности.

Чтобы пояснить, почему квадратичный закон взаимности является примером локально-глобального принципа, мы приведём его эквивалентную формулировку в терминах символа Гильберта.

Определение 7. Для пары ненулевых $a, b \in \mathbb{Q}_p$ определим *символ Гильберта*

$$(a,b)_p \overset{\text{def}}{=} \begin{cases} 1, & \text{если уравнение } x^2 - ay^2 - bz^2 = 0 \\ & \text{имеет \textit{нетривиальное} решение над полем } \mathbb{Q}_p, \\ -1 & \text{в противном случае.} \end{cases}$$

Аналогично доопределим символ Гильберта $(a,b)_\infty$, подразумевая под $\mathbb{Q}_\infty$ поле $\mathbb{R}$.

Символ Гильберта зависит лишь от классов a и b в факторгруппе $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ (т. е. не меняется при домножении на квадрат) и мультипликативен по обеим переменным.

Теперь сформулируем закон взаимности для символа Гильберта.

Теорема 3 (закон взаимности для символа Гильберта). *Пусть a, $b \in \mathbb{Q}^*$, тогда $(a,b)_p = 1$ для почти всех простых p, причём*

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} (a,b)_p = 1. \tag{8}$$

Оказывается, что для нечётных простых a и b эта формула *равносильна квадратичному закону взаимности*. Это может показаться несколько таинственным, но самом деле вполне естественно, так как для целого a, не делящегося на p, справедливо равенство

$$(a,p)_p = \left(\frac{a}{p}\right),$$

в чём можно убедиться при помощи леммы Гензеля. За подробностями мы снова отсылаем читателя к [Па08].

Закон взаимности Вейля, в свою очередь, является классическим примером локально-глобального принципа в алгебраической геометрии. Другим классическим примером из алгебраической геометрии, но аддитивным, является тождество

$$\sum_{p\in S} \operatorname{ord}_p f = 0,$$

где f — мероморфная функция на компактной римановой поверхности S.

Между законом взаимности Гильберта и законом взаимности Вейля есть вполне прозрачная связь, но она уже не столь элементарна. Состоит она в том, что как символ Гильберта, так и символ Вейля выражаются через *отображение взаимности Артина* (см. [Mil20, с. 114] и [Ser12]).

Формулу Востокова для символа Гильберта в расширениях с примитивным корнем степени p^n можно найти в части 3.21.4 книги [Iva]. Эта книга содержит современное введение в теорию полей классов и доступна упорным и вдумчивым младшекурсникам.

Список литературы

[Art24] *Artin E.* Quadratische Körper im Gebiete der höheren Kongruenzen. I. (Arithmetischer Teil.) // Math. Z. 1924. Bd. 19, № 1. P. 153–206.

[Ded57] *Dedekind R.* Abriss einer Theorie der höhern Congruenzen in Bezug auf einen reellen Primzahl-Modulus // J. Reine Angew. Math. 1857. Bd. 54. P. 1–26.

[GW86] *Gauss C. F.* Disquisitiones Arithmeticae. New York, NY: Springer, 1986.

[Iva] *Fesenko I.* Basic algebraic number theory. https://ivanfesenko.org/wp-content/uploads/Q/C1/partIn.pdf.

[KM24] *Kalinin N., Magin M.* Tropical Weil's reciprocity law and Weil's pairing. 2024. https://arxiv.org/abs/2408.06372.

[Mil20] *Milne J. S.* Class Field Theory. V4.03.2020. https://www.jmilne.org/math/CourseNotes/CFT.pdf.

[Mil22] *Milne J. S.* Fields and Galois Theory. V5.10.2022. https://www.jmilne.org/math/CourseNotes/FT.pdf.

[Pre91] *Previato E.* Another algebraic proof of Weil's reciprocity // Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. 1991. Vol. 2, № 2. P. 167–171.

[Ser12] *Serre J.-P.* Algebraic groups and class fields. New York, NY: Springer, 2012. (Graduate Texts in Mathematics; Vol. 117).

[Ар16] *Артин Э.* Теория Галуа. 3-е изд., стереотипное. М.: МЦНМО, 2016.

[Го13] *Горин Е. А.* Перестановки и квадратичный закон взаимности по Золотареву — Фробениусу — Руссо // Чебышевский сборник. 2013. Т. 14, вып. 4. С. 80–94.

[Ле65] *Ленг С.* Алгебра. М.: Наука, 1965.

[Ме] *Мерзон Г.* От результанта до взаимности // Математическое просвещение, Сер. 3. Вып. 35. М.: МЦНМО, 2025. С. **???–???**.

[Па08] *Панчишкин А. А.* Локальные и глобальные методы в арифметике // Математическое просвещение. Сер. 3. Вып. 12. С. 55–79. М.: МЦНМО, 2008.

[По63] *Постников М. М.* Теория Галуа. М.: Государственное издательство физико-математической литературы, 1963.

[Че34] *Чеботарев Н. Г.* Основы теории Галуа. Л.; М.: Государственное технико-теоретическое издательство, 1934.

Никита Сергеевич Калинин, Guangdong Technion Israel Institute of Technology (GTIIT),
Technion — Israel Institute of Technology

nikaanspb@gmail.com

Матвей Ильич Магин, СПбГУ

matheusz.magin@gmail.com