Московский физико-технический институт
Физтех-школа прикладной математики и информатики

ТЕОРИЯ КОЛЕЦ И ПОЛЕЙ

IV СЕМЕСТР

Лектор: *Ильинский Дмитрий Геннадьевич*

Автор: *Лизюра Дмитрий*
Проект на Github

весна 2024

Содержание

1 Кольца

1.1 Основные понятия

Определение. $(K, +, \cdot)$ называется *кольцом*, если $(K, +)$ является абелевой группой и выполняется дистрибутивность.

Определение. K называется *коммутативным кольцом*, если оно является кольцом с ассоциативностью и коммутативностью умножения и единицей.

Определение. Пусть $a, b \in K$. Говорят, что a *делится на* b, или же $b \mid a$, если найдётся $c \in K$, такой что $a = bc$.

Определение. $a \in K \setminus \{0\}$ называется *делителем нуля*, если найдётся $b \in K \setminus \{0\}$, такой что $bc = 0$.

Определение. Пусть K — кольцо. Будем обозначать через $K[x]$ кольцо многочленов с коэффициентами из K. Если же $K \subset L$ и $a \in L$, то $K[a]$ — это либо многочлены из $K[x]$, в которые подставили a, либо пересечение всех надколец K, содержащих a.

Определение. *Область целостности* — это коммутативное кольцо без делителей нуля.

Утверждение. Если K — область целостности, то из $ac = bc$ при $c \neq 0$ следует $a = b$. Очевидно.

Определение. K^* — это множество всех обратимых элементов K, то есть делителей единицы.

Утверждение. Пусть M_a — множество делителей элемента $a \in K$. Тогда $M_a = M_b \iff \exists c \in K^* : a = bc$. Очевидно.

Следствие. Группа K^* действует на множество K умножениями. Здесь орбиты называются *классами ассоциированности*, то есть $a \sim b$, если $\exists c \in K^* : a = bc$.

Утверждение. Ассоциированность является отношением эквивалентности, очевидно.

Определение. Элемент a кольца K называется *неразложимым*, если $a \neq 0$, $a \notin K^*$, и если мы смогли разложить a на множители $a = bc$, то $b \in K^*$ или $c \in K^*$.

Пример. Рассмотрим кольцо $\mathbb{Z}[i]$. Заметим, что оно представляет из себя числа вида $a+bi$ для $a, b \in \mathbb{Z}$. Тогда неразложимыми элементами являются ± 1, $\pm i$, а остальные — нет из-за того, что модуль больше единицы. Глобально, можно пользоваться понятием *нормы*, $N(a + bi) = a^2 + b^2$, но это позже.

Определение. Область целостности K называется *факториальным кольцом*, если:

1. Для любого $x \in K \setminus \{0\}$ существует разложение $x = u \cdot p_1 p_2 \dots p_s$, где $u \in K^*$ и $p_1, \dots, p_s$ неразложимы.

2. Если $x \neq 0$ удалось разложить двумя способами: $x = u \cdot p_1 \dots p_s = w \cdot q_1 \dots q_s$, то можно перенумеровать неразложимые так, что все $p_i \sim q_i$.

Пример. Второе свойство не всегда идёт вместе с первым: например, в кольце $\mathbb{Z}[2i]$ есть два разложения $4 = 2 \cdot 2 = (2i) \cdot (-2i)$. Элементы 2 и $2i$ не ассоциированы, так как мы не в кольце $\mathbb{Z}[i]$.

Пример. Первое тоже не всегда есть: например, кольцо корней многочленов из $\mathbb{Z}[x]$ со старшим коэффициентом, равным единице. Тогда $\sqrt{2} = \sqrt[4]{2} \cdot \sqrt[4]{2} = \sqrt[8]{2} \dots$

Утверждение. Поле является факториальным кольцом. Очевидно, так как все элементы неразложимы.

Определение. $\mathbb{Z}[i]$ называется кольцом *гауссовых чисел*, $\mathbb{Z}[\omega]$ называется *числами Эйзенштейна*, где ω — корень третьей степени из единицы. Обычно берут $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.

Как доказывается факториальность кольца? Во-первых, нужно доказать существования разложения, то есть ограничить глубину разложения, например, норма в $\mathbb{Z}[i]$. Во-вторых, единственность, но здесь обычно можно доказать следующее свойство: если $x \mid ab$ и x неразложим, то $x \mid a$ или $x \mid b$. Из него следует единственность разложения.

Определение. $x \in K$ называется *простым*, если $x \neq 0$, $x \notin K^*$, и если $x \mid ab$, то $x \mid a$ или $x \mid b$.

Утверждение. Простой элемент неразложим, очевидно.

Утверждение. В факториальном кольце любой неразложимый элемент прост, очевидно.

Теорема. Пусть K — область целостности. Если любой неразложимый элемент прост и выполнено условие (1) факториальности кольца, то оно факториально.

Доказательство. По индукции можно доказать, что если $x \mid a_1 \dots a_t$, то найдётся j, такое что $x \mid a_j$. Пусть у нас есть два разложения $y = u \cdot p_1 \dots p_s = w \cdot q_1 \dots q_l$. Будем делать то же, что и в натуральных числах. Сократим все ассоциированные, тогда все $p_i \not\sim q_j$. Получаем, что $q_1 \mid u \cdot p_1 \dots p_s$, теперь из неразложимости получаем, что один из сомножителей делится на q_1. Если $q_1 \mid u$, то по транзитивности делимости $q_1 \mid 1$, то есть $q_1 \in K^*$ — противоречие.

Иначе $q_1 \mid p_i$ для какого-то i. По определению найдётся $a \in K$, такое что $p_i = aq_1$, а из неразложимости $a \in K^*$ или $q_1 \in K^*$. Второе быть верно не может, а из первого следует, что $p_i \sim q_1$, но мы изначально сократили ассоциированные — противоречие.

□

1.2 Евклидовы кольца

Определение. Область целостности K называется *евклидовым кольцом*, если существует $N : K \setminus \{0\} \to \mathbb{Z}_{\geqslant 0}$, такая что:

1. $N(ab) \geqslant N(a)$.

2. Деление с остатком: для любых a, b найдутся частное q и остаток r, такие что $a = bq + r$, причём $r = 0$ или $N(r) < N(b)$.

Замечание. Может захотеться доопределить норму N в нуле, чтобы в делении с остатком не было двух случаев, но тогда придётся везде писать $a, b \neq 0$, и это, в целом, не всегда удобно (например, в кольце многочленов). Однако на практике в большинстве случаев норму можно сделать мультипликативной, и тогда с доопределением проблем не будет. Например, у многочленов можно ввести $N(f) = 2^{\deg(f)}$.

Пример. Докажем, что кольцо гауссовых чисел является евклидовым. Положим $N(a+bi) = a^2 + b^2$. Первое свойство следует из того, что норма вне нуля положительна. Разберёмся с делением с остатком: если $u = qv + r$, то $\frac{u}{v} = q + \frac{r}{v}$. Так как $\left|\frac{r}{v}\right| < 1$, достаточно найти $q \in \mathbb{Z}[i]$, которое будет близко к $\frac{u}{v}$. Это можно сделать геометрически: $\frac{u}{v}$ — это какая-то точка на плоскости, а нам нужна точка с целочисленными координатами, недалёкая от неё. Из соображений длины диагонали квадрата можно найти точку на расстоянии не более $\frac{\sqrt{2}}{2}$.

Утверждение. Если в области целостности K выполняется деление с остатком по норме N, то можно подкрутить норму так, чтобы выполнялось первое свойство.

Доказательство. Мы хотим сделать так, чтобы норма a не превосходила норму всего, что можно из него получить умножением. Так и определим:

$$\tilde{N}(a) = \min_{b \in K \setminus \{0\}} (N(ab)).$$

Проверим свойства. 1) Сравним $\tilde{N}(ab)$ и $\tilde{N}(a)$. Существует $c \in K \setminus \{0\}$, такое что $\tilde{N}(ab) = N(abc) \geqslant \min_{x \in K \setminus \{0\}}(N(ax)) = \tilde{N}(a)$.

2) Пусть $\tilde{N}(b) = N(bc)$. Разделим a на bc с остатком по норме N: существуют q и r, такие что $a = (bc)q + r$ и либо $r = 0$, либо $N(r) < N(bc)$. Первый случай очевиден, рассмотрим второй случай:

$$\tilde{N}(r) \leqslant N(r) < N(bc) = \tilde{N}(b).$$

Остаётся сказать, что cq — это частное и r — остаток (так можно делать в силу ассоциативности).

□

Теорема. Евклидово кольцо факториально.

Доказательство. Индукцией по норме. От противного: пусть $x \in K \setminus \{0\}$, и для него не существует разложения, причём среди всех таких x рассмотрим элемент с минимальной нормой. Пусть $x = ab$. Если $N(x) > N(a)$ и $N(x) > N(b)$, то по индукции a и b разложимы и x разложим, как произведение. Если $N(x) = N(a)$, то $N(ab) = N(a)$. Разделим a на ab с остатком (это единственный способ выбрать делимое и делитель так, чтобы было нетривиально). Тогда $a = ab \cdot q + r$. Если $r = 0$, то $bq = 1$ и $b \in K^*$. Иначе $N(r) < N(ab) = N(a)$. Но $r = a(1 - bq)$, так что по свойству 1 $N(r) \geqslant N(a)$ — противоречие. Следовательно, b обратим. Таким образом, либо x разложим, либо $b \in K^*$ и x неразложим по определению.

Теперь докажем, что разложение единственно. Для этого докажем лемму: если p неразложимо и $p \mid ab$, то $p \mid a$ или $p \mid b$. А для этого будем использовать обычновенный алгоритм Евклида: $r_1 = a$, $r_2 = b$, $r_n = q_{n+2} r_{n+1} + r_{n+2}$. Так как нормы уменьшаются, это рано или поздно закончится: пусть $r_{n+1} = 0$. Как и в натуральных числах $\exists x, y : r_n = ax + by$. Это доказывается индукцией по n. Теперь индукцией по n доказываем, что все НОДы r_k и r_{k+1} равны.

Обратно к лемме: пусть $p \mid ab$, но $p \nmid a$. Тогда $\gcd(a, p) = 1$ с точностью до ассоциированных. Как известно, все делители p — это ассоциированные с ним или обратимые. Тогда это же верно и для делителей $\gcd(a, p)$, то есть существуют x и y, такие что $ax + py = 1$. Остаётся домножить на b и получить $p \mid b$.

□

Замечание. r_n делится на любой общий делитель a и p. Доказывается рассмотрением разложения $r_n = ax + py$.

Пример. Рассмотрим $R = \mathbb{Z}[i]$. Как в нём искать неразложимые элементы, а для разложимых как искать это самое разложение? Возьмём обычную меру $N(a + bi) = a^2 + b^2$, тогда она мультипликативна. В этом случае $N(z) = 1 \iff z \in R^*$. Более того, если $N(z) = p$ — простое целое число (не элемент кольца), то z неразложимо (доказывается прямой проверкой). Есть ещё один случай неразложимых элементов: если $N(z) = p^2$ и нет элементов нормы p, то $z \sim p$ (ассоциированы) неразложим.

Интересный факт: все простые нормы вида $4k + 3$ дают неразложимые элементы.

1.3 Неразложимые элементы

Обозначение. D — одно из колец $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}i]$, $\mathbb{Z}[\omega]$, На них норма — $N(z) = z \cdot \overline{z}$: мультипликативна и $N(z) = 1 \iff z \in D^*$.

Теорема. (Об описании неразложимых элементов) В кольце D элемент z неразложим тогда и только тогда, когда выполнено одно из:

- $N(z) = p$, где p — простое целое число (не обязательно элемент кольца).
- $z \sim p$. В этом случае не существует элемента w, такого что $N(w) = p$.

В случае $D = \mathbb{Z}[i]$ числа p в двух случаях имеют вид (2 или $4k+1$) и $4k+3$ соответственно, в случае $\mathbb{Z}[\omega]$ — (3 или $3k+1$) и $3k+2$ соответственно.

Доказательство. $\Rightarrow$. Пусть z неразложим, тогда z прост. Норма $N(z)$ — это целое число, поэтому его можно разложить на простые множители: $N(z) = p_1 \cdots p_s$. Причём $z \mid N(z)$, поэтому какое-то p_j делится на z, то есть $p_j = xz$. В силу мультипликативности нормы $N(p_j) = N(x)N(z)$, то есть делится на $N(z)$. Следовательно, $p_j^2 = N(p_j)$ делится на $N(z)$, то есть $N(z) \in \{1, p_j, p_j^2\}$. В первом случае z обратим, это неинтересно. А два оставшихся случая как раз дают следствие теоремы.

Докажем несуществование w, такого что $N(w) = p$: пусть $N(z) = p_j^2$, то есть $z \sim p_j$. По условию z неразложим, поэтому и p_j неразложим. Допустим, что существует w, такой что $N(w) = p_j$. Так как $w \mid N(w)$, $p_j = N(w) = w \cdot u$. Применим N к обеим частям: $N(p_j) = N(w)N(u)$, подставляя, $p_j^2 = p_j \cdot N(u)$, то есть $N(u) = p_j$. Таким образом, $p_j = w \cdot u$, и $N(u) = N(w) = p_j$ — оба неразложимы, противоречие с неразложимостью p_j.

$\Leftarrow$. Пусть $z \in D$, и $N(z) = p$. Разложим на множители: $z = a \cdot b$, тогда $N(a) \cdot N(b) = N(z) = p$, то есть $N(a) = 1$ или $N(b) = 1$. Получается, что a или b обратим, то есть z неразложим.

Пусть $z \sim p$ и не существует w, таких что $N(w) = p$. Если $z = a \cdot b$, то $N(a)N(b) = N(z)$. По определению ассоциированности $z = dp$ для $d \in D^*$. То есть $N(z) = N(dp) = N(p) = p^2$. Это равно произведению $N(a)$ и $N(b)$, поэтому либо $N(a) = 1$, либо $N(b) = 1$ и z неразложим.

Теперь докажем часть про вид простых чисел в $\mathbb{Z}[i]$. Если $p = N(z) = a^2 + b^2$, то, так как $a^2, b^2 \equiv 0, 1 \mod 4$, сумма не может иметь вид $4k+3$. Пусть $p = 4k+1$, докажем, что существует разложение. Найдём символ Лежандра... $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$, то есть существует $x \in \mathbb{Z}$, такой что $x^2 + 1$ делится на p. Это значит, что $(x+i)(x-i)$ делится на p. Если бы p было неразложимо, то одна из скобок бы делилась на p. Заметим, что, глобально, если $p \mid (a + bi)$, то $p \mid a$ и $p \mid b$. Поэтому $p \mid \pm 1$ — противоречие.

Теперь для $\mathbb{Z}[\omega]$. Если $p = 3k+2$, то $(a+b)^2 \equiv a^2 - ab + b^2 \mod 3$ — получаем плохой остаток. Если $p = 3k+2$, то заметим, что $3 = \lambda\overline{\lambda}$, где $\lambda = 1 - \omega$. Найдём символ Лежандра:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = \left(\frac{1}{3}\right) = 1.$$

Следовательно, существует x, такое что $x^2 + 3$ делится на p, то есть $p \mid (x + \sqrt{i})(x - \sqrt{3}i)$. Аналогично предыдущему случаю доказываем от противного, здесь $p \mid \pm 2$, ибо $\sqrt{3}i = 2\omega + 1$.

∎

Следствие. (Рождественская теорема Ферма) Число n представимо в виде суммы двух квадратов тогда и только тогда, когда в разложении n на простые делители все простые числа вида $4k+3$ входят в чётных степенях.

Доказательство. Разделим n на все квадраты простых чисел, входящих в разложение, теперь n будет произведением $p_1 \cdots p_s$ различных простых чисел. Также будем доказывать через гауссовы числа.

$\Leftarrow$. Рассмотрим одно из простых чисел в разложении p. По доказанному p разложимо, причём $N(p) = p^2$, то есть оно представимо в виде произведения двух чисел $(a+bi)(a-bi)$ нормы p. Вот, собственно, и сумма — $(a+bi)(a-bi) = a^2+b^2$. Теперь для представления n в виде суммы двух квадратов воспользуемся тождеством

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad-bc)^2.$$

$\Rightarrow$. От противного: $n = a^2+b^2$, но следствие нарушается. Заметим, что a и b взаимно просты (иначе бы n делилось на квадрат). Пусть, без ограничения общности, $p_1 = 4k+3$. Так как $p_1 \mid n = a^2+b^2$, имеем $p_1 \mid N(a+bi)$. Если $p_1^2 \mid N(a+bi)$, то $p_1^2 \mid n$ и получим противоречие с первым шагом доказательства. Иначе разложим $a+bi$ на неразложимые: пусть $c+di$ — делитель, норма которого делится на p_1. По теореме об описании неразложимых $N(c+di) = p_1^2$ — противоречие.

□

Следствие 2. Алгоритм разложения на неразложимые в кольце $\mathbb{Z}[i]$. Рассмотрим $z \in \mathbb{Z}[i]$, пусть $N(z) = p_1 \cdots p_s$. Простые вида $4k+3$ неразложимы, их пропускаем. Простые вида $4k+1$ или 2 раскладываются дальше, например, $5 = (1+2i)(1-2i)$.

Фан факт. Положим $\mathcal{O}(d)$ — корни многочленов из $\mathbb{Z}[x]$ со старшим коэффициентом, равным 1, в $\mathbb{Q}[\sqrt{d}]$. Тогда при $d = -1, -2, -7, -11$ это Евклидовы кольца, а при $d = -19, -43, -67$ и ещё одном значении получаются не Евклидовы, но ОТА там работает. При остальных d ОТА работает только для идеалов.

1.4 Пифагоровы тройки

Научимся перечислять решения уравнения $x^2+y^2 = z^2$. Сразу будем считать, что x и y взаимно просты, и перейдём в гауссовы числа, тогда $(x+yi)(x-yi) = z^2$. Заметим, что $(x+yi, x-yi) = (2x, x+yi)$.

Пусть этот НОД равен d. Заметим, что если $d \mid x$, то $d \mid y$, поэтому в этом случае $d = 1$ с точностью до ассоциированности. Иначе пусть $d \nmid x$, тогда $N(d) > 1$. Более того, $N(d) \mid 4x^2$, откуда $N(d)$ чётно (если нечётно, то $d^2 \mid x^2$). Следовательно, d чётно. Но тогда получается, что $d \mid x+yi$, то есть $2 \mid x, y$ — противоречие со взаимной простотой.

Следовательно, остаётся лишь случай $d = 1$ (с точностью до ассоциированности). Так как $(x+yi)(x-yi) = z^2$, множители можно записать в виде $x+yi = a_1b_1^2$, $x-yi = a_2b_2^2$, где a_1, a_2 свободны от квадратов. Допустим, что $a_1 \notin \mathbb{Z}[i]^*$, тогда существует неразложимый $p \mid a_1$. Так как $z^2 = a_1a_2b_1^2b_2^2$, $p \mid \frac{z^2}{b_1^2b_2^2}$ — это полный квадрат, поэтому $p^2 \mid \frac{z^2}{b_1^2b_2^2} = a_1a_2$. По условию a_1 свободно от квадратов, откуда $p \mid a_2$. Следовательно, НОД чисел $x+yi$, $x-yi$ делится на p, то есть его норма больше единицы — противоречие.

Итак, $a_1, a_2 \in \mathbb{Z}[i]^*$, то есть равны ± 1 или $\pm i$. Распишем b_1 через целые числа: $b_1 = u+vi$. Тогда $x+yi = a_1(u^2-v^2+2uvi)$. Если $a_1 = \pm 1$, то получаем $x = \pm(u^2-v^2)$ и $y = \pm 2uv$, если же $a_1 = \pm i$, то наоборот. В обоих случаях $z = u^2+v^2$, и, как можно проверить подстановкой, все такие тройки подходят.

2 Идеалы

2.1 Кольца главных идеалов

Определение. Идеал I в коммутативном кольце K — это подмножество, такое что

1. $(I,+)$ — абелева группа.
2. $\forall a \in K\ \forall x \in I\ ax \in I$.

Утверждение. $I \subset K$ является идеалом тогда и только тогда, когда оно замкнуто относительно сложения и второе свойство.

Доказательство. $\Rightarrow$ очевидно. $\Leftarrow$. Проверим, что $0 \in I$: возьмём $a = 0$, $x \in I$, тогда их произведение $0 \in I$. Проверим, что обратный лежит: возьмём $a = -1$, $x \in I$, тогда $ax = -x \in I$.

$\square$

Определение. Пусть $x \in K$. Тогда *главный идеал* — это $(x) = \{ax \mid a \in K\}$.

Определение. Пусть $x_1, \ldots, x_n \in K$. Тогда $(x_1, \ldots, x_n) = \{a_1x_1 + \cdots + a_nx_n \mid a_1, \ldots, a_n \in K\}$ — *конечно порождённый идеал.*

Замечание. Не все идеалы являются главными: возьмём кольцо $\mathbb{Q}[x, y]$ и идеал (x, y).

Замечание 2. И не все идеалы конечно порождены: возьмём кольцо многочленов над $\mathbb{Q}$ со счётным числом переменных.

Определение. *Кольцо главных идеалов* — область целостности, в которой все идеалы главные.

2.2 Идеалы и делимость

Заметим, что (a) — это все элементы, которые делятся на a.

Свойства.

- $a \mid b \iff (a) \supset (b)$.
- Если $a \sim b$, то $(a) = (b)$, так как делятся друг на друга.
- $(a) + (b) = ((a, b))$ (это НОД).
- $(a) \cap (b) = ([a, b])$ (это НОК).

Цель параграфа — доказать, что кольца главных идеалов лежат между факториальными и евклидовыми кольцами. Для этого переформулируем определение евклидовых колец: K евклидово, если существует норма N, такая что работает деление с остатком: для $a, b \neq 0$ либо $b \mid a$, либо найдётся g, такой что $N(a - bg) < N(b)$. А теперь обобщим:

Определение. Область целостности K *обладает нормой Дедекине-Хассе*, если существует норма $N : K \setminus \{0\} :\to \mathbb{Z}_{\geqslant 0}$, такая что для любых $a, b \neq 0$: либо $b \mid a$, либо найдутся x, y, такие что $N(ax - by) < N(b)$. В частности, $ax - by \neq 0$, так как $N(ax - by)$ определена.

То есть коэффициент при a теперь не обязан быть единицей.

Теорема. K является кольцом главных идеалов тогда и только тогда, когда K обладает нормой Дедекине-Хассе.

Доказательство. $\Leftarrow$. Рассмотрим идеал $I \subset K$, а в нём — элемент с наименьшей нормой d. Теперь любой элемент либо делится на d, либо разделим с остатком и противоречие с выбором d. Следовательно, $I = (d)$. Доказательство в другую сторону будет позже.

$\square$

Теорема. Кольцо главных идеалов факториально.

Доказательство. Докажем существование разложения. От противного: здесь нужно аккуратно сформулировать, что это значит. Пусть у элемента a_0 нет разложения. Тогда при любом разложении $a_0 = b_1 \cdot c_1$ один из множителей можно бесконечно раскладывать, б.о.о a_1, а другой необратим, то есть $b_1 \notin K^*$. Повторяем для a_1: $a_1 = a_2 \cdot b_2$ и так далее, получаем цепочку $a_0, a_1, a_2, \ldots$. Тогда их идеалы вложены друг в друга: $(a_0) \subset (a_1) \subset (a_2) \subset \ldots$. Докажем, что эта цепочка стабилизируется: положим $I = \bigcup_{i=0}^{\infty}(a_i)$. Очевидно, что это идеал, а значит, $I = (c)$ для $c \in K$ (так как мы в кольце главных идеалов). Но тогда $c \in (a_N)$ для какого-то N, и $(a_N) = (a_{N+1}) = \ldots$. Следовательно, при $n \geqslant N$ мы брали обратимые b_n — противоречие.

Докажем единственность, а именно, лемму Евклида: если $p \mid ab$, где p неразложим и $p \nmid a$, то $p \mid b$ — неразложимый элемент прост. Положим $I = \{x \in K \mid p \mid ax\}$. Это идеал (прямой проверкой), причём $1 \notin I$ и $b, p \in I$, а ещё $I = (d)$, так как кольцо главных идеалов. d необратим, так как нет единицы, поэтому $d \mid p$, то есть $p \sim d$ и $I = (p)$. $b \in I$, поэтому $p \mid b$.

$\square$

Обратно к предыдущей теореме. Зная, что K факториально, возьмём с потолка норму и докажем, что подходит. Положим

$$N(x) = 2^{\text{количество простых в разложении } x \text{ с повторами}}.$$

Возьмём $a, b \neq 0$, такие что $b \nmid a$. Пусть $(a, b) = (d)$ (как идеалы). Тогда $d \mid a, b$, так как $a, b \in (d)$. Отсюда $N(b) \geqslant N(d)$. Более того, $b \neq d$, откуда неравенство строгое. Остаётся взять разложение $d = ax - by$ из того, что $d \in (a, b)$.

$\square$

Пример. Кольцо главных идеалов, не являющееся евклидовым:

$$\mathbb{Z}\left[-\frac{1}{2} + \frac{\sqrt{19}i}{2}\right].$$

Доказательство занимает около 40 минут и пропущено.

2.3 Факторкольца

Определение. Пусть K, L — кольца. Отображение $f : K \to L$ называется *гомоморфизмом*, если оно сохраняет операции и единицу.

Свойства.

- ▷ Если $I \subset K$ — идеал, то $f(I)$ не обязательно идеал в L. Пример: $K = \mathbb{Z}$, $L = \mathbb{Q}$, $f(x) = x$.
- ▷ Но $f(I)$ является идеалом в $f(K)$.
- ▷ Если $I \subset L$ — идеал, то $f^{-1}(I)$ — идеал в K.

Определение. Факторкольцо — K/I, всё, как обычно.

Теорема. (О гомоморфизмах) $K/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$.

Теорема. (О гомоморфизмах, 2) Если $I \subset J \subset K$, то $(K/I)/(J/I) \cong (K/J)$. Смысл её в том, что мы можем факторизовать по очереди. Например, для $\mathbb{Z}[x]/(5, x-2)$ можно сначала найти $\mathbb{Z}[x]/(5)$, потом по $(x-2)$, причём порядок не важен.

Пусть $I \subset K$, K — область целостности. Когда K/I является областью целостности? Когда для всех $a, b \in K$ верно, что если $[a] \cdot [b] = [0]$, то $[a] = [0]$ или $[b] = [0]$ (здесь $[x] = x + I$). То есть если $ab \in I$, то $a \in I$ или $b \in I$. Отсюда вытекает

Определение. Идеал I *простой*, если I нетривиальный и для всех $ab \in I$ верно $a \in I$ или $b \in I$.

Утверждение. Пусть I — нетривиальный идеал. Тогда K/I — область целостности тогда и только тогда, когда I простой. Доказательство двумя абзацами выше.

Утверждение. Число x простое тогда и только тогда, когда (x) простой.

Когда K/I является полем? Например,

Утверждение. Пусть F — коммутативное кольцо. Тогда F является полем тогда и только тогда, когда в F нет нетривиальных идеалов.

Доказательство. $\Rightarrow$. Пусть $I \subset F$. Либо $I = (0)$, что нас устраивает, либо $a \in I \setminus \{0\}$, тогда $1 = a \cdot a^{-1} \in I$ и $I = F$, что нас вновь устраивает.

$\Leftarrow$. Пусть $a \in F$, $a \neq 0$. Рассмотрим (a). $(a) = (0)$ быть не может, поэтому $(a) = F$. Следовательно, $a \mid 1$, то есть существует $b \in F$, такой что $ab = 1$ — обратим.

□

Утверждение. Пусть K — коммутативное кольцо. K/I — поле тогда и только тогда, когда в K нет нетривиальных идеалов, строго содержащих I. Следует из того, что можно установить биекцию между идеалами K/I и идеалами, содержащими I, — по доказанному в поле идеалов нет.

Определение. Идеал I *максимальный*, если нет идеала $I \subsetneq J \subsetneq K$.

Следствие. Любой максимальный идеал простой. Следует из того, что K/I — поле.

Утверждение. В кольце главных идеалов любой простой идеал максимальный.

Утверждение. В кольце главных идеалов все нетривиальные простые идеалы максимальны.

Доказательство. Если $I = (x)$ — простой идеал, то x простой, а значит, если $x \subset (y)$, то $y \mid x$. Тогда либо $x \sim y$, либо $(y) = K$, оба случая нам подходят.

□

Следствие. Если идеал I лежит в области целостности K, причём K/I — это область целостности, но не поле, то K не является кольцом главных идеалов и не евклидово. Пример — $\mathbb{Q}[x, y]/(y) \cong \mathbb{Q}[x]$, поэтому $\mathbb{Q}[x, y]$ — не кольцо главных идеалов.

Следствие 2. Пусть F — поле, $f(x)$ — неприводимый многочлен над F. Тогда $F[x]/f(x)$ — поле.

Доказательство. Так как $F[x]$ — кольцо главных идеалов, $f(x)$ является простым, откуда $(f(x))$ простой, максимальный, а значит, $F[x]/(f(x))$ — поле.

□

Теорема. (б/д, доказательство — на отл.(10)) Если K — факториальное кольцо, то K является кольцом главных идеалов тогда и только тогда, когда любой нетривиальный простой идеал максимален.

Следствие. Если для любого идеала $I \subset K$ верно, что K/I конечен, то K факториально тогда и только тогда, когда K — кольцо главных идеалов. Здесь мы пользуемся тем, что конечная область целостности является полем.

Оффтоп. Из теории групп мы знаем, что конечно порождённые абелевы группы можно разложить на $\mathbb{Z} \oplus \dots \oplus \mathbb{Z} \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\alpha_s}}$. Для колец есть похожая вещь: если K —

кольцо главных идеалов, то конечно порождённый модуль представим в виде $K \oplus \ldots K \oplus K/(p_1^{\alpha_1}) \oplus \ldots$. А теперь возьмём $K = \mathbb{C}[T]$, где T — линейный оператор над V. Тогда

$$V = \mathbb{C}[T]/(T-\lambda_1)^{m_1} \oplus \cdots \oplus \mathbb{C}[T]/(T-\lambda_s)^{m_s}$$

— жорданова нормальная форма.

2.4 Нётеровы кольца

Теорема. Пусть K — область целостности. Следующие условия эквивалентны:

1. Любой идеал конечно порождён.

2. Любая цепочка возрастающих идеалов стабилизируется.

3. Любая цепочка вида $(a_0) \subset (a_0, a_1) \subset (a_0, a_1, a_2) \subset \ldots$ стабилизируется.

Доказательство. $2 \Rightarrow 3$ очевидно.

$3 \Rightarrow 1$. Пусть $I \subset K$ — идеал. Возьмём $a_0 \in I$. Есть 2 варианта: либо $I = (a_0)$, либо есть $a_1 \in I \setminus (a_0)$. Повторяем — рано или поздно мы стабилизируемся.

$1 \Rightarrow 2$. Рассмотрим цепочку $I_0 \subset \cdots \subset I_n \subset \cdots$. Возьмём объединение всех идеалов $J = \bigcup_{j=0}^{\infty} I_j$ — легко проверить, что это идеал. Так как он конечно порождён, $J = (x_0, \ldots, x_n)$. Теперь возьмём первый идеал из цепочки, который содержит все порождающие элементы — дальше все будут совпадать.

$\square$

Определение. Такие кольца называются *нётеровыми*.

Утверждение. (б/д) Если K нётерово, то K/I нётерово.

Теорема. (Гильберта о базисе) Если K нётерово, то $K[x]$ нётерово.

Доказательство. Пусть $I \subset K[x]$, докажём его конечную порождённость, от противного. Возьмём многочлен с минимальной степенью f_0 из I, f_1 — из $I \setminus (f_0)$, и так далее. Обозначим за $d_0, d_1, \ldots$ степени взятых многочленов, a_i — их старшие коэффициенты.

Теперь возьмём идеалы на a_i, тогда по нётеровости кольца K получим, что $(a_0, a_1, \ldots) = (a_0, \ldots, a_N)$. В частности, мы можем выразить a_{N+1} через предыдущие: $a_{N+1} = a_0 b_0 + \cdots + a_N b_N$. Теперь уменьшим степень f_{N+1}, вычев из него

$$b_0 f_0 x^{d_{N+1}-d_0} + \cdots + b_N f_N x^{d_{N+1}-d_N}.$$

Мы получили многочлен g, лежащий в I, причём он не лежит в $(f_0, \ldots, f_N)$ (иначе там же лежит f_N). Следовательно, пришли к противоречию с минимальностью степени f_{N+1}.

$\square$

Доказательство в лоб. Пусть $I \subset K[x]$ — идеал. Положим J — множество старших коэффициентов многочленов в I — это, очевидно, идеал в K, так что его можно конечно породить $J = (a_1, \ldots, a_n)$. (J замкнут относительно сложения, так как два многочлена из I можно привести к одной степени, после чего сложить)

Пусть $f_1, \ldots, f_n \in K[x]$ — многочлены, старшие коэффициенты которых породили J. Зафиксируем $d := \max\{\deg(f_1), \ldots, \deg(f_n)\}$. Теперь положим J_k — множество старших коэффициентов многочленов в I, степень которых не превосходит k. Как и с J, это идеал, и можно взять многочлены $f_{k,1}, \ldots, f_{k,n_k} \in J_k$.

Пусть $I^* = \langle J \cup \{f_{k,i} \mid i \leqslant n_k, k \leqslant d\}\rangle$, он, очевидно, конечно порождён и вложен в I. Докажем, что $I \subset I^*$, от противного: допустим, что нашёлся $g \in I \setminus I^*$, возьмём с минимальной степенью. Дополнительно скажем, что a — старший коэффициент многочлена g.

Если $\deg(g) > d$, то $a \in J$, то есть $a = \sum_{i=1}^n \lambda_i a_i$. Рассмотрим многочлен $g - \sum_{i=1}^n \lambda_i x^{\deg(g)-\deg(f_i)} f_i$: он всё ещё не лежит в I^*, но его степень строго меньше — противоречие.

Иначе $a \in J_k$, где $k = \deg(g)$. Аналогично.

□

Минутка пафоса. Если у нас есть семейство многочленов $f_k(x_1, \ldots, x_n)$ на n переменных над $\mathbb{C}$, и мы рассмотрим систему

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ f_2(x_1, \ldots, x_n) = 0 \\ \vdots \end{cases},$$

то все эти многочлены образуют идеал в кольце $\mathbb{C}[x_1, \ldots, x_n]$. По теореме Гильберта о базисе можно выделить конечное число порождающих элементов (отсюда базис в названии), и исходная система эквивалентна новой конечной системе.

Теорема. (Ласкера-Нётер, б/д) Любой идеал в нётеровом кольце является конечным пересечением примарных идеалов. Примарный идеал — простой идеал в какой-то степени (умножение идеалов определено, степень получаем интуитивным образом).

Теорема. Если K факториально, то $K[x]$ факториально. Доказательство чуть позже.

Определение. Хотелось бы построить поле из кольца, чтобы строить разложения. Будем это делать аналогично рациональным числам. *Поле частных* — это

$$\mathrm{Quot}(K) = \{(a, b) \mid a \in K, b \in K \setminus \{0\}\}/\sim,$$

где $(a, b) \sim (b, c) \iff ad = bc$.

Лемма. Это отношение эквивалентности порождается заменами $(a, b) \to (xa, xb)$, где $x \neq 0$.

Теперь вводим операции очевидным образом (как на дробях) и доказываем, что получилось поле.

Итак, положим $F = \mathrm{Quot}(X)$, мы знаем, что K факториально, F — поле, $F[x]$ факториально, и теперь мы хотим что-то сказать про факториальность $K[x]$. Аналогия: $K = \mathbb{Z}$, $F = \mathbb{Q}$.

Утверждение. Если p — неразложимый элемент в K, то p — простой элемент в $K[x]$ (как многочлен степени 0).

Доказательство. Рассмотрим $K[x]/(p)$: оно изоморфно $K/(p)[x]$, поэтому оба кольца являются областями целостности. Следовательно, p прост в $K[x]$.

□

Определение. Пусть $f \in K[x]$. Его *носителем* называется $C(f) = gcd(a_n, \ldots, a_0)$ — НОД его коэффициентов.

Определение. Многочлен $f \in K[x]$ называется *примитивным*, если $C(f) \sim 1$.

Утверждение. Если $Af_1 \cdots f_k = Bg_1 \cdots g_l$, где f_i и g_i — примитивные над K и $A, B \in K$, то $f_1 \cdots f_k$ — примитивный многочлен и $A \sim B$. То есть многочлены можно сократить.

Доказательство. Докажем примитивность произведения: пусть $f_1 f_2$ не примитивен. Тогда $f_1 f_2$ делится на какой-то просто $p \in K$. Значит, один из них делится на p, что противоречит их исходной примитивности.

Теперь заметим, что $C(Af_1\cdots f_k)=A$ и $C(Bg_1\cdots g_l)=B$, откуда $A\sim B$.

$\square$

Обозначение. $f(x)$ — многочлен над $K[x]$, $\widehat{f}(x)$ — примитивная компонента f, $\widetilde{f}(x)$ — многочлен над $F[x]$, где $F=\mathrm{Quot}(K)$.

Тогда любой многочлен $\widetilde{f}$ можно написать в виде $\widetilde{f}(x)=\frac{A}{B}\widehat{f}(x)$.

Утверждение 2. Если $f(x)=\widetilde{g}(x)\cdot\widetilde{h}(x)$, то $\widehat{f}(x)\sim\widehat{g}(x)\cdot\widehat{h}(x)$ (доказывается прямой проверкой со свойством выше).

Теперь наконец-то можно перейти к доказательству факториальности $K[x]$. Нужно доказать две вещи: у любого элемента существует разложение и неразложимый элемент прост.

Пусть $f(x)\in K[x]$ неразложим. Если $\deg(f)=0$, то $f\in K$, откуда простота следует из простоты в K — факториальном кольце. Пусть $\deg(f)>0$, тогда $C(f)\sim 1$ (иначе есть очевидное разложение), то есть f примитивен.

Утверждение 3. Пусть $f(x)\in K[x]$, $\deg(f)>0$. Тогда $f(x)$ неприводим в $K[x]$ тогда и только тогда, когда $f(x)$ примитивен и неприводим в $F[x]$.

Доказательство. $\Rightarrow$. Примитивность доказали, докажем неприводимость. Допустим, что нашлось: пусть $f(x)=\overline{g}(x)\overline{h}(x)$. По утверждению 2 $\widehat{f}(x)\sim\widehat{g}(x)\widehat{h}(x)$. Следовательно, $\widehat{f}(x)$ приводим в $K[x]$ — противоречие.

$\Leftarrow$. Пусть $f(x)=g(x)h(x)$. Если $\deg(g),\deg(H)>0$, то $F[x]$ приводим в $F[x]$ — противоречие. Иначе одно из $g(x),h(x)$ обратимо, что следует из примитивности f.

$\square$

Утверждение 4. Если $\deg(f)>0$ и f неприводим в $K[x]$, то $f(x)$ прост.

Доказательство. $f(x)$ примитивен и неприводим: пусть $g(x)h(x)$ делится на $f(x)$ в $K[x]$. Без ограничения общности $g(x)=f(x)\widehat{q}(x)$ (разделили над $F[x]$). Тогда $\widehat{g}(x)\sim\widehat{f}(x)\widehat{q}(x)$, а значит, $g(x)=Af(x)\widehat{q}(x)$ и $f(x)\mid g(x)$.

$\square$

На этом моменте мы доказали всё необходимое для факториальности $K[x]$.

2.5 Признак неприводимости Эйзенштейна

Пусть $a_nx^n+\cdots+a_0=f(x)\in K[x]$, $I\subset K$ — простой идеал. Если $a_n\notin I$, $a_{n-1},\ldots,a_0\in I$ и $a_0\notin I^2$, то $f(x)$ неприводим в $\mathrm{Quot}(K[x])$.

Доказательство. Рассмотрим $K/I[x]$ — область целостности, так как I прост. Пусть $f(x)$ приводим, то есть $f(x)=g(x)h(x)$. Рассмотрим их над $K/I[x]$: получится $[a_n]x^n=[b_k]x^k[c_l]x^l$ — слева все остальные члены исчезли, так как они по условию лежат в идеале. Отсюда следует, что $[b_0]=[c_0]=[0]$, так как в равенстве они исчезли, поэтому $a_0=b_0\cdot c_0\in I^2$ — противоречие.

$\square$

Другой признак. Пусть $f(x)\in\mathbb{Z}[x]$, $[f](x)\in\mathbb{Z}/(p)[x]$. Если $[f](x)$ неприводим и $p\nmid a_n$, то $f(x)$ неприводим.

Другой признак. Пусть $f(x)\in K[x]$, I — максимальный идеал, $a_n\notin I$. Тогда если $[f](x)$ неприводим в $K/I[x]$, то $f(x)$ неприводим в $\mathrm{Quot}(K)[x]$.

Доказательство. Пусть $f(x)=g(x)h(x)$, тогда $[f](x)=[g](x)\cdot[h](x)$, откуда $[a_n]=[b_m]\cdot[c_l]$, где b_m и c_l — старшие коэффициенты. Тогда $[b_m]\cdot[c_l]\notin 0$, то есть нашли разложение в $K/I[x]$.

$\square$

Упражнение. Придумать многочлен из $\mathbb{Z}[x]$ со старшим коэффициентом 1, такой что $f(x)$ неприводим, а $f(x) \mod p$ приводим для всех p.

Напоминание. Пусть F — поле. Если $\deg(f) = 1$, то f неприводим. Если $\deg(f) = 2$ или 3, то $f(x)$ неприводим тогда и только тогда, когда у $f(x)$ нет корней.

Утверждение. (Из школы) Если $a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ и $\frac{p}{q}$ — корень, где $(p, q) = 1$, то $q \mid a_n$ и $p \mid a_0$.

Утверждение. Пусть p — простое целое число. Тогда $x^{p-1} + \cdots + x + 1$ неприводим над $\mathbb{Q}$.

Доказательство. Многочлен равен $\frac{x^p-1}{x-1}$, поэтому хочется сделать замену $t = x - 1$. Тогда это равно

$$(t+1)^{p-1} + \cdots + (t+1) + 1 = \frac{(t+1)^p - 1}{t}.$$

Можно заметить, что это будет

$$t^{p-1} + C_p^1 t^{p-2} + \cdots + C_p^{p-1}.$$

По признаку Эйзенштейна многочлен неприводим, идеал — (p).

□

3 Расширение полей

Вопросы этого параграфа: разрешимость в радикалах, основная теорема алгебры и замечательная

Теорема. Правильный m-угольник можно построить цикрулем и линейкой тогда и только тогда, когда $\varphi(m) = 2^k$.

Напоминание. Характеристика поля — ноль или простое число. При гомоморфизме $\varphi : F \to L$ выполнено $\mathrm{char}(F) = \mathrm{char}(L)$. Любой гомоморфизм — это вложение, ибо ядро либо равно нулю, либо всему полю.

Утверждение. Пусть $F \subset L$ — расширение поля. Тогда L — линейное пространство над F.

Определение. $[L : F]$ — *степень расширения*, то есть размерность L, как линейного пространства.

Утверждение. Пусть $F \subset L \subset K$ — "башня расширений". Тогда $[K : F] = [K : L] \cdot [L : F]$ (при условии, что всё конечно).

Определение. Расширение *конечно*, если $[L : F] < \infty$, иначе *бесконечно*.

Определение. $F(\alpha)$ — поле с элементом $\alpha \in L \setminus F$. Можно определять двумя способами:

- $\mathrm{Quot}(F[\alpha])$.
- Пересечение всех полей K, таких что $F \subset K \subset L$ и $\alpha \in K$.

Расширения $F \subset L$ глобально делятся на конечные и бесконечные. Первые можно записать в виде $L = F(\alpha_1, \ldots, \alpha_k)$.

Определение. Алгебраический элемент $\alpha \in L$ — такой элемент, что $[F(\alpha) : F] < \infty$ или, эквивалентно, найдётся многочлен $f \in F[x]$, такой что $f(\alpha) = 0$.

Определение. Минимальный многочлен $m_{\alpha,F}(x)$ — многочлен, корнем которого является α, и одно из эквивалентных:

- ▷ Его степень минимальна.
- ▷ Он неприводим.
- ▷ $(m_{\alpha,F})$ совпадает с идеалом $\{g(x) \mid g(\alpha) = 0\}$.

Утверждение. $F[\alpha] \cong F(\alpha) \cong F[x]/(m_{\alpha,F}(x))$.

3.1 Поле разложения многочлена

Определение. L — поле разложения многочлена $f(x)$, если:

- ▷ $f(x)$ линейно факторизуем над L.
- ▷ L минимально по включению.

Утверждение. Для поля F и $f(x) \in F[x]$ поле разложения L многочлена f существует и $[L : F] \leqslant (\deg(f(x)))!$.

Примеры. Все над $\mathbb{Q}$:

- ▷ $x - 1$, $L = \mathbb{Q}$, степень — 1.
- ▷ $x^2 - 2$, $L = \mathbb{Q}(\sqrt{2})$, степень — 2.
- ▷ $x^3 - 2$, $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)$, степень — 6.
- ▷ $(x - 1)(x - 2)(x - 3)$, $L = \mathbb{Q}$, степень — 1.

Доказательство. Индукцией по $\deg(f(x))$. Разложим f на неприводимые: $f(x) = g_1(x) \cdot \ldots \cdot g_s(x)$. Положим $L_0 = F$, $L_1 = F[x]/(g_1(x))$. По утверждению с предыдущей лекции в L_1 есть корень α_1 многочлена $g_1(x)$. Тогда $f(x) = (x-\alpha_1)h_1(x)$ над L_1. Применим предположение индукции к h_1 и L_1, откуда $[L : L_0] = [L : L_1] \cdot [L_1 : L_0] \leqslant n \cdot (n - 1)! = n!$. □

Теорема. (б/д) Поле разложения единственно с точностью до изоморфизма.

Рассуждения. Пусть F — конечное поле, $\mathrm{char}(F) = p$, $[F : \mathbb{Z}_p] = m$. Тогда $|F| = p^m$, $|F^*| = p^m - 1$, откуда для всех $a \in F^*$ выполнено $a^{p^m-1} = 1$, то есть a является корнем многочлена $x^{p^m-1} - 1$, а значит, все $a \in F$ являются корнями многочлена $x^{p^m} - x$, то есть F является полем разложения многочлена $x^{p^m} - x$ над $\mathbb{Z}_p$. По утверждению выше такое поле единственно с точностью до изоморфизма.

3.2 Алгебраически замкнутые поля

Определение. Алгебраическое расширение поля F — расширение, в котором все элементы алгебраические относительно F.

Определение. Поле F называется *алгебраически замкнутым*, если выполнено одно из следующих эквивалентных условий:

1. Любой многочлен имеет корень.
2. Любой многочлен линейно факторизуем.
3. Любое конечное расширение F тривиально.

4. Любое алгебраическое расширение F тривиально.
5. Поле разложения любого многочлена совпадает с F.
6. (На лекции не было, но было в листочке) Все неприводимые над F многочлены имеют степень 1.

Корректность. $1 \Rightarrow 2$. Очевидно.

$2 \Rightarrow 4$. Пусть $L \supset F$ — алгебраическое расширение, $\alpha \in L$. Тогда $m_{\alpha,F}(x)$ неприводим, откуда его степень равна единице, то есть $\alpha \in F$.

$4 \Rightarrow 3$. Любое конечное расширение является алгебраическим.

$3 \Rightarrow 5$. Поле разложения конечно по утверждению выше, тривиально по условию.

$5 \Rightarrow 1$. Рассмотрим многочлен, полем его разложения является F, откуда все его корни лежат в F.

$1 \iff 6$. Очевидно.

□

Определение. Пусть F — поле. Тогда $\overline{F}$ — это *алгебраическое замыкание* F, то есть алгебраическое расширение, которое алгебраически замкнуто.

Утверждение. (И корректность) Пусть $F \subset L \subset K$ — башня алгебраических разложений, то есть $F \subset L$ и $L \subset K$ алгебраические. Тогда расширение $F \subset L$ алгебраическое.

Доказательство. Пусть $\alpha \in K$. Из алгебраичности существуют $\beta_0, \ldots, \beta_m \in L$, такие что $\beta_0 + \cdots + \beta_m\alpha^m = 0$, причём по условию они все алгебраические. Теперь мы хотим заменить L на поля с конечным расширением. А именно, $F \subset F(\beta_0, \ldots, \beta_m) \subset F(\beta_0, \ldots, \beta_m)(\alpha)$ — башня конечных расширений. Значит, α лежит в конечном расширении F, то есть в алгебраическом.

□

3.3 Построение алгебраического замыкания для счётного поля

Если F не более, чем счётно, то можно перечислить все неприводимые многочлены $f_1, f_2, \ldots$ и строим цепочку $F = F_0 \subset F_1 \subset \ldots$, где F_N — поле разложения f_N над F_{N-1}. Тогда $\overline{F} = \bigcup_{k=0}^{\infty} F_k$. То, что это является полем, очевидно, алгебраичность следует из того, что каждое промежуточное расширение конечно, то есть алгебраично, теперь по утверждению каждое из полей алгебраично относительно F.

Для более чем счётных полей делается то же самое, но там начинается аксиома выбора.

Другой вариант: можно рассмотреть алгебраически замкнутое $K \supset F$, тогда $\overline{F} = \{\alpha \in L \mid \alpha \text{ — алгебраическое над } F\}$. Корректность: пусть $\alpha, \beta \in \overline{F}$, тогда $\alpha, \beta \in K$, а значит, $F(\alpha, \beta) \supset F$ — конечное расширение. Значит, это расширение алгебраическое, и $\alpha + \beta, \alpha \cdot \beta, \alpha^{-1} \in \overline{F}$. Алгебраичность аналогично доказательству выше.

Теорема. (б/д) $\overline{F}$ единственно с точностью до изоморфизма.

3.4 Построение алгебраического замыкания в общем случае

Пусть M — множество многочленов положительной степени над F. Введём для каждого $f \in M$ формальную переменную x_f. Пусть $I \subset F[x_f]$ — идеал, порождённый всеми многочленами вида $f(x_f)$. Заметим, что I нетривиален, так как в нём не может быть единицы, ибо у всех многочленов положительная степень. Расширим его до максимального идеала, тогда $F[x_f]/I$ будет полем.

Рассмотрим $f \in M$ над полем $F[x_f]/I$. Заметим, что у него есть корень $\overline{x_f}$, ибо $f(x_f) \in I$. Следовательно, все многочлены из $F[x]$ имеют корень над этим полем. Положим $F_1 = F[x_f]/I$, F_2 — сделаем то же самое, но над F, и так далее. Получается цепочка $F_1 \subset F_2 \subset \ldots$, пусть K — её объединение.

Тогда над K любой многочлен имеет корень (пусть мы его добавили на i-ом шаге, тогда на $(i+1)$-ом шаге мы добавили его корень) и $F \subset K$, откуда, по определению, $K = \overline{F}$.

3.5 Теорема о примитивном элементе

Если $\mathrm{char}(F) = 0$ и $F \subset L$ конечно, то существует $\alpha \in L$, такое что $L = F(\alpha)$.

Доказательство. Понятно, что $L = F(\alpha_1, \ldots, \alpha_s)$. По индукции достаточно доказать, что $F(\alpha, \beta) = F(\gamma)$. Будем искать γ в виде $\alpha + c \cdot \beta$. Так как $F(\gamma) \subset F(\alpha, \beta)$, достаточно доказать обратное включение. А именно, хочется сделать так, чтобы $\beta \in F(\gamma)$. Во-первых, β — корень $m_{\beta,F}(x)$. Во-вторых, β — корень $m_{\alpha,F}(\gamma - cx) \in F(\gamma)[x]$.

Теперь мы хотим доказать, что НОД многочленов $m_{\beta,F}(x)$ и $m_{\alpha,F}(\gamma - cx))$ имеет степень 1, то есть β — их единственный общий корень. Пусть $\beta_1, \ldots, \beta_N$ $(\beta_1 = \beta)$ — корни $m_{\beta,F}(x)$ и $\alpha_1, \ldots, \alpha_s$ $(\alpha_1 = \alpha)$ — корни $m_{\alpha,F}(x)$. Сейчас мы рассматриваем многочлены над $\overline{F}$, так что это все возможные корни. Рассмотрим какой-то корень β_j многочлена $m_{\alpha,F}(\gamma - cx)$. Допустим, что нашёлся ещё один общий корень $\gamma - c\beta_j = \alpha_k$. Тогда

$$\gamma = \alpha_k + c\beta_j = \alpha + c\beta \Rightarrow c = \frac{\alpha_k - \alpha}{\beta - \beta_j}.$$

Можно взять c так, чтобы это равенство не случилось, ибо мы выкинули конечное число элементов (в определении β_i и α_j элемент c не фигурировал). Следовательно, β — единственный общий корень, однако есть проблема: кратные корни в $m_{\beta,F}(x)$ (если они есть, то произойдёт деление на ноль). Но в этом случае можно взять НОД с производной (тогда не единица) и получить противоречие с неприводимостью.

Таким образом, кратных корней нет и единственный общий корень — это β, то есть НОД многочленов лежит в $F(\gamma)[x]$ и равен $x - \beta$. Отсюда $\beta \in F(\gamma)$.

□

3.6 Построение цикрулем и линейкой

Что значит "построить точку цикрулем и линейкой"? Изначально нам даны точки 0 и 1 в $\mathbb{C}$. Теперь, если у нас есть точки p и q, мы можем совершать следующие действия:

- ▷ Провести между ними прямую.
- ▷ Провести окружность с центром в p, проходящую через q.
- ▷ Отметить пересечение двух окружностей или прямых.

Будем обозначать через $M_{\mathbb{C}}$ множество построимых точек. Также положим $M_{\mathbb{R}} = M_{\mathbb{C}} \cap \mathbb{R}$.

Примеры.

- ▷ Можно построить медиану точек.
- ▷ Можно найти перпендикуляр из точки на прямую.

▷ А оттуда и параллельные прямые.

Следствие. Так как мы можем строить перпендикуляры на оси, то есть проекции, $M_{\mathbb{C}} = \{a + bi \mid a, b \in M_{\mathbb{R}}\}$.

Утверждение. $M_{\mathbb{R}}$ замкнуто относительно сложения, вычитания, умножения, деления и взятия квадратного корня.

Доказательство. Упражнение. Например, разность: даны a и b, можно окружностью и прямой построить $-b$, после этого найти их медиану ($\frac{a-b}{2}$) и удвоить.

□

Следствие. $M_{\mathbb{R}}$ — поле, а $M_{\mathbb{C}} = M_{\mathbb{R}}(i)$.

Теорема. (Критерий принадлежности $M_{\mathbb{R}}$) Пусть $\delta \in \mathbb{R}$. Тогда $\delta \in M_{\mathbb{R}}$ тогда и только тогда, когда найдутся $\delta_1, \ldots, \delta_n \in \mathbb{R}$, такие что для всех k выполняется $[\mathbb{Q}(\delta_1, \ldots, \delta_k) : \mathbb{Q}(\delta_1, \ldots, \delta_{k-1})] = 2$ и $\delta \in \mathbb{Q}(\delta_1, \ldots, \delta_n)$.

Доказательство. $\Leftarrow$. Очевидно, так как при каждом расширении мы получаем корни квадратных многочленов, а брать корень мы умеем.

$\Rightarrow$. Пусть мы на k-ом шаге строили точку (x_1, y_1). Будем строить поля $F_k = \mathbb{Q}(x_1, y_1, x_2, \ldots, x_k, y_k)$. Тогда для всех k выполнено $[F_{k+1} : F_k] \in \{1, 2\}$. Докажем разбором случаев.

▷ $p_{k+1} = (x_{k+1}, y_{k+1})$ появилась, как пересечение двух прямых. Тогда она выражается через точки на этих двух прямых с коэффициентами из поля, так что поле не изменилось.

▷ p_{k+1} является пересечением окружности и прямой, то есть, без ограничения общности,

$$\begin{cases} y_{k+1} = ax_{k+1} + b \\ x_{k+1}^2 + y_{k+1}^2 + cx_{k+1} + dy_{k+1} + e = 0 \end{cases}$$

В этом случае координаты находятся решением квадратного уравнения, откуда F_{k+1} можно получить добавлением в поле корня из дискриминанта.

▷ Получилось пересечением окружностей, аналогично, или можно свести к предыдущему случаю радиальной осью.

□

Следствие. (Критерий принадлежности $M_{\mathbb{C}}$) $z \in M_{\mathbb{C}}$ тогда и только тогда, когда найдутся $z_1, \ldots, z_n$, такие что для всех k выполнено $[\mathbb{Q}(z_1, \ldots, z_{k+1}) : \mathbb{Q}(z_1, \ldots, z_k)] = 2$ и $z \in \mathbb{Q}(z_1, \ldots, z_k)$.

Следствие. Если $z \in M_{\mathbb{C}}$, то $[\mathbb{Q}(z) : \mathbb{Q}] = 2^k$ для $k \in \mathbb{N}$. Иными словами, мы умеем строить только очень специфичные алгебраические числа. В частности, $\sqrt{\pi} \notin M_{\mathbb{C}}$, так что квадратура круга не построима. Также $\sqrt[3]{2} \notin M_{\mathbb{C}}$, так что удвоение куба не построить. Можно попытаться построить правильные n-угольники, это эквивалентно построению корней n-ой степени из единицы. Например, восемнадцатиугольник не построим, так как $x^9 + 1$ — один из многочленов, обнуляющих ξ_{18}, его можно разложить в $(x^3 + 1)(x^6 - x^3 + 1)$, и второй многочлен неприводим, ибо можно сдвинуть на единицу и применить признак Эйзенштейна. В частности, если n простое, то степень минимального многочлена ξ_n равна $n - 1$, откуда

Следствие. Если правильный p-угольник построим, то $p = 2^k + 1$.

Определение. Многочлен деления круга — это

$$\Phi_n(x) = \prod_{\substack{1\leqslant m\leqslant n\\(m,n)=1}} (x - \xi_n^m),$$

где ξ_n — примитивный корень n-ой степени из единицы.

Утверждение. (Доказательство позже) Коэффициенты Φ_n целые, и он неприводим над $\mathbb{Q}$.

Следствие. Если правильный n-угольник построим, до $\varphi(n) = 2^k$.

Итог. Мораль в том, что построение циркулем и линейкой — это расширение поля $\mathbb{Q}$ корнями квадратных многочленов.

3.7 Автоморфизмы расширений

Определение. Пусть $K \subset F$ — поле. *Группа автоморфизмов расширения* $K \subset F$ — это

$$\mathrm{Aut}_K(F) = \{\psi \in \mathrm{Aut}(F) \mid \varphi|_K = id\},$$

то есть автоморфизмы, которые не двигают подполе.

Пример. $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))$. Заметим, что если ψ подходит, то $\psi(a+b\sqrt{2}) = \psi(a)+\psi(b\sqrt{2}) = a + b \cdot \psi(\sqrt{2})$. Куда может переходить $\sqrt{2}$? Заметим, что $\sqrt{2}$ является корнем $x^2 - 2$, а значит, если применить к многочлену ψ, то $\psi(\sqrt{2})$ будет корнем $x^2 - \psi(2) = 0$, то есть $\psi(\sqrt{2}) = \pm\sqrt{2}$.

Определение. Пусть $K \subset F$ — расширение, $a, b \in \overline{K}$. Тогда a и b называются *сопряжёнными*, если их минимальные многочлены над K совпадают.

Утверждение. (О мощности $\mathrm{Aut}_F(F(\gamma))$) Пусть γ — алгебраический элемент над F. Тогда $|\mathrm{Aut}_F(F(\gamma))|$ равно количеству сопряжённых к γ элементов из $F(\gamma)$, где $\alpha \sim \beta$ сопряжены над F, если $m_{\alpha,F} = m_{\beta,F} \iff m_{\alpha,F}(\beta) = 0$.

Доказательство. Будем строить биекцию. Пусть $\varphi \in \mathrm{Aut}_F(F(\gamma))$, тогда $m_{\gamma,F}(\varphi(\gamma)) = \varphi(m_{\gamma,F}(\gamma)) = \varphi(0) = 0$, то есть $\varphi(\gamma) \sim \gamma$.

Обрано, пусть $\gamma \sim \gamma'$, тогда $m_\gamma = m_{\gamma'}$, то есть $F(\gamma) \cong F[x]/(m_\gamma) \cong F[x]/(m_{\gamma'}) \cong F(\gamma')$. □

Следствие. $|\mathrm{Aut}_F(F(\gamma))| \leqslant \deg(m_{\gamma,F})$.

Пример 2. $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = \{id\}$. Следует напрямую из утверждения.

3.8 Сепарабельные расширения

Пусть $f(x) \in K[x]$ и f неприводим над K. Разложим его над алгебраическим замыканием: $f(x) = \prod_{i=1}^n (x - x_i)$. Верно ли, что все x_i различны? Это будет верно тогда и только тогда, когда $\mathrm{char}(K) = 0$ или $\mathrm{char}(K) = p$ и можно брать корень p-ой степени, то есть отображение $a \mapsto a^p$ сюръективно.

Определение. Расширение $K \supset F$ называется *сепарабельным*, если для любого $\alpha \in K$ многочлен $m_{\alpha,F}$ не имеет кратных корней.

Замечание. Не сепарабельные расширения встреачаются крайне редко, ибо нам нужно бесконечное поле с конечной характеристикой. Пример: $\mathbb{Z}_p(x)$, добавим туда корень многочлена $x^p - a$ для $a \in \mathbb{Z}_p$, то есть $\sqrt[p]{x}$. Тогда $x^p - a = (x - \sqrt[p]{a})^p$.

3.9 Расширения Галуа

Теорема. Пусть $F \subset K$ — конечное расширение и ($\operatorname{char}(F) = 0$ или K конечное). Иными словами, выполнена теорема о примитивном элементе. Следующие условия эквивалентны:

1. K — поле разложения некоторого $f(x) \in F[x]$.
2. Если $\gamma \in K$, то все сопряжённые с γ над F элементы лежат в K.
3. $|\operatorname{Aut}_F(K)| = [K : F]$.
4. $K^{\operatorname{Aut}_F(K)} = F$ (множество неподвижных точек при действии $\operatorname{Aut}_F(K)$).

Первые два условия называются *нормальным расширением*, а последние два — *расширением Галуа*, то есть нормальное и сепарабельное.

Доказательство. $2 \Rightarrow 3$. Имеем $K = F(\gamma)$ по теореме о примитивном элементе, тогда $|\operatorname{Aut}_F(F(\gamma))|$ равно количеству сопряжённых к γ в $F(\gamma)$ по утверждению о мощности, а по условию это равно $\deg(m_\gamma)$, что в точности равно $[F(\gamma) : F]$.

$3 \Rightarrow 4$. Пусть $K^{\operatorname{Aut}_F(K)} = L \supset F$, тогда $\operatorname{Aut}_F(K) = \operatorname{Aut}_L(K)$ по построению L. Теперь по условию $[K : F] = |\operatorname{Aut}_F(K)|$, далее $|\operatorname{Aut}_F(K)| = |\operatorname{Aut}_L(K)| \leqslant [K : L]$, так как по утверждению о мощности $|\operatorname{Aut}_L(K)| \leqslant \deg(m_{\gamma,L}) = [K : L]$, где $K = L(\gamma)$. Наконец, $[K : L] \leqslant [K : F]$, поэтому все неравенства обращаются в равенства.

$4 \Rightarrow 2$. Пусть $\gamma \sim \gamma'$, тогда $\gamma' \in K$. Рассмотрим

$$f(x) = \prod_{g \in \operatorname{Aut}_F(K)} (x - g(\gamma)).$$

Утверждается, что $f(x) \in F[x]$. Действительно, если мы подействуем на $f(x)$ любым автоморфизмом $h \in \operatorname{Aut}_F(K)$, то многочлен не изменится, откуда по условию $f(x) \in F[x]$. Более того, один из автоморфизмов в произведении из определения f — тождественный, что даёт $f(\gamma) = 0$. Следовательно, f делится на $m_\gamma(x)$. Теперь все корни m_γ являются корнями $f(x)$, а они лежат в K (потому что область значений всех $g \in \operatorname{Aut}_F(K)$ совпадает с K). Следовательно, если $\gamma' \sim \gamma$, то он является корнем m_γ и лежит в K.

$2 \Rightarrow 1$. $m_{\gamma,F}$ линейно факторизуем над $K = F(\gamma)$, ибо все корни там лежат, а минимальность очевидна.

$1 \Rightarrow 2$. Зафиксируем $f(x) \in F[x]$. Пусть $\gamma \in K$ и $\tilde{\gamma} \in \overline{F}$ сопряжено. У нас есть изоморфизм $\varphi : F(\gamma) \to F(\tilde{\gamma})$, сохраняющий F и переводящий γ в $\tilde{\gamma}$ (задача с семинара). Мы хотим построить гомоморфизм $\psi : K \to \overline{F}$, продолжающий φ.

Утверждение. (О продолжении гомоморфизма) Пусть F — поле, $L \supset F$ — конечное расширение, $\varphi : L \to \overline{F}$ — гомоморфизм, сохраняющий F, и α — алгебраический над L. Если β — корень $\varphi(m_{\alpha,L})$, то существует единственный гомоморфизм $\tilde{\varphi} : L(\alpha) \to \overline{F}$, такой что $\tilde{\varphi}|_L = \varphi$ и $\tilde{\varphi}(\alpha) = \beta$.

Пример. Рассмотрим башню $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}\omega) \subset \overline{\mathbb{Q}}$. Гомоморфизм $\varphi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}\omega)$ можно продолжить до $\mathbb{Q}(\sqrt[3]{2}, \omega) \to \mathbb{Q}(\sqrt[3]{2}, \omega)$.

Доказательство. Положим $\tilde{L} = \varphi(L)$, тогда $\varphi : L \to \tilde{L}$ — изоморфизм. Тогда $\varphi : L[x] \to \tilde{L}[x]$ — изоморфизм, так что $L(\alpha) \cong L[x]/(m_{\gamma,L}) \cong \tilde{L}[x]/(\varphi(m_{\alpha,L})) \cong \tilde{L}(\beta)$.

$\square$

Возьмём продолжение изоморфизма $\tilde{\varphi} : K \to \overline{F}$, оно существует по утверждению и теореме о примитивном элементе. Пусть $f(x) = (x - \gamma)(x - \gamma_1) \ldots (x - \gamma_s)$, по условию

$\gamma, \gamma_1, \ldots \gamma_s \in K$. Заметим, что $f(x) = \tilde{\varphi}(f(x)) = (x - \gamma')(x - \tilde{\varphi}(\gamma_1)) \ldots (x - \tilde{\varphi}(\gamma_s))$. Следовательно, $\gamma', \tilde{\varphi}(\gamma_1), \ldots, \tilde{\varphi}(\gamma_s) \in K$, и, в частности, $\gamma' \in K$.

$\square$

Лемма. (О собственной подгруппе группы Галуа) Если $K \supset F$ — расширение Галуа и $H \subsetneq \mathrm{Aut}_F(K)$, то $K^H \neq F$.

Доказательство. От противного: $K^H = F$. По теореме о примитивном элементе $K = F(\gamma)$, теперь рассмотрим $f(x) = \prod_{h \in H}(x - h(\gamma))$. Теперь, как и в ($4 \Rightarrow 2$) основной теоремы Галуа, $f(x) \in K^H[x] = F[x]$. Так как $f(\gamma) = 0$, $\deg(f(x)) \geqslant \deg(m_\gamma)$. Наконец, $|H| = \deg(f(x))$, а $|\mathrm{Aut}_F(K)| = |\mathrm{Aut}_F(F(\gamma))| \leqslant \deg(m_\gamma)$ по лемме о мощности $\mathrm{Aut}_F(F(\gamma))$. Собирая неравенства вместе, получаем $|H| \geqslant |\mathrm{Aut}_F(K)|$ — противоречие с $H \neq \mathrm{Aut}_K(F)$.

$\square$

Лемма. (О башне нормальных расширений) Пусть $K \supset L \supset F$ — башня расширений, причём $K \supset F$ нормальное. Тогда $K \supset L$ тоже нормальное.

Доказательство. Действительно, по первому условию K является полем разложения некоторого $f(x) \in F[x] \subset L[x]$.

$\square$

Теорема. (Основная теорема теории Галуа) Пусть $K \supset F$ — расширение Галуа. Тогда существует биекция между конечными расширениями и группой Галуа $\mathrm{Aut}_F(K)$, а именно, подгруппе $H \subset \mathrm{Aut}_F(K)$ сопоставляется расширение $F \subset K^H$, и расширению $F \subset L$ сопоставляется подгруппа $\mathrm{Aut}_L(K)$. Причём $H \triangleleft \mathrm{Aut}_F(K)$ тогда и только тогда, когда $L \supset F$ нормальное (где H и L сопоставлены биекцией). Более того, если $L \mapsto H$, то $|H| = [K : L]$ и $[\mathrm{Aut}_F(K) : H] = [L : F]$.

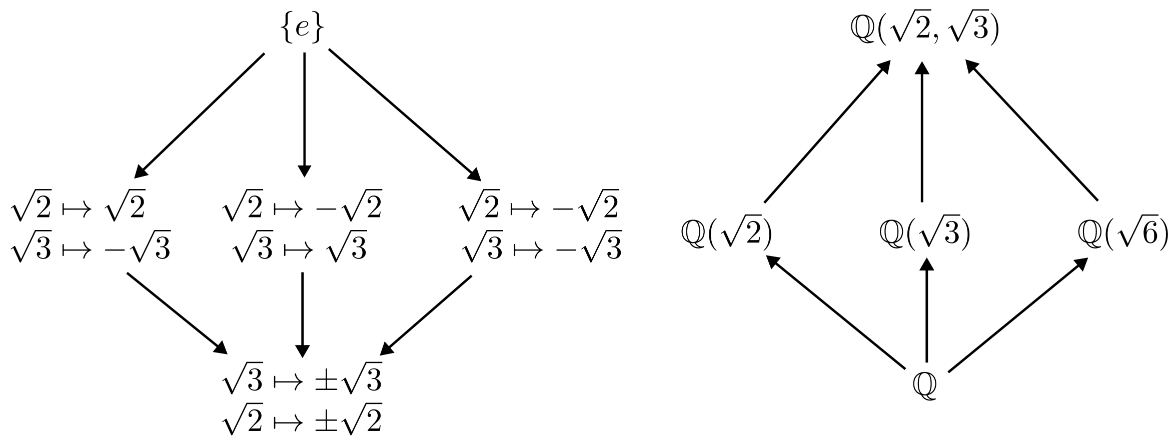

Рис. 1: Пример биекции из основной теоремы Галуа

Доказательство. Мы хотим доказать три вещи. Первая, если $F \subset L$ — конечное расширение, то $K^{\mathrm{Aut}_L(K)} = L$. Вторая, если $H \subset \mathrm{Aut}_F(K)$, то $\mathrm{Aut}_{K^H}(K) = H$. Третья, про нормальность.

Первое совсем очевидно: по лемме о башне нормальных расширений $L \subset K$ является расширением Галуа, после чего четвёртое условие даёт искомое.

Второе: заметим, что $K^H = K^{\mathrm{Aut}_{K^H}(K)}$ и $H \subset \mathrm{Aut}_{K^H}(K)$. По лемме о башне нормальных расширений $K^H \subset K$ является расширением Галуа, откуда по контрапозиции с леммой о собственной подгруппе Галуа $H = \mathrm{Aut}_{K^H}(K)$.

Третье: проверим, что $K^{gHg^{-1}} = g \circ K^H$. Это просто факт из теории групп, и он проверяется в лоб:

$$K^{gHg^{-1}} = \{x \in K \mid \forall h \in H \; ghg^{-1}(x) = x\} =$$

$$= \{x \in K \mid \forall h \in H\ hg^{-1}(x) = g^{-1}(x)\} =$$
$$= \{x \in K \mid g^{-1}(x) \in K^H\} = \{x \in K \mid x \in g \circ K^H\} = g \circ K^H.$$

Теперь заметим, что нормальность K^H над F это то же самое, что для всех $g \in \mathrm{Aut}_F(K)$ выполняется $g \circ K^H = K^H$ (доказано ниже). Последнее эквивалентно тому, что для всех $g \in \mathrm{Aut}_F(K)$ выполнено $K^{gHg^{-1}} = K^H$. По первым двум пунктам у нас уже есть биекция, так что это эквивалентно тому, что $gHg^{-1} = H$, а это уже нормальность H в $\mathrm{Aut}_F(K)$.

Обратно к утверждению: $F \subset K^H$ нормальное тогда и только тогда, когда для всех $g \in \mathrm{Aut}_F(K)$ выполнено $g \circ K^H = K^H$.

$\Rightarrow$: рассмотрим $\gamma \in K^H$, по нормальности все сопряжённые тоже лежат в K^H. Пусть $g \in \mathrm{Aut}_F(K)$, тогда $g(m_\gamma(x)) = m_\gamma(x)$. Раскладывая m_γ на множители, получаем, что γ переходит в сопряжённый ему, то есть $g(\gamma) \in K^H$.

$\Leftarrow$: пусть $\gamma \sim \gamma'$, тогда найдётся изоморфизм $g : F(\gamma) \to F(\gamma')$, такой что $g(\gamma) = \gamma'$. По теореме о продолжении гомоморфизма его можно продолжить до K, а значит, $g \circ K^H = K^H$. Следовательно, $g(\gamma) \in K^H$.

$\square$

Замечание. До этого мы говорили, что башни расширений хорошие: башня конечных конечная, башня алгебраических алгебраическая. Однако если в башне $K \supset L \supset F$ расширения $K \supset L$ и $L \supset F$ нормальные, то $K \supset F$ не обязательно нормальное, здесь критерием является то, что $\mathrm{Aut}_L(K) \triangleleft \mathrm{Aut}_F(K)$.

Пример: $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$. Каждый этаж расширения нормальный, так как степень равна единице. Но всё расширение — нет, так как вместе с $\sqrt[4]{2}$ нужны ещё сопряжённые $\pm\sqrt[4]{2}i$.

3.10 Следствия из основной теоремы Галуа

Определение. Пусть $f(x) \in F[x]$. $\mathrm{Gal}_F(f) = \mathrm{Aut}_F(K)$ — это группа Галуа поля разложения K многочлена $f(x)$.

Факт из теории групп. Если $|G| = 2^k$, то найдётся цепочка $G = G_0 \supset G_1 \supset \dots \supset G_k = \{e\}$, такая что все $[G_i : G_{i+1}] = 2$. Для доказательства берётся центр группы, фактор по нему и индукция.

Теорема. (Основная теорема алгебры) $\mathbb{C}$ алгебраически замкнуто.

Доказательство. Пусть $L \supset \mathbb{R}$, $[L : \mathbb{R}] = 2k+1$ — конечное расширение нечётной степени. По теореме о примитивном элементе $L = \mathbb{R}(\gamma)$, откуда $\deg(m_\gamma) = 2k+1$. Как известно, многочлен нечётной степени над $\mathbb{R}$ всегда имеет корень, откуда $\deg(m_\gamma) = 1$, то есть $L = \mathbb{R}$ (здесь просто какая-нибудь непрерывность).

Второй известный факт: если $L \supset \mathbb{C}$, такое что $[L : \mathbb{C}] \leqslant 2$, то $L = \mathbb{C}$.

Теперь пусть $K \supset \mathbb{C}$ — какое-то конечное расширение, продолжим его до нормального над $\mathbb{R}$ (если $K = \mathbb{R}(\gamma)$, то возьмём K — поле разложения m_γ над $\mathbb{R}$). Пусть $|\mathrm{Gal}_\mathbb{R}(K)| = 2^k \cdot M$, где M нечётно. По теоремам Силова найдётся силовская подгруппа $H \subset \mathrm{Gal}_\mathbb{R}(K)$, такая что $|H| = 2^k$. Пусть ей соответствует расширение $K \supset L \supset \mathbb{R}$, тогда $[L : \mathbb{R}] = M$. По первому факту $M = 1$. Следовательно, $|\mathrm{Aut}_\mathbb{R}(K)| = 2^k$ и $|\mathrm{Aut}_\mathbb{C}(K)| = 2^{k-1}$.

Если $k = 1$, то победа, иначе рассмотрим подгруппу $\tilde{H} \subset \mathrm{Aut}_\mathbb{C}(K)$ индекса 2, то есть $|\tilde{H}| = 2^{k-2}$. Пусть ей сопоставлено расширение $K \supset L \supset \mathbb{C}$. По основной теореме Галуа $[L : \mathbb{C}] = [\mathrm{Aut}_\mathbb{C}(K) : \tilde{H}] = 2$, откуда по второму известному факту $L = \mathbb{C}$, то есть $\tilde{H} = \mathrm{Aut}_\mathbb{C}(K)$ — противоречие.

Следовательно, $K = \mathbb{C}$, что эквивалентно алгебраической замкнутости.

□

Утверждение. α построимо циркулем и линейкой тогда и только тогда, когда $|\operatorname{Gal}(m_\alpha)| = 2^k$.

Доказательство. $\Leftarrow$. По факту из теории групп найдётся цепочка $\operatorname{Gal}(m_\gamma) = G_0 \supset G_1 \supset \dots \supset G_n = \{e\}$. По основной теореме Галуа им можно сопоставить цепочку $K = K_n \supset \dots \supset K_0 = \mathbb{Q}$. Теперь все $[K_i : K_{i-1}] = [G_i : G_{i-1}] = 2$, что эквивалентно построимости.

$\Rightarrow$. Остаётся в качестве вопроса на отл.(10).

□

Пример. Для примитивного корня n-ой степени из единицы ξ_n всё довольно просто, ибо $\mathbb{Q}(\xi_n)$ является полем разложения m_{ξ_n}, то есть $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = |\operatorname{Gal}(\xi_n)|$. Засим правильный n-угольник построим $\iff$ ξ_n построим $\iff$ $\deg(m_{\xi_n}) = 2^k$ $\iff$ $\varphi(n) = 2^k$. Откуда взялось φ?

Теорема. $\deg(m_{\xi_n}) = \varphi(n)$.

Доказательство. Для начала вспомним, как выглядит m_{ξ_n}, а именно, выпишем первые несколько многочленов: $x - 1$, $x + 1$, $x^2 + x + 1$, $x^2 + 1$, $x^4 + x^3 + x^2 + x + 1$, $x^2 - x + 1$. Может показаться, что коэффициенты всегда равны ± 1, но уже для $m_{\xi_{105}}$ это неверно.

Положим $\Phi(x) = \prod_{(k,n)=1}(x - \varphi_n^k)$. Сначала докажем, что $\Phi(x) \in \mathbb{Z}[x]$, по индукции. Заметим, что $x^n - 1 = \Phi(x) \cdot \prod_{d|n, d\neq n} m_{\xi_d}(x)$, доказано.

Если α — корень $m_{\xi_n}(x)$, то α^p тоже является его корнем для всех простых p, таких что $(p, n) = 1$. От противного: $x^n - 1 = m_{\xi_n}(x) \cdot g(x)$, такие что α является корнем $m_{\xi_n}(x)$, а α^p является корнем $g(x)$. Тогда α является корнем $g(x^p)$, а отсюда $g(x^p) = m_{\xi_n}(x) \cdot h(x)$. Беря по модулю p, получаем $(\overline{x})^n - 1 = \overline{m}_{\xi_n}(x) \cdot \overline{g}(x)$. Но $\overline{g}(x^p) = (\overline{g}(x))^p = \overline{m}_{\xi_n}(x) \cdot \overline{h}(x)$. Отсюда получается, что $m_{\xi_n}(x) \mid (\overline{g}(x))^p$, то есть у $\overline{m}_{\xi_n}(x)$ и $\overline{g}(x)$ есть общий корень. Так как $(\overline{x})^n - 1$ делится на их произведение, у него есть кратный корень — противоречие, ибо их нет.

Наконец, если α — корень $m_{\xi_n}(x)$, то α^k является корнем $m_{\xi_n}(x)$ для k, взаимно простого с n. Пусть $k = p_1 \dots p_s$, тогда α, α^{p_1}, $\dots$, $\alpha_{p_1 \dots p_s} = \alpha_k$ являются корнями.

Отсюда получаем, что $\deg(m_{\xi_n}) \geqslant \varphi(n)$. Итак, $\Phi(x)$ — это неприводимый многочлен степени $\varphi(n)$ (доказательство не случилось), корнем которого является ξ_n. Следовательно, он является минимальным.

□

Утверждение. Если $\deg(f(x)) = n$, то $\operatorname{Gal}(f) \subset S_n$. То есть любой автоморфизм переставляет корни местами.

Утверждение. Если $f(x)$ неприводим, то $\operatorname{Gal}(f) \subset S_n$ транзитивна, то есть для любых i, j найдётся $\sigma \in \operatorname{Gal}(f)$, такая что $\sigma(i) = j$. Очевидно, так как мы можем любой корень перевести в любой другой и продолжить изоморфизм до K.

4 Симметрические многочлены

Пусть K — область целостности. Рассмотрим многочлены в $K[x_1, \dots, x_n]$, которые сохраняются при перестановке переменных, они называются *симметрическими*. Иными словами, для любой $\sigma \in S_n$ выполнено $f(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$.

Определение. Элементарные симметрические многочлены:

$$\sigma_1 = x_1 + \dots + x_n$$

$$\sigma_2 = x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n$$

$$\vdots$$

$$\sigma_k = \sum_{\{i_1,\dots,i_k\}\subset\{1,\dots,n\}} x_{i_1}\cdot\ldots\cdot x_{i_k}.$$

Теорема. (Множество неподвижных точек относительно действия группой S_n — это) $K[x_1,\dots,x_n]^{S_n} = K[\sigma_1,\dots,\sigma_n]$. Иными словами, любой симметрический многочлен единственным образом представляется в виде многочлена от $\sigma_1,\dots,\sigma_n$. Например, $x_1^2+\dots+x_n^2 = \sigma_1^2 - 2\sigma_2$ и $(x_1-x_2)^2 = \sigma_1^2 - 4\sigma_2$. Доказательство позже.

Введём лексикографический порядок на мономах:

$$x_1^{a_1}\dots x_n^{a_n} \geqslant x_1^{b_1}\dots x_n^{b_n} \iff (a_1,\dots,a_n) \geqslant_{lex} (b_1,\dots,b_n).$$

Будем называть *старшим мономом* наибольший в таком порядке моном.

Лемма. (О старшем мономе) Если f симметрический, то старший моном имеет вид $x_1^{a_1}\dots x_n^{a_n}$, где $a_1\geqslant\ldots\geqslant a_n$.

Доказательство. От противного, пусть он имеет такой же вид, но найдутся $a_i<a_j$ для $i<j$. Применяя к многочлену транспозицию (i,j), получаем его же, но теперь старший моном стал строго больше — противоречие.

□

Лемма 1. Для любых $a_1\geqslant\ldots\geqslant a_n$ найдётся многочлен $g(x_1,\dots,x_n)$, такой что старший моном $g(\sigma_1,\dots,\sigma_n)$ равен $x_1^{a_1}\dots x_n^{a_n}$.

Доказательство. Явно построим g. Старший моном должен получаться из произведения вида $(x_1+\dots+x_n)^{b_1}(x_1x_2+\dots)^{b_2}\dots(x_1\dots x_n)^{b_n}$. Теперь заметим, что по лемме о старшем мономе из этого произведения старший моном получается взятием как можно большей степени x_1, потом x_2 и так далее. Как максимизировать степень при x_1? Выбрать из всех скобок слагаемое с x_1. Теперь x_2: первая скобка уже зафиксирована, но в остальных можно выбрать слагаемое с x_2, и так далее. Получается

$$x_1^{b_1+\dots+b_n}x_2^{b_2+\dots+b_n}\dots x_n^{b_n}.$$

Коэффициенты $b_1,\dots,b_n$ восстанавливаются однозначно.

□

Доказательство теоремы. Индукцией по старшему моному. База: если $f=0$, то $g=0$.

Переход: пусть старший моном f имеет вид $A\cdot x_1^{a_1}\dots x_n^{a_n}$. По лемме 1 подбираем многочлен g с таким старшим мономом и вычитаем его. Старший моном станет строго меньше, дальше по предположению индукции.

Докажем единственность от противного: пусть $g_1(\sigma_1,\dots,\sigma_n)=g_2(\sigma_1,\dots,\sigma_n)$, рассмотрим их разность $h(\sigma_1,\dots,\sigma_n)$ — сей многочлен не является тождественным нулём, но если раскрыть определения $\sigma_1,\dots,\sigma_n$, то тождественный ноль всё-таки получится. Найдём среди мононов многочлена h моном вида $\sigma_1^{b_1},\dots,\sigma_n^{b_n}$, у которого $b_1+\dots+b_n$ максимально, среди таких — у которого $b_2+\dots+b_n$ максимально, и так далее. Раскрывая скобки, мы получим, среди прочего, моном $B\cdot x_1^{b_1+\dots+b_n}x_2^{b_2+\dots+b_n}\dots x_n^{b_n}$. Если бы он с чем-то сократился, то получится противоречие с тем, как мы взяли $\sigma_1^{b_1}\dots\sigma_n^{b_n}$.

□

Замечание. Может показаться плохим, что в переходе индукции у нас может быть бесконечно много многочленов с меньшим старшим мономом. Однако в силу фундированности множества старших мононов это не проблема.

4.1 Решение уравнений второй степени

Только в случае, когда у нас поле F и $\mathrm{char}(F) \neq 2, 3$. Пусть у нас есть уравнение $x^2 + ax + b = 0$. Тогда у него имеется два корня α_1, α_2. Мы знаем, что $\alpha_1 + \alpha_2 = -a \in F$ и $\alpha_1\alpha_2 = b \in F$. Рассмотрим дискриминант $(\alpha_1 - \alpha_2)^2 = a^2 - 4b \in F$.

Если $\alpha_1 - \alpha_2 \in F$, то и $\alpha_1\alpha_2 \in F$, так что оба корня лежат в F и легко находятся. В противном случае корни лежат в расширении $F(\sqrt{D})$, и здесь группа Галуа изоморфна S_2.

4.2 Решение уравнений третьей степени

Пусть у нас есть уравнение $x^3 + ax + b = 0$ и $\alpha_1, \alpha_2, \alpha_3$ — его корни. (Коэффициент при x^2 можно убрать подходящей заменой) Пусть

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = \beta_1 \in F \\ \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 = \beta_2 \\ \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3 = \beta_3 \end{cases}.$$

Если мы найдём $\beta_1, \beta_2, \beta_3$, то мы найдём корни, решив вышеуказанную систему. Применим S_3 к $\alpha_1, \alpha_2, \alpha_3$, после чего β_2 будет равно одному из $\{\beta_2, \omega\beta_2, \omega^2\beta_2, \beta_3, \omega\beta_3, \omega^2\beta_3\}$, так как нужно внимательно посмотреть на то, как меняются последние два уравнения. Грустно, так как слишком много вариантов. Возведём в куб, тогда останется только β_2^3 и β_3^3. Заметим, что при любых перестановках значения $\beta_2^3 + \beta_3^3 \in F$ и $\beta_2^3\beta_3^3 \in F$ не меняются, то есть получились симметрические многочлены от $\alpha_1, \alpha_2, \alpha_3$. Теперь их можно найти (а-ля по теореме Виета), как корни многочлена второй степени и решить исходное уравнение.

Группа Галуа здесь — S_3 или A_3. Также если f неприводим, то $\mathrm{Gal}(f)$ транзитивна (как доказывалось в прошлом параграфе).

Утверждение. Для уравнений степени n: $\sqrt{D} \in F \iff \mathrm{Gal}(f) \subset A_n$, где $D = \prod_{i \neq j}(\alpha_i - \alpha_j)^2$ — дискриминант.

Доказательство. Запишем эквивалентные утверждения:

$$\sqrt{D} \in F$$

$$\forall \sigma \in \mathrm{Gal}(f)\ \sigma(\sqrt{D}) = \sqrt{D}$$

$$\forall \sigma \in \mathrm{Gal}(f)\ \sigma \in A_n$$

$$\mathrm{Gal}(f) \subset A_n$$

□

В частности, для $n = 3$ получится $\mathrm{Gal}(f) = A_3$.

4.3 Решение уравнений четвёртой степени

Пусть у нас есть уравнение $x^4 + ax^2 + bx + c = 0$, опять же обозначим корни за α_i. Мы вновь хотим найти три переменные β_i, такие что многочлен $r_3(f) = (x - \beta_1)(x - \beta_2)(x - \beta_3)$ является симметрическим.

Возьмём с потолка

$$\begin{cases} \beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3 \end{cases}.$$

Определение. Многочлен $r_3(f)$ называется *кубической резольвентой.*

Теперь остаётся построить кубическое уравнение с корнями β_1, β_2, β_3, найти все α_i, пользуясь тем, что $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$ (коэффициент при x^3).

Вся эта магия сработала из-за того, что в S_4 есть нормальная подгруппа

$$\{e, (12)(34), (13)(24), (14)(23)\},$$

что делает S_4 разрешимой, то есть для бóльших степеней уже не прокатит.

Остаётся построить классификацию группы $\mathrm{Gal}(f)$. Если $\sqrt{D} \in F$, то по утверждению выше $\mathrm{Gal}(f)$ — это A_4 или V_4. Иначе S_4, D_4 или $\mathbb{Z}/4\mathbb{Z}$. А именно, варианты A_4 и S_4 возможны тогда и только тогда, когда $r_3(f)$ неприводим.

Утверждение. $3 \mid |\,\mathrm{Gal}(f)| \iff r_3(f)$ неприводим.

Доказательство. $\Leftarrow$. Если $r_3(f)$ неприводим, то $\mathrm{Gal}(r_3(f)) \subset \mathrm{Gal}(f)$, причём $3 \mid |\,\mathrm{Gal}(r_3(f))|$.

$\Rightarrow$. Рассмотрим $(1\ 2\ 3) \in \mathrm{Gal}(f)$. Тогда $(1\ 2\ 3)\beta_1 = \beta_3$, $(1\ 2\ 3)\beta_3 = \beta_2$ и $(1\ 2\ 3)\beta_3 = \beta_1$. Следовательно, $\beta_1 \sim \beta_2 \sim \beta_3$, откуда $r_3(f)$ неприводим.

$\square$

5 Разрешимость в радикалах

Пусть F — поле, $f(x) \in F[x]$. Мы хотим понять, разрешим ли $f(x)$ в радикалах.

Определение. $f(x)$ *разрешим в радикалах*, если его корни можно получить операциями '+', '-', '·', '/', '$\sqrt[n]{}$'. Более формально:

1. Поле разложения $f(x)$, обозначим за L, удовлетворяет условию

$$L \subset K = K_0 \supset K_1 \supset K_2 \supset \cdots \supset K_s = F,$$

   где K_i получено из K_{i+1} добавлением корня $x^{n_i} - a_{i+1}$, где $a_{i+1} \in K_{i+1}$.

2. Альтернативно, что эквивалентно, можно сказать, что все $K_i \supset K_{i+1}$ являются полями разложения $x^{n_i} - a_i$, где $a_i \in K_i$.

3. Ещё альтернатива: $K \supset F$ — расширение Галуа и все $K_{i-1} \supset K_i$ — поля разложения $x^{n_i} - a_i$.

Теорема. (2) и (3) эквивалентны. Идея в том, чтобы взять второе свойство и рассмотреть поле разложения произведения минимальных многочленов для $a_1, \ldots, a_s$, после чего доказать, что оно нормальное. Детали — на отл.(10).

Почему это не тривиально: рассмотрим расширения $\mathbb{Q} \subset L \subset M$, где в L добавили корень $x^2 - 2$, а в M — корень $x^2 - \sqrt{2}$. Получается, что $M = \mathbb{Q}(\sqrt[4]{2})$, но это расширение не нормальное, так что нужно следить за сопряжёнными корнями. Как полагается, далее мы будем пользоваться самым сильным, третьим, определением.

Пусть $\mathrm{Gal}(f) \subset G_s \supset G_{s-1} \supset \dots \supset G_0 = \{e\}$ — соответствующая цепочке полей разложения цепочка групп Галуа.

Лемма. $K_{i-1} \supset K_i$ — поле разложения тогда и только тогда, когда $G_{i-1} \triangleleft G_i$. Доказательства не было.

Утверждение. $\mathrm{Aut}_{K_i}(K_{i-1}) \cong G_i/G_{i-1}$. Доказательства не было.

Утверждение. Пусть $K \supset L \supset F$, причём все три расширения нормальные. Тогда $\mathrm{Aut}_F(L) \cong \mathrm{Aut}_F(K)/\mathrm{Aut}_L(K)$.

Доказательство. Положим $\varphi : \mathrm{Aut}_F(K) \to \mathrm{Aut}_F(L)$, такой что $\varphi(g) = g|_L$. Тогда это сюръективный гомоморфизм, причём $\mathrm{Ker}(\varphi) = \mathrm{Aut}_L(K)$. По ОТГ получаем искомое.

$\square$

Теорема. $f(x)$ разрешим в радикалах тогда и только тогда, когда $\mathrm{Gal}(f)$ разрешима.

Доказательство. $\Rightarrow$. Мы знаем, что все $G_{i-1} \triangleleft G_i$ и $G_i/G_{i-1} = \mathrm{Gal}(x^{n_i} - a_i)$. Теперь мы хотим, чтобы все $\mathrm{Gal}(x^{n_i} - a_i)$ были абелевы, а отсюда по утверждению из теории групп $\mathrm{Gal}(f)$ разрешима.

$\Leftarrow$. Так как $\mathrm{Gal}(f)$ разрешима можно построить цепочку $\mathrm{Gal}(f) = G_s \supset G_{s-1} \supset \dots \supset G_0 = \{e\}$, такую что все G_i/G_{i-1} циклические. Отсюда все $K_{i-1} \supset K_i$ являются полями разложения $x^{n_i} - a_i$.

В доказательстве остались дырки, которые вынесены в отдельные утверждения.

$\square$

Замечание. Дырка в $\Rightarrow$: слишком много хотим. А именно, например, $\mathrm{Gal}(x^3 - 2) = S_3$, $\mathrm{Gal}(x^4 - 2) = D_4$ — совсем не абелевы. Решается расширением полей в два шага: сначала добавим $x^n - 1$, получится циклическая группа Галуа, потом $x^n - a$, с корнями из единицы это уже будет абелева. Дырка в $\Leftarrow$ не особо серьёзная, а именно, называется теорией Куммера.

Утверждение. Если $L \supset F$ — поле разложения $x^n - 1$ и $(\mathrm{char}(F), n) = 1$, то $\mathrm{Gal}_F(L)$ абелева.

Доказательство. В частности, $L = F(\xi_n)$. Заметим, что любой элемент $\mathrm{Gal}_F(L)$ задаётся, как $\xi_n \mapsto \xi_n^k$, сохраняющий F. Рассмотрим $g, h \in \mathrm{Gal}_F(L)$, $g(\xi_n) = \xi_n^k$ и $h(\xi_n) = \xi_n^l$, тогда $g \circ h(\xi_n) = \xi_n^{kl}$.

Теперь возьмём $\varphi : \mathrm{Gal}_F(L) \to \mathbb{Z}_n^*$, $\varphi(g)$ — степень ξ_n в выражении $g(\xi_n)$. По доказанному это гомоморфизм, так что $\mathrm{Gal}_F(L)$ абелева.

$\square$

Утверждение. Если $L \supset F$ — поле разложения $x^n - a$ и в F если все корни $x^n - 1$, то $\mathrm{Gal}_F(L)$ вкладывается в $\mathbb{Z}_n$, то есть $\mathrm{Gal}_F(L)$ циклическая.

Доказательство. Возьмём один из корней α: $\alpha^n = a$ и $g \in \mathrm{Aut}_F(L)$. Тогда $\frac{g(\alpha)}{\alpha} \in F$, так как g переводит α в один из корней $x^n - a$, а это в точности α, умноженное на корень n-ой степени из единицы, который лежит в поле. Теперь можно положить $\varphi : \mathrm{Aut}_F(L) \to F^*$, сопоставляющий отображениям g элемент $\frac{g(\alpha)}{\alpha}$. Это гомоморфизм, так как

$$\frac{h \circ g(\alpha)}{\alpha} = \frac{h(g(\alpha))}{g(\alpha)} \cdot \frac{g(\alpha)}{\alpha} = \frac{h(g(\alpha))}{\alpha}.$$

Теперь из этого гомоморфизма можно построить вложение в $\mathbb{Z}_n$: так как $\frac{g(\alpha)}{\alpha} = \xi_n^k$, достаточно взять этот самый k. Во-первых, определение корректно, так как если взять другой корень $\alpha \cdot \xi_n^m$, то получится

$$\frac{g(\alpha\xi_n^m)}{\alpha\xi_n^m} = \frac{\xi_n^m g(\alpha)}{\xi_n^m \alpha} = \frac{g(\alpha)}{\alpha}.$$

Во-вторых, степени суммируются при композиции: пусть $\frac{g(\alpha)}{\alpha} = \xi_n^k$, $\frac{h(\alpha)}{\alpha} = \xi_n^l$, тогда

$$g \circ h(\alpha) = g(\xi_n^l \cdot \alpha) = \xi_n^k g(\alpha) = \alpha \cdot \xi_n^{k+l}.$$

□

Замечание. В доказательстве теоремы о разрешимости мы теперь будем специально брать поля разложения так, чтобы $G_i/G_{i-1} = \mathrm{Gal}(x^n - 1)$, тогда будет абелева, или $G_i/G_{i-1} = \mathrm{Gal}(x^n - a)$, и все корни из единицы уже есть.

Пример. Пусть $f(x) = x^5 - 4x + 2$ над $\mathbb{Q}$. По признаку Эйзенштейна он неприводим, по матанализу у него есть 3 вещественных корня. Из первого следует, что $\mathrm{Gal}(f)$ транзитивна, из второго — что комплексное сопряжение является автоморфизмом. Получается, что $\mathrm{Gal}(f) \subset S_5$ и найдётся транспозиция $(i, j) \in \mathrm{Gal}(f)$.

Утверждение. Если $G \subset S_p$ транзитивна и найдётся $(i, j) \in G$, то $G = S_p$.

Доказательство. Рассмотрим граф транспозиций. Мы хотим доказать, что во всех компонентах связности одинаковое число элементов. Рассмотрим какую-то вершину k, теперь докажем, что $\deg(1) \leqslant \deg(k)$. Без ограничения общности $(1\ 2) \in G$, также зафиксируем $i \in \{1, \ldots, n\}$, тогда найдётся $\sigma \in G$, такая что $\sigma(1) = i$ (в силу транзитивности). Тогда в группе есть элемент $\sigma(1\ 2)\sigma^{-1} = (i\ \sigma(2))$. Следовательно, любой транспозиции из единицы мы сопоставили транспозицию из i, откуда $\deg(1) \leqslant \deg(i)$.

Таким образом, все компоненты связности содержат одинаковое число элементов, откуда в силу того, что p простое и группа не пустая, все эти размеры равны p.

□

Пример. (Уравнение, не разрешимое в радикалах) Будем строить так, чтобы группа Галуа $\mathrm{Gal}(f)$ была равна S_5, ибо $S_5' = A_5$ и $A_5' = A_5$. Построим многочлен с ровно тремя вещественными корнями, тогда два будут комплексными. Тогда у нас будет автоморфизм, соответствующий транспозиции, — комплексное сопряжение. Более того, любые два корня можно перевести друг в друга автоморфизмом, откуда группа Галуа транзитивна. Следовательно, $\mathrm{Gal}(f) = S_5$. Пример подходящего многочлена: $x^5 - 4x + 2$.

Теорема. (Теория Куммера) Пусть $K \supset F$ — расширение Галуа и F содержит все корни $x^n - 1$, причём $(n, \mathrm{char}(F)) = 1$. Тогда $\mathrm{Gal}_F(K) \cong \mathbb{Z}_n$ циклическая тогда и только тогда, когда найдётся $a \in F$, такое что K является полем разложения $x^n - a$ над F.

Доказательство. $\Leftarrow$ доказали ранее. $\Rightarrow$. Пусть $\mathrm{Gal}_F(K) = \langle g \rangle_n$. Мы хотим найти $\alpha \in K$, такой что $\frac{g(\alpha)}{\alpha} = \gamma$, где γ — корень n-ой степени из единицы. Это нужно, чтобы получить, что все $g^k(\alpha) = \gamma^k \cdot \alpha$ лежат в поле, а это и есть все корни уравнения $x^n - \alpha^n = 0$. Но почему α^n лежит в F? Всё просто: $g(\alpha^n) = g(\alpha)^n = \gamma^n \alpha^n = \alpha^n$, то есть $\alpha^n \in K^{\mathrm{Gal}_F(K)} = F$.

Теперь найдём α: для этого возьмём $b \in F$ и запишем очень интересную линейную комбинацию

$$\alpha = \lambda_0 b + \lambda_1 g(b) + \cdots + \lambda_{n-1} g^{n-1}(b).$$

Для пафоса применим к ней ещё раз g:

$$g(\alpha) = \lambda_0 g(b) + \lambda_1 g^2(b) + \cdots + \lambda_{n-1} b,$$

в конце просто b, так как по условию $g^n = id$. Теперь в линейной комбинации возьмём $\lambda_i = \gamma^i$, получится

$$g(\alpha) = g(b) + \gamma g^2(b) + \cdots + \gamma^{n-1} b = \gamma^{-1}(\gamma g(b) + \gamma g^2(b) + \cdots + \gamma^n b) =$$

(просто поставим последнее слагаемое в начало)

$$= \gamma^{-1}(b + \gamma g(b) + \cdots + \gamma^{n-1} g^{n-1}(b)).$$

Заметим, что это в скобках получилась в точности линейная комбинация, написанная в начале, то есть $g(\alpha) = \gamma^{-1}\alpha$ — а это и есть то, что мы хотели.

□

Замечание. В доказательстве есть дырка — α может быть равно нулю. Но можно подобрать так, чтобы проблем не было.

Определение. Пусть G — группа, F — поле. *Характером* называется гомоморфизм $\chi : G \to F^*$.

Теорема. (Артена о характерах) Пусть $\chi_1, \ldots, \chi_n$, $\chi_i : G \to F^*$, — различные характеры, где G конечна. Тогда они линейно независимы.

Доказательство. Индукцией по k. При $k = 1$ имеем $\lambda\chi_1(g) = 0$, тогда $\lambda = 0$, так как в F^* нет нуля.

Переход $k \to k + 1$: пусть для всех g

$$\lambda_1\chi_1(g) + \cdots + \lambda_{k+1}\chi_{k+1}(g) = 0.$$

Без ограничения общности будем считать, что $\lambda_1 \neq 0$. Так как характеры различны, найдётся $g_0 \in G$, такой что $\chi_1(g_0) \neq \chi_{k+1}(g_0)$. Домножим (*) на $\chi_{k+1}(g_0)$:

$$\lambda_1\chi_1(g)\chi_{k+1}(g_0) + \cdots + \lambda_{k+1}\chi_{k+1}(g)\chi_{k+1}(g_0) = 0.$$

Теперь подставим в (*) $g = g + g_0$:

$$\lambda_1\chi_1(g)\chi_1(g_0) + \cdots + \lambda_{k+1}\chi_{k+1}(g)\chi_{k+1}(g_0) = 0.$$

Наконец, вычтем:

$$\lambda_1\chi_1(g)(\chi_{k+1}(g_0) - \chi_1(g_0)) + \cdots + \lambda_k\chi_k(g)(\chi_{k+1}(g_0) - \chi_k(g_0)) = 0.$$

Так как $\chi_{k+1}(g_0) - \chi_i(g_0)$ — это какие-то константы, их можно загнать в λ_i и дальше по индукции. По построению сверху не всё сократилось, так как $\chi_{k+1}(g_0) \neq \chi_1(g_0)$.

□

Замечание. Беря $G = F^*$, мы получаем, что различные автоморфизмы F^* линейно независимы. Это закрывает дырку в теории Куммера: если для всех b мы получаем $\alpha = 0$, то автоморфизмы $g, g^2, \ldots, g^n$ линейно зависимы.

6 Великая теорема Ферма при $n = 3$

Мы хотим доказать, что уравнение $x^3 + y^3 = z^3$ не имеет нетривиальных решений в целых числах. Докажем более сильное утверждение: нетривиальных решений нет в числах Эзенштейна $\mathbb{Z}[\omega]$. Тогда уравнение переписывается в виде $(x + y)(x + \omega y)(x + \omega^2 y) = z^3$. Сразу скажем, что x, y, z взаимно просты, иначе сократим.

Исследуем НОДы: $(x+y, x+\omega y) = (x+y, (1-\omega)y)$, $(x+\omega y, x+\omega^2 y) = (x+\omega y, \omega(1-\omega)y)$, $(x + y, x + \omega^2 y) = (x + y, (1 + \omega)(1 - \omega)y)$.

Далее мы будем доказывать, что все вышеуказанные НОДы равны $1 - \omega$. Для этого будем считать сумму $\pm x^3 \pm y^3 = \pm z^3$ по модулю 9. Почему? Потому что $(1-\omega)^2 \sim 3$, то есть $9 \sim (1-\omega)^4$. Положим $\lambda = 1-\omega$.

Утверждение. Если один из $x+y, x+\omega y, x+\omega^2 y$ делится на $1-\omega$, то и все делятся на $1-\omega$. Действительно, они отличаются друг от друга на $(1-\omega)y$ или $(1-\omega)\omega y$.

Лемма 1. Пусть $x \in \mathbb{Z}[\omega]$. Тогда либо $\lambda \mid x$, либо $x \equiv r \mod 3$, где $r \in \mathbb{Z}[\omega]^*$.

Доказательство. Так как $(1-\omega)^2 \sim 3$, получаем $3 \mid (x-r) \iff (1-\omega)^2 \mid (x-r)$. Теперь можно перебрать все 9 вариантов того, чему равен r: а именно, $a+b\omega$, где $a, b \in \{0, \pm 1\}$, и увидеть, что это действительно так. В частности, $1, 1+\omega, \omega, -1, \omega^2, 1+\omega^2$ обратимы, так как лежат на единичной окружности, а $1-\omega, 0, -1+\omega$ делятся на λ.

□

Лемма 2. Если $x \in \mathbb{Z}[\omega]$ и $\lambda \nmid x$, то $x^3 \equiv \pm 1 \mod 9$.

Доказательство. По лемме 1 $x = 3z + u$, где $u \in \mathbb{Z}[\omega]^*$. Возведём в куб: $x^3 = u^3$ (снова можно перебрать все остатки и убедиться).

□

Лемма 3. Если $\pm x^3 \pm y^3 \pm z^3 = 0$ и $x, y, z \in \mathbb{Z}[\omega]$, причём $(x,y) = (x,z) = (y,z) = 1$, то $\lambda \mid xyz$.

Доказательство. Действительно, в противном случае по лемме 2 получаем $\pm x^3 \pm y^3 \pm z^3 \equiv \pm 1 \pm 1 \pm 1 \equiv 0 \mod 9$, что быть не может.

□

Теперь рассмотрим уравнение $r_x x^3 + r_y y^3 + r_z z^3 = 0$, где $r_x, r_y, r_z \in \mathbb{Z}[\omega]^*$. По лемме 3 можно сичтать, что $\lambda \mid z$. Вынесем λ из z: $r_x x^3 + r_y y^3 = r_z \lambda^{3k} \cdot \overline{z}^3$, где $\lambda \nmid xy\overline{z}$ (так можно считать в силу взаимной простоты).

Утверждение. Если существует решение этого уравнения, то существует решение уравнения $x^3 + y^3 = \tilde{r}_z \lambda^{3k} z^3$, где $k \geqslant 2$.

Доказательство. Рассмотрим наше уравнение по модулю 9. По лемме 1 $x^3 = y^3 = z^3 = \pm 1 \mod 9$, откуда $\pm r_x \pm r_y \pm r_z \lambda^{3k} \equiv 0 \mod 9$. Заметим, что $|\lambda^3| = 3\sqrt{3} \approx 5$, и от него нельзя отойти на расстояние 2 (то есть прибавить $\pm r_x \pm r_y$, модуль которых равен единице) до числа, делящегося на 9. Немного рукомахательно, но теперь $k \geqslant 2$, откуда $\pm r_x \pm r_y \equiv 0 \mod 9$, значит, $\pm r_x \pm r_y = 0$, так как они обратимы, то есть остаток по модулю 9 их однозначно определяет. Остаётся подставить и сократить.

□

Теперь пусть (x, y, z) — решение $x^3 + y^3 = z^3$. Перейдём к решению уравнения $x^3 + y^3 = \tilde{r}_z \lambda^{3k} z^3$, возьмём такое, что k минимально. Тогда $(x+y)(x+\omega y)(x+\omega^2 y) = \tilde{r}_z \lambda^{3k} z^3$. Так как произведение слева делится на λ^{3k}, хотя бы один из них делится на λ, а по первому утверждению они все делятся на λ. Нетрудно заметить, что если НОД выражений под скобками не равен λ, то НОД x, y, z будет не равен единице. Отсюда имеет место запись

$$\begin{cases} x + y = r_{x_0} \lambda x_0^3 \\ x + \omega y = r_{y_0} \lambda y_0^3 \\ x + \omega^2 y = r_{z_0} \lambda^{3k-2} z_0^3 \end{cases}.$$

Оставшуюся степень можно запихнуть в последнее без ограничения общности, ибо достаточно сделать замену. Теперь заметим, что

$$0 = (x+y) + \omega(x+\omega y) + \omega^2(x+\omega^2 y) =$$

$$= r_{x_0} \lambda x_0^3 + \omega r_{y_0} \lambda y_0^3 + \omega^2 r_{z_0}^3 \lambda^{3k-2} z_0^3.$$

Сократим λ и перегруппируем слагаемые:

$$r_{x_0}x_0^3 + \tilde{r}_{y_0}y_0^3 + \tilde{r}_{z_0}\lambda^{3k-3}z_0^3 = 0.$$

Итак, нашлась новая тройка (x_0, y_0, z_0), такая что $(x_0, y_0, z_0) = 1$ и k строго меньше — противоречие со взятием k.

□

7 Теорема Гильберта о нулях

Пусть F — поле, $K \supset F$ — алгебраически замкнутое алгебраическое расширение. Положим для идеала $I \subset F[x_1, \ldots, x_n]$ отображение $V(I)$ — множество таких $(t_1, \ldots, t_n) \subset K^n$, что для всех $f \in I$ выполняется $f(t_1, \ldots, t_n) = 0$. Иными словами, $V(I)$ — множество наборов переменных, обнуляющих все многочлены в I.

Теорема. (Nullstellensatz, сильная форма, доказательство на отл.(10)) Пусть $f \in F[x_1, \ldots, x_n]$, $I \subset F[x_1, \ldots, x_n]$ — идеал, такой что $f(x) = 0$ для всех $x \in V(I)$. Тогда найдётся $r \in \mathbb{N}$, такое что $p^r \in I$.

Теорема. (Nullstellensatz, слабая форма) Пусть $I \subset F[x_1, \ldots, x_n]$ — идеал. I содержит единицу тогда и только тогда, когда $V(I)$ пусто.

Доказательство. $\Rightarrow$: идеал совпадает с $F[x_1, \ldots, x_n]$, очевидно пусто.

$\Leftarrow$. От противного: пусть I не содержит единицу, тогда его можно расширить до максимального идеала J. Как известно, $J = (x_1 - a_1, \ldots, x_m - a_m)$, где $a_1, \ldots, a_m \in K$. Тогда заметим, что все многочлены в J обнуляются на $(a_1, \ldots, a_m)$, значит, и все многочлены в I обнуляются, то есть $(a_1, \ldots, a_m) \in V(I)$ — противоречие.

□