Алгебра и смежные области

Ещё одно доказательство из Книги: теорема Гаусса — Ванцеля

А. Б. Скопенков*

§ 1. Введение

Мы приводим самое простое[1)] (из известных) доказательство теоремы Гаусса — Ванцеля о построимости правильных многоугольников циркулем и линейкой (в нижеприведённой эквивалентной формулировке). Оно отлично от данного в [2, 6, 9] (в этих статьях, внешне столь непохожих, излагается одно и то же доказательство). Ещё одно доказательство см. в [7]. Приводимое доказательство принадлежит ещё Гауссу (см. детали и оговорки в [5, § 27]). Но, к сожалению, оно малоизвестно. См. подробнее замечания 1(b), 1(e).

На примере этого доказательства мы продемонстрируем некоторые важные идеи высшей алгебры (подводящие к теории Галуа, см. подробнее замечание 1(d)). При этом для понимания доказательства достаточно уметь извлекать корни из комплексных чисел и делить многочлены с остатком. Поэтому его разбор может использоваться для отработки тем «многочлены» и «комплексные числа».

Вещественное число называется *вещественно построимым*, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений квадратных корней

* Частично поддержан грантом фонда Саймонса-НМУ.

1) Это объясняет название заметки, ср. [1].

из положительных чисел. Иначе говоря, если некоторое множество, его содержащее, можно получить из множества $\{1\}$, используя лишь добавление к уже имеющемуся множеству $M \subset \mathbb{R}$, содержащему числа x, y,

чисел $x+y$, $x-y$, xy, числа x/y при $y \neq 0$ и числа $\sqrt{x}$ при $x > 0$.

Теорема (Гаусс — Ванцель). *Число* $\cos(2\pi/n)$ *вещественно построимо тогда и только тогда, когда* $n = 2^\alpha p_1 \cdot \ldots \cdot p_l$, *где* $p_1, \ldots, p_l$ — *различные простые числа вида* $2^{2^s}+1$.

Замечание 1. (a) Для практики приближённые методы вычисления тригонометрических функций полезнее формул с радикалами. Однако проблема построимости интересна как пробная задача современных теории символьных вычислений и теории сложности вычислений.

(b) Приводимое изложение намного проще и короче стандартного (ср. [8, 10]). Здесь я имею в виду доказательство «с нуля», а не вывод нужной теоремы из построенной перед этим теории, в которой фактически заключается всё доказательство.

Доказательство построимости элементарно, но основано на идее *резольвент Лагранжа* (см. элементарное изложение, например, в [12, п. 5.2.2]). Оно получено из [5, § 24] некоторым упрощением, см. подробнее замечание 3. См. [12, § 5.3].

Доказательство непостроимости похоже на стандартное доказательство, но в нём используется «степень многочлена» вместо «степени расширения поля». Оно похоже на [4, Supplement to § 35–37], [12, § 5.5.2].

Приводимое доказательство остаётся настолько малоизвестным, что ссылки на него отсутствуют в [2, 6, 9, 10]. (Это отчасти связано со сложностью его пути к читателю [12, конец п. 5.2.2].)

(c) Мы показываем в п. 2, *как можно догадаться* до формулировки теоремы. Хотя *придумать* доказательство непросто, *изложить* его можно коротко (см. п. 3 и 4).

(d) На примере этого доказательства продемонстрированы следующие идеи симметрии, воплощённые в понятии группы (в этой конкретной ситуации — группы автоморфизмов поля). Важно отображение сопряжения поля $F[\sqrt{a}]$, см. лемму 10 о сопряжении. Важна равноправность корней неприводимого многочлена (в этой конкретной ситуации — многочлена деления круга на простое число частей). Приведённые в скобках термины не используются далее в заметке.

(e) Другие ссылки и комментарии (в частности, на мотивировки и историю) приведены, например, в [12, § 5.1, § 5.2, § 27, § 28], [11, § 9.1].

Завершим это введение «комплексификацией» теоремы Гаусса — Ванцеля, используемой в её доказательстве.

Комплексное число называется (комплексно) *построимым*, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений квадратных корней. Иначе говоря, если некоторое множество, его содержащее, можно получить из множества $\{1\}$, используя лишь добавление к уже имеющемуся множеству $M \subset \mathbb{C}$, содержащему числа x, y,

$$\text{чисел } x+y,\ x-y,\ xy, \quad \text{числа } x/y \text{ при } y \neq 0$$
$$\text{и любого такого числа } r \in \mathbb{C}, \text{ что } r^2 = x.$$

Лемма 2 (о комплексификации). *Комплексное число построимо тогда и только тогда, когда его вещественная и мнимая части вещественно построимы.*

Набросок доказательства. Часть «тогда» очевидна. Для доказательства части «только тогда» запишите равенство $\sqrt{a+bi} = u+vi$ и выразите u, v через a и b с помощью четырёх арифметических операций и квадратных радикалов. □

Из этой леммы вытекает, что теорему Гаусса — Ванцеля достаточно доказать с заменой числа $\cos(2\pi/n)$ на число

$$\varepsilon_n := \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

и «вещественной построимости» на «построимость».

§ 2. Идея доказательства построимости в теореме Гаусса — Ванцеля

Этот параграф формально не используется в дальнейшем.

Идея доказательства построимости числа $\varepsilon := \varepsilon_5$. Во-первых,

$$T_0 := \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1.$$

Докажем построимость числа

$$T_2 := \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8.$$

При замене ε на ε^2 число T_2 переходит в $-T_2$. Значит, T_2^2 не меняется при этой замене. Поэтому T_2^2 не меняется при двукратной и трёхкратной такой замене, т. е. при заменах ε на ε^4 и ε на $\varepsilon^8 = \varepsilon^3$. Итак, для любого k число T_2^2 не меняется при замене ε на ε^k.

Раскроем скобки в произведении T_2^2 и заменим ε^5 на 1. Получим равенство

$$T_2^2 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{для некоторых } a_k \in \mathbb{Z}.$$

Так как для любого k число T_2^2 не меняется при замене ε на ε^k, мы получаем $a_1 = a_2 = a_3 = a_4$. Поэтому $T_2^2 = a_0 - a_1 \in \mathbb{Z}$. Значит, T_2 построимо.

Обозначим

$$T_1 := \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8 \quad \text{и} \quad T_3 := \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8.$$

Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать построимость чисел T_1 и T_3. Сделаем это для T_1; доказательство для T_3 аналогично.

При замене ε на ε^2 число T_1 переходит в $-iT_1$. Значит, T_1^4 при этой замене не меняется. Поэтому T_1^4 не меняется при двукратной и трёхкратной такой замене, т. е. при заменах ε на ε^4 и ε на $\varepsilon^8 = \varepsilon^3$. Итак, для любого k число T_1^4 не меняется при замене ε на ε^k.

Раскроем скобки в произведении T_1^4 и заменим ε^5 на 1. Получим равенство

$$T_1^4 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{для некоторых } a_k \in \mathbb{Z} + i\mathbb{Z}.$$

Так как для любого k число T_1^4 не меняется при замене ε на ε^k, мы получаем $a_1 = a_2 = a_3 = a_4$. Поэтому $T_1^4 = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$. Значит, T_1 построимо. □

Замечание 3. В этих рассуждениях нужно обосновать корректность «замены ε на ε^k» (т. е. что при другом представлении числа в виде многочлена от ε результат замены будет таким же.) Нужное представление единственно (даже для общего случая) [5, § 24, Lemma 2]. Отметим, что именно в отсутствии доказательства этой единственности заключается недочёт в рассуждениях Гаусса [5, § 24, § 27].

Доказательство единственности непросто [5, § 71]. Так что вместо этого мы немного изменим наше рассуждение. Именно этим приводимое доказательство проще данного в [5]. Вместо работы с *числами* мы будем работать с *многочленами* и подставлять в них ε в качестве аргумента.

Два многочлена с комплексными коэффициентами называются *сравнимыми по модулю многочлена* p, если их разность делится (в $\mathbb{C}[x]$) на p.

Задача. Обозначим $T_1(x) := x + ix^2 - x^4 - ix^8$. Тогда
(a) $iT_1(x^2) \equiv T_1(x) \bmod (x^5 - 1)$;
(b) $T_1^4(x^2) \equiv T_1^4(x) \bmod (x^5 - 1)$;
(c) $T_1^4(x^k) \equiv T_1^4(x) \bmod (x^5 - 1)$ для любого k.

Доказательство построимости числа $\varepsilon := \varepsilon_5$. Обозначим

$$T_1(x) := x + ix^2 - x^4 - ix^8.$$

Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышеприведённым. Как и выше,

$$(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon.$$

Поэтому достаточно доказать построимость каждого из чисел $T_r(\varepsilon)$, $r = 1, 2, 3$. Имеем

$$iT_1(x^2) \underset{x^5-1}{\equiv} T_1(x) \;\Rightarrow\; T_1^4(x^2) \underset{x^5-1}{\equiv} T_1^4(x) \;\Rightarrow\; T_1^4(x^k) \underset{x^5-1}{\equiv} T_1^4(x) \quad \text{для любого } k.$$

Возьмём многочлен $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ с коэффициентами в $\mathbb{Z} + i\mathbb{Z}$, сравнимый с $T_1^4(x)$ по модулю $x^5 - 1$.

Тогда $a_1 = a_2 = a_3 = a_4$. Поэтому $T_1^4(\varepsilon) = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$.

Значит, $T_1(\varepsilon)$ построимо. Аналогично $T_2(\varepsilon)$ и $T_3(\varepsilon)$ построимы. □

Задача. (a) Обозначим

$$\beta := \varepsilon_6 = \frac{1 + i\sqrt{3}}{2} \quad \text{и} \quad T(x) := x + \beta x^3 + \beta^2 x^9 + \beta^3 x^{27} + \beta^4 x^{81} + \beta^5 x^{243}.$$

Докажите, что $T(x) \equiv \beta T(x^3) \bmod (x^7 - 1)$.

(b) Докажите, что число ε_7 можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений комплексных корней второй или третьей степени из комплексных чисел.

Задача. (a) Обозначим

$$\beta := \varepsilon_{10} \quad \text{и} \quad T(x) := x + \beta x^2 + \beta^2 x^4 + \beta^3 x^8 + \beta^4 x^{16} + \ldots + \beta^9 x^{512}.$$

Докажите, что $T(x) \equiv \beta T(x^2) \bmod (x^{11} - 1)$.

(b) Докажите, что число ε_{11} можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений комплексных корней второй или пятой степени из комплексных чисел.

§ 3. Доказательство построимости в теореме Гаусса — Ванцеля

Лемма 4 (об умножении). (a) *Если ε_n построимо, то ε_{2n} построимо.*
(b) *Если ε_n и ε_m построимы и m, n взаимно просты, то ε_{mn} построимо.*

Доказательство получается из формул $\varepsilon_{2n} \in \sqrt{\varepsilon_n}$ и $\varepsilon_{mn} = \varepsilon_m^x \varepsilon_n^y$, где x и y — целые числа, для которых $nx + my = 1$. □

Доказательство построимости в теореме Гаусса — Ванцеля. По лемме 2 о комплексификации и по лемме 4 об умножении достаточно доказать, что $\varepsilon := \varepsilon_n$ построимо для любого простого $n = 2^{2^s} + 1$. Так как $(n-1)$ — степень двойки, по лемме 4 об умножении $\beta := \varepsilon_{n-1}$ построимо. Используем обозначение

$$\mathbb{Z}[\beta] := \{b_0 + b_1\beta + b_2\beta^2 + \ldots + b_{n-2}\beta^{n-2} \mid b_0, b_1, \ldots, b_{n-2} \in \mathbb{Z}\}.$$

Обозначим через g первообразный корень по модулю n (т. е. такое число g, для которого остатки от деления на n чисел $g^1, g^2, g^3, \dots, g^{n-1}$ различны.) Для $r = 0, 1, 2, \dots, n-2$ обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \dots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

Тогда $(T_0 + T_1 + \dots + T_{n-2})(\varepsilon) = (n-1)\varepsilon$. Кроме того, $T_0(\varepsilon) = -1$. Поэтому достаточно доказать построимость каждого из чисел $T_r(\varepsilon)$, $r = 1, 2, \dots, n-2$. Имеем

$$\beta^r T_r(x^g) \underset{x^n-1}{\equiv} T_r(x) \quad \Rightarrow \quad T_r^{n-1}(x^g) \underset{x^n-1}{\equiv} T_r^{n-1}(x) \quad \Rightarrow \quad T_r^{n-1}(x^k) \underset{x^n-1}{\equiv} T_r^{n-1}(x)$$

для любого k. Возьмём многочлен $a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1}$ с коэффициентами в $\mathbb{Z}[\beta]$, сравнимый с $T_r^{n-1}(x)$ по модулю $x^n - 1$. Тогда $a_1 = a_2 = \dots = a_{n-1}$. Поэтому $T_r^{n-1}(\varepsilon) = a_0 - a_1 \in \mathbb{Z}[\beta]$. Значит, $T_r(\varepsilon)$ построимо. □

§ 4. Доказательство непостроимости в теореме Гаусса — Ванцеля

Лемма 5 (признак Эйзенштейна). *Пусть p простое. Если для многочлена с целыми коэффициентами старший коэффициент не делится на p, остальные делятся на p, а свободный член не делится на p^2, то этот многочлен неприводим над $\mathbb{Z}$.*

Лемма 6 (Гаусс). *Если многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$.*

И признак Эйзенштейна, и лемма Гаусса доказываются переходом к многочленам с коэффициентами в $\mathbb{Z}_p$.

Лемма 7 (о степенях двойки). *Если неприводимый над $\mathbb{Q}$ многочлен P с рациональными коэффициентами имеет построимый корень, то* $\deg P$ *есть степень двойки.*

Доказательство приведено ниже.

Доказательство непостроимости в теореме Гаусса — Ванцеля. Так как $\varepsilon_n = \varepsilon_{nk}^k$, из построимости числа ε_{nk} вытекает построимость числа ε_n. Если число $2^m + 1$ простое, то m — степень двойки. Ввиду этих фактов и леммы 2 о комплексификации достаточно показать, что ε_n непостроимо для

(A) простого числа n, не представимого в виде $2^m + 1$;

(B) квадрата нечётного простого числа.

Непостроимость числа ε_n следует из леммы 7 о степенях двойки для корня ε_n многочлена

- $P(x) := x^{n-1} + x^{n-2} + \ldots + x + 1 = \dfrac{x^n - 1}{x - 1}$ в случае (A) и
- $P(x) := x^{p(p-1)} + x^{p(p-2)} + \ldots + x^p + 1 = \dfrac{x^{p^2} - 1}{x^p - 1}$ в случае (B), где $p = \sqrt{n}$.

Неприводимость этих многочленов над $\mathbb{Q}$ вытекает из их неприводимости над $\mathbb{Z}$ и леммы 6 Гаусса. Неприводимость этих многочленов $P(x)$ над $\mathbb{Z}$ вытекает из неприводимости многочленов $P(x+1)$ над $\mathbb{Z}$. Последняя неприводимость доказывается применением признака Эйзенштейна. Выполнение предположений признака Эйзенштейна для многочленов $P(x+1)$ проверяется с помощью сравнения $(x+1)^p \equiv x^p + 1 \bmod p$. □

Лемма 7 о степенях двойки вытекает из леммы 9 о башне расширений и леммы 10(b) о сопряжении (см. ниже).

Подмножество множества $\mathbb{C}$ называется *полем*, если оно замкнуто относительно операций сложения, умножения, вычитания и деления на ненулевое число.

Если $F \subset \mathbb{C}$, $r \in \mathbb{C}$ и $r^2 \in F$, то обозначим $F[r] := \{a + br : a, b \in F\}$.

Лемма 8. *Пусть $F \subset \mathbb{C}$ — поле, $r \in \mathbb{C}$ и $r^2 \in F$. Тогда $F[r]$ — поле.*

Доказательство. Нужно доказать, что $F[r]$ замкнуто относительно сложения, вычитания, умножения и деления на ненулевое число. Это не очевидно только в случае деления, который следует из равенства

$$\frac{1}{a+br} = \frac{a}{a^2 - b^2 r^2} - \frac{b}{a^2 - b^2 r^2} r. \qquad \square$$

Лемма 9 (о башне расширений). *Число $x \in \mathbb{C}$ построимо тогда и только тогда, когда существуют такие $r_1, \ldots r_{s-1} \in \mathbb{C}$, что*

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset \ldots \subset F_{s-1} \subset F_s \ni x,$$

где $r_k^2 \in F_k$, $r_k \notin F_k$ и $F_{k+1} = F_k[r_k]$ для любого $k = 1, \ldots, s-1$. □

Лемма 10 (о сопряжении). *Пусть $F \subset \mathbb{C}$ — поле, $r \in \mathbb{C}$, $r \notin F$ и $r^2 \in F$.*

(a) *Определим отображение сопряжения $\bar{\cdot} : F[r] \to F[r]$ формулой*

$$\overline{x + yr} := x - yr.$$

Это отображение корректно определено, $\overline{z + w} = \bar{z} + \bar{w}$ и $\overline{zw} = \bar{z} \cdot \bar{w}$.

(b) *Если многочлены $P \in F[x]$ и $Q \in F[r][x]$ имеют общий корень и неприводимы над F и над $F[r]$ соответственно, то* $\deg P \in \{\deg Q, 2 \deg Q\}$.

Доказательство части (a) оставляем читателю в качестве упражнения.

Доказательство части (b). По лемме 8 множество $F[r]$ — поле. Делимость, неприводимость и НОД рассматриваются в $F[r]$. Так как P и Q имеют общий корень и Q неприводим, мы получаем P делится на Q.

Тогда по п. (а) $P = \overline{P}$ делится на $\overline{Q}$. Так как Q неприводим и делится на $D := \gcd(Q, \overline{Q})$, мы получаем либо $D = Q$, либо $D = 1$.

Если $D = Q$, то из $\overline{D} = D$ получаем $Q = D \in F[x]$. Так как P неприводим над F, отсюда получаем $P = Q$.

Если $D = 1$, то P делится на $M := Q\overline{Q}$. Так как $\overline{M} = M$, получаем $M \in F[x]$. Так как P неприводим над F, получаем $P = M$. Значит, $\deg P = 2 \deg Q$. □

Благодарности

Благодарю А. Канунникова и В. Кириченко за полезные замечания.

Список литературы

[1] *Айгнер М.*, *Циглер Г.* Доказательства из Книги. Лучшие доказательства со времён Евклида до наших дней. М.: БИНОМ. Лаборатория знаний, 2017.

[2] *Бурда Ю.*, *Кадец Л.* Семнадцатиугольник и закон взаимности Гаусса // Математическое просвещение. Сер. 3. Вып. 17. М.: МЦНМО, 2013. С. 61–67.

[3] *Бурда Ю.*, *Кадец Л.*, *Скопенков А.* Письмо в редакцию // Математическое просвещение. Сер. 3. Вып. 18. М.: МЦНМО, 2014. С. 251–252.

[4] *Dörrie H.* 100 Great Problems of Elementary Mathematics: Their History and Solution. New York: Dover Publ, 1965.

[5] *Edwards H. M.* Galois Theory. Springer, 1984.

[6] *Канунников А. Л.* Как придумать построение правильного семнадцатиугольника // Математическое просвещение. Сер. 3. Вып. 26. М.: МЦНМО, 2020. С. 143–166.

[7] *Канунников А. Л.* Как придумать построение правильного семнадцатиугольника (продолжение) // Математическое просвещение. Сер. 3. Вып. 27. М.: МЦНМО, 2021. С. 142–149.

[8] *Кириченко В. А.* Построения циркулем и линейкой и теория Галуа. http://www.mccme.ru//dubna/2005/courses/kirichenko.html.

[9] *Козлов П. Ю.*, *Скопенков А. Б.* В поисках утраченной алгебры: в направлении Гаусса (подборка задач) // Математическое просвещение. Сер. 3. Вып. 12. М.: МЦНМО, 2008. С. 127–143. \http://arxiv.org/abs/0804.4357 (v1).

[10] *Салимгареев Р.* К теореме Гаусса — Ванцеля // Константиновский сборник Приложение к журналу «Математическое образование». Сер. «Образование: история, персоналии, проблемы». Вып. 1(02). Февраль 2019. С. 2–5.

[11] *Skopenkov A.* Mathematics via problems: from olympiads and math circles to a profession. Algebra. Providence: AMS. To appear.

[12] Элементы математики в задачах: через олимпиады и кружки к профессии / Ред. А. А. Заславский, А. Б. Скопенков, М. Б. Скопенков. М.: МЦНМО, 2018. http://www.mccme.ru/circles/oim/materials/sturm.pdf.

А. Б. Скопенков, МФТИ, НМУ

skopenko@mccme.ru, https://users.mccme.ru/skopenko