Теория Галуа*

Александр Лузгарев

19 мая 2016 г.

Содержание

*Конспект лекций факультатива для механиков весны 2016 года; предварительная версия.

1 Мотивация

1.1 Квадратные уравнения

Люди с древних времен хотели решать алгебраические уравнения. По-видимому, методы для решения квадратных уравнений были известны как минимум четыре тысячи лет назад в Вавилоне; явная формула была приведена Брахмагуптой в 628 году нашей эры. Эта формула теперь изучается школьниками: для вещественных чисел p, q уравнение $x^2 + px + q = 0$ имеет корни

$$x = \frac{-p \pm \sqrt{p^2 - 4q}}{2}.$$

Разумеется, если $p^2 - 4q < 0$, эта формула не приводит к вещественным решениям, но, как мы знаем теперь, она остается верной, если искать корни в поле комплексных чисел. Отметим также, что более общее квадратное уравнение вида $ax^2 + bx + c = 0$ приводится к указанному выше делением на a (а если $a = 0$, то это и не квадратное уравнение вовсе, а линейное).

Для вывода этой формулы заметим, что первые два слагаемых в выражении $x^2 + px + q$ можно рассматривать как начало формулы квадрата суммы: $(x+?)^2 = x^2 + 2?x+?^2$. Если мы хотим получить в правой части px, нужно взять $? = p/2$ и рассмотреть тождество $(x + p/2)^2 = x^2 + px + p^2/4$. Это подсказывает, что можно прибавить и вычесть из нашего уравнения $p^2/4$:

$$x^2 + px + p^2/4 - p^2/4 + q = 0,$$

что приводит нас к

$$(x + p/2)^2 = p^2/4 - q$$

(эта процедура называется «выделение полного квадрата»). Если $p^2/4 - q < 0$, полученное уравнение, очевидно, не имеет решений. Если же $p^2/4 - q \geqslant 0$, то, извлекая корень из обеих частей, получаем

$$x + p/2 = \pm\sqrt{p^2/4 - q},$$

откуда несложным преобразованием получается известная школьная формула.

Отметим, что неопределенность в знаке при извлечении корня как раз и приводит в итоге к двум решениям, а не одному. При переходе к комплексным числам картина резко упрощается: не нужно заботиться о знаке выражения $p^2/4 - q$, поскольку в поле $\mathbb{C}$ из *любого* ненулевого числа извлекается ровно два квадратных корня, и, таким образом, исходное квадратное уравнение с $p^2/4 - q \neq 0$ всегда имеет ровно два решения (а если $p^2/4 - q = 0$, то в некотором смысле решения тоже два, но они совпали — появился кратный корень).

Разумеется, четыре тысячи лет назад в древнем Вавилоне (да и в древней Индии седьмого века) комплексных чисел не знали. Более того, были проблемы даже с отрицательными числами, так что речь шла о решении уравнений трех различных видов: $x^2 = px + q$, $x^2 + px = q$, $x^2 + q = px$ — а уравнение вида $x^2 + px + q = 0$ вообще не имело решений, поскольку и решения-то искались только среди положительных чисел.

1.2 Кубические уравнения

Отрицательные числа не вошли в обиход широкой публики и к 1515 году, когда Сципионе дель Ферро получил формулу для решения кубического уравнения вида $x^3 + px = q$. Его метод, впрочем, остался неопубликованным (и до сих пор о нем не так много известно), но он передал его некоторым своим ученикам перед тем, как умер в 1526 году. Одного из них звали Антонио Мария Фьор, и он вошел в историю тем, что в 1535 году вызвал на соревнование по решению задач Никколо Фонтана (по прозвищу Тарталья), который к тому времени научился решать некоторые очень частные случаи кубических уравнений. Узнав, что Фьор получил от своего учителя секретную формулу, Тарталья с необычайной энергией взялся за эту задачу и успел прийти к решению до начала соревнования — в котором одержал победу.

Об этом достижении узнал Джироламо Кардано, ученый широкого кругозора, который в то время как раз писал учебник по арифметике. Он долго упрашивал Тарталью сообщить ему формулу, и в итоге в 1539 году Тарталья сообщил ему (разумеется, в стихах) формулы для решения уравнений вида $x^3 + px = q$, $x^3 = px + q$, и намек на решение уравнения вида $x^3 + q = px$. Получив стихи, Кардано, приложив определенные усилия, восстановил вывод этих формул, а также разобрал все оставшиеся случаи (у него получилось тринадцать видов уравнений) — и изложил в своем учебнике, не забыв сослаться на Тарталью и дель Ферро. После этого между Кардано и Тартальей разгорелся масштабный диспут о праве на интеллектуальную собственность: Тарталья утверждал, что он посылал Кардано стихи не для публикации, а вовсе наоборот, под обязательство о неразглашении, и т. д. Тем не менее, формула для решения кубических уравнений традиционно называются «формулой Кардано».

Разумеется, мы изложим вывод этой формулы в общем случае и в современных обозначениях. Итак, нас интересует уравнение вида $x^3 + ax^2 + bx + c = 0$. Первый шаг напоминает начало решения квадратного уравнения: выделим «полный куб», содержащий слагаемые $x^3 + ax^2$. Для этого совершим замену переменной x на $y = x + a/3$. Наше уравнение примет вид $(x + a/3)^3 + ?x + ? = 0$, то есть, $y^3 + ?y + ?$. Это показывает, что можно с самого начала считать, что $a = 0$. Поэтому сейчас мы займемся решением уравнения

$$x^3 + px + q = 0.$$

Идея решения состоит в том, чтобы искать x в виде $x = \sqrt[3]{u} + \sqrt[3]{v}$. Разумеется, при этом мы получим уравнение с двумя неизвестными, u и v, и получим больше свободы: каждое вещественое число x многими разными способами представляется в таком виде. После подстановки получаем

$$(\sqrt[3]{u} + \sqrt[3]{v})^3 + p(\sqrt[3]{u} + \sqrt[3]{v}) + q = 0.$$

Раскрывая куб и группируя слагаемые, получаем

$$u + v + q + (3\sqrt[3]{u}\sqrt[3]{v} + p)(\sqrt[3]{u} + \sqrt[3]{v}) = 0$$

Неформально говоря, мы получили сумму «рациональной части» $u + v + q$ и «иррациональной части» $(3\sqrt[3]{u}\sqrt[3]{v} + p)(\sqrt[3]{u} + \sqrt[3]{v})$. Хочется верить, что каждое из этих слагаемых в

отдельности равно нулю. Более точно, пользуясь свободой в определении u и v, мы будем искать такие пары (u, v), для которых $u+v+q = 0$ и $(3\sqrt[3]{u}\sqrt[3]{v}+p)(\sqrt[3]{u}+\sqrt[3]{v}) = 0$. Равенство нулю последнего выражения означает, что один из двух его сомножителей равен нулю — и вряд ли это $\sqrt[3]{u} + \sqrt[3]{v} = x$ (если у исходного уравнения есть корень $x = 0$, то $q = 0$, и все уравнение можно свести к квадратному делением на x; поэтому далее можно считать, что $q \neq 0$). Поэтому нам хочется решить систему из двух уравнений

$$\begin{aligned} u + v &= -q, \\ 3\sqrt[3]{u}\sqrt[3]{v} &= -p. \end{aligned}$$

Возводя второе равенство в куб, получаем, что мы знаем сумму двух чисел ($u+v = -q$) и их произведение ($uv = -p^3/27$). Теорема Виета говорит нам, что u и v тогда должны быть корнями квадратного (относительно t) уравнения

$$t^2 + qt - p^3/27 = 0.$$

Пользуясь формулой для корней квадратного уравнения, получаем, что

$$u, v = \frac{-q \pm \sqrt{q^2 + 4p^3/27}}{2}.$$

Вспоминая, что $x = \sqrt[3]{u} + \sqrt[3]{v}$, находим

$$x = \sqrt[3]{\frac{-q + \sqrt{q^2 + 4p^3/27}}{2}} + \sqrt[3]{\frac{-q - \sqrt{q^2 + 4p^3/27}}{2}}.$$

Примерно это и называется «формулой Кардано». К ней возникает несколько вопросов.

- Еще Кардано развлекался тем, что сочинял кубические уравнения с заранее известным корнем: типа, уравнение $x^3 + 16 = 12x$ заведомо имеет корень $x = 2$. Однако, подстановка в формулу Кардано (проверьте!) дает нам $x = \sqrt[3]{-8} + \sqrt[3]{-8} = -4$, что, конечно, тоже является корнем того же уравнения, но не тем, который ожидал получить Кардано (не любивший отрицательные числа). Возможно, именно такие эффекты привели его к осознанию необходимости повышения статуса отрицательных чисел.

- Если взять кубическое уравнение с заранее известным «хорошим» корнем, может так получиться, что формула Кардано даст тот же корень, но записанный в какой-то странной форме. Для примера посмотрим на уравнение $x^3 + x = 2$. Оно имеет корень $x = 1$ — и, более того, это единственный вещественный корень (функция $x^3 + x$ монотонно возрастает). Формула Кардано дает нам вещественный ответ

  $$x = \sqrt[3]{1 + \frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1 - \frac{2}{3}\sqrt{\frac{7}{3}}},$$

  который обязан равняться 1 — но кто из нас умеет это доказывать, не ссылаясь, фактически, на ту самую формулу Кардано?

- Бывает и хуже: рассмотрим уравнение $x^3 = 15x + 4$. Невооруженным глазом видно, что у него есть корень $x = 4$. Формула Кардано же утверждает, что у него есть корень

  $$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}},$$

что вообще не имеет никакого смысла, если на дворе середина шестнадцатого века. Тем не менее, именно такого рода примеры фактически привели Кардано не только к отрицательным, но и к комплексным числам: в том же учебнике арфиметики он рассуждает в том духе, что решая квадратное уравнение $x^2-10x+40=0$ по известной формуле, мы, конечно, получаем бессмысленные выражения $5+\sqrt{-15}$ и $5-\sqrt{-15}$, но сумма их все же равна 10, а произведение (с учетом не вполне осмысленных манипуляций с корнями из отрицательных величин) равно 40, как и предсказывает теорема Виета. Рафаэли Бомбелли в 1572 году проделал аналогичные (но чуть более замысловатые) манипуляции с выражением $\sqrt[3]{2+\sqrt{-121}}+\sqrt[3]{2-\sqrt{-121}}$ и получил, что оно все-таки равно 4, хотя и записано в таком экзотическом виде.

- В двадцать первом веке мы не боимся ни отрицательных, ни комплексных чисел, но формула Кардано выглядит не лучше, а в каком-то смысле еще хуже. Мы теперь понимаем, что из каждого числа можно извлечь [ровно] три кубических корня — но это значит, что выражение в формуле Кардано может, вообще говоря, иметь девять различных значений (выбор знака при извлечении квадратного корня лишь переставляет местами слагаемые). И действительно, рассмотрение примеров показывает, что формула Кардано действительно может давать три корня кубического корня — и еще шесть выражений, не являющихся корнями. Разгадка, разумеется, проста: при выводе мы возвели в куб равенство $3\sqrt[3]{u}\sqrt[3]{v}=-p$. Три различных кубических корня из u (и из v) отличаются друг от друга на кубические корни из 1, и при выборе корня из u и корня из v необходимо проследить, чтобы их произведение все-таки равнялось $-p/3$ (а не отличалось от него на кубический корень из 1).

1.3 Уравнения четвертой степени

Метод решения уравнений четвертое степени появился вскоре после метода для кубических уравнений. Его автор, Людовико Феррари, был учеником Кардано, и метод в итоге попал в тот же самый учебник арифметики. Однако, для просвещенной публики того времени уравнения четвертой степени (и выше) не представляли большого интереса, поскольку не имели «физического» смысла. Дело в том, что восприятие операции возведения в степень было в большой степени геометрическим: неизвестная x мыслилась отрезком длины x, а ее квадрат x^2 — буквально квадратом со стороной x (что, впрочем, не мешало еще в глубокой древности складывать эти разноразмерные величины). Разумеется, куб x^3 виделся геометрическим кубом с ребром длины x, а возведение в четвертую степень было операцией допустимой, но довольно бессмысленной, по причине отсутствия перед глазами наглядного четырехмерного пространства.

Первый шаг в решении уравнения четвертой степени вида

$$x^4+ax^3+bx^2+cx+d=0$$

вполне ожидаем: заменой $y=x+a/4$ мы избавляемся от коэффициента при x^3 и получаем

$$y^4+py^2+qy+r=0.$$

Далее выделим квадрат из первых двух слагаемых:

$$\left(y^2+\frac{p}{2}\right)^2=-qy-r+\frac{p^2}{4}.$$

Теперь посмотрим, что происходит, когда к выражению, стоящему под квадратом в левой части, мы прибавляем некоторое u:

$$\left(y^2+\frac{p}{2}+u\right)^2=-qy-r+\frac{p^2}{4}+2uy^2+pu+u^2.$$

Идея состоит в том, чтобы подобрать добавку u так, чтобы правая часть также стала полным квадратом от некоторого линейного по y выражения. Коэффициент при y^2 равен $2u$, поэтому хочется, чтобы правая часть имела вид $(y\sqrt{2u}+\dots)^2$; коэффициент при y же равен $-q$, поэтому она должна иметь вид $(y\sqrt{2u} - q/2\sqrt{2u})^2$. Осталось добиться, чтобы свободные члены совпали, а это означает, что

$$-r + \frac{p^2}{4} + pu + u^2 = \frac{q^2}{8u}.$$

Избавляясь от знаменателей, видим, что искомая добавка u должна удовлетворять — о чудо! — *кубическому* уравнению

$$8u^3 + 8pu^2 + (2p^2 - 8r)u - q^2 = 0.$$

Решая это уравнение, мы находим необходимое значение u; возвращаясь к нашему уравнению на y, мы видим, что оно привелось (за счет специального выбора добавки u) к виду

$$\left(y^2 + \frac{p}{2} + u\right)^2 = \left(\sqrt{2u}y - \frac{q}{2\sqrt{2u}}\right)^2,$$

откуда

$$y^2 + \frac{p}{2} + u = \pm\left(\sqrt{2u}y - \frac{q}{2\sqrt{2u}}\right).$$

Таким образом, остается решить два квадратных уравнения.

Формально мы должны также разобрать случай $u = 0$, поскольку в полученном выражении u встречается в знаменателе. Мы не будем этого делать, а обсудим общий смысл полученных результатов. При желании можно было бы выписать формулу для y: решение полученного квадратного уравнения приводит нас к выражению, в которое входит квадратный корень, причем под корнем стоит что-то связанное с u. В свою очередь, u получается решением кубического уравнения, то есть, записывается как сумма корней третьей степени из выражения, включающего квадратный корень (по формуле Кардано). Таким образом, итоговое выражение для u включает «трехэтажные» радикалы: квадратный корень под кубическим корнем под квадратным корнем. Сравните это с двухэтажными радикалами в формуле Кардано (квадратный корень под кубическим корнем) и с одноэтажными в формуле для корней квадратного уравнения (квадратный корень). Позже мы увидим высоконаучное объяснение такой формы ответа в каждом случае.

Одним из первых следствий теории Галуа стала теорема Руффини–Абеля, которая утверждает, грубо говоря, что на этом история «хороших» формул для решения алгебраических уравнений заканчивается: уже для уравнения пятой степени вида

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e$$

невозможно написать формулу с «многоэтажными» радикалами, в которую входили бы коэффициенты a, b, c, d, e, и которая давала бы (хотя бы один!) корень данного уравнения при произвольной (или даже почти произвольной) подстановке значений a, b, c, d, e в нее. Для уравнений третьей степени аналогичная формула есть — это формула Кардано (при желании можно в ней совершить замену, обратную к самому первому выделению точного куба); для уравнений четвертой степени мы не выписали явную формулу, но поняли, что ее при желании можно получить.

1.4 Три классические задачи на построение

Еще одно применение теории Галуа — доказательство неразрешимости трех классических задач на построение циркулем и линейкой. Эти задачи были сформулированы еще в древности:

- (Квадратура круга). Построить квадрат, равновеликий данному кругу.
- (Трисекция угла). Разделить данный угол на три равные части.
- (Удвоение куба). Дано ребро куба. Построить ребро куба, объем которого в два раз больше объема данного куба.

Ниже (в разделе ??) мы уточним формулировки этих задач (и формализуем до некоторой степени понятие построения циркулем и линейкой). Представим, что мы начинаем с плоскости, на которой отмечен отрезок длины 1. Тогда квадратура круга фактически означает построение отрезка длины $\sqrt{\pi}$; невозможность этого мы докажем в предположении трансцендентности числа π. Саму трансцендентность π мы доказывать не будем (хотя это и не очень сложно). Трисекция произвольного угла невозможна хотя бы потому, что невозможно поделить на три равные части уже угол в 60°. А именно, мы покажем, что невозможно построить угол в 20°, поскольку невозможно (начав снова с плоскости с отмеченным единичным отрезком) построить отрезок длины $\sin(20^\circ)$. Наконец, удвоение куба будет следовать из невозможности построения отрезка длины $\sqrt[3]{2}$.

Невозможность построения в этих трех задачах мы докажем (по модулю доказательства трансцендентности π) в разделе ??.

2 Основные определения

2.1 Кольца и идеалы

Мы начинаем с напоминания. Пусть на множестве R заданы две бинарные операции — «сложение» $+\colon R \times R \to R$ и «умножение» $\cdot\colon R \times R \to R$. Говорят, что R является **кольцом** относительно этих операций, если выполняются следующие свойства:

1. $(a + b) + c = a + (b + c)$ для любых $a, b, c \in R$;
2. существует $0 \in R$, называемый **нулем**, такой, что $a + 0 = a = 0 + a$ для любого $a \in R$;
3. для любого $a \in R$ существует элемент $-a \in R$ такой, что $a + (-a) = 0 = (-a) + a$ (такой элемент называется **противоположным** к элементу a);
4. $a + b = b + a$ для любых $a, b \in R$;
5. $(a + b) \cdot c = a \cdot c + b \cdot c$ и $c \cdot (a + b) = c \cdot a + c \cdot b$ для любых $a, b, c \in R$.

Заметим, что первые четыре свойства касаются только операции сложения. Вместе они выражают тот факт, что R с операцией $+$ является *абелевой группой* (а первые три свойства — ассоциативность, наличие нейтрального элемента и наличие обратных — тот факт, что R является *группой*. Позднее мы вернемся к определению группы; пока же отметим, что *аддитивная запись* (в отличие от *мультипликативной*) используется в основном для абелевых групп. Таким образом, лишь последнее свойство накладывает ограничения

на операцию умножения. Однако, большинство встречающихся в математике колец удовлетворяют различным дополнительным условиям. От операции умножения можно требовать ассоциативность:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ для любых } a, b, c \in R;$$

наличие нейтрального элемента:

$$\text{существует элемент } 1 \in R \text{ такой, что } 1 \cdot a = a = a \cdot 1 \text{ для любого } a \in R;$$

коммутативность:

$$a \cdot b = b \cdot a \text{ для любых } a, b \in R.$$

Нам будут встречаться в основном кольца, удовлетворяющие всем этим трем условиям. Поэтому под словом кольцо мы всегда будем подразумевать ассоциативное коммутативное кольцо с 1, если явно не оговорено обратное. Самый простой пример — кольцо целых чисел $\mathbb{Z}$ относительно обычных операций сложения и умножения.

Если же кольцо удовлетворяет дополнительному условию

$$\text{для любого } a \in R, \text{ не равного } 0, \text{ существует элемент } a^{-1} \in R \text{ такой, что } a \cdot a^{-1} = 1 = a^{-1} \cdot a,$$

оно называется **полем**. Таким образом, в поле есть обратные элементы (по умножению) у всех элементов, кроме 0. Обратного элемента у 0 в кольце быть почти никогда не может по простой причине: несложно показать, что $a \cdot 0 = 0$ для любого $a \in R$ (действительно, $0 + 0 = 0$, откуда по дистрибутивности $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, и, вычитая $a \cdot 0$ из обеих частей, получаем $a \cdot 0 = 0$). Если бы существовал элемент 0^{-1}, обратный к 0, мы имели бы $1 = 0^{-1} \cdot 0 = 0$ по только что доказанному; но если в кольце $1 = 0$, то для любого $a \in R$ получаем $a = a \cdot 1 = a \cdot 0 = 0$, поэтому это тривиальное кольцо из одного элемента.

Вам хорошо известны следующие примеры колец.

Примеры 2.1.1.

1. Как уже говорилось, множество $\mathbb{Z}$ целых чисел является кольцом; оно не является полем, поскольку обратные по умножению элементы есть только у ± 1.
2. Множества $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ рациональных, вещественных, комплексных чисел являются полями относительно обычных арифметических операций сложения и умножения.
3. Пусть k — кольцо. Множество $k[x]$ многочленов от одной переменной относительно стандартных операций сложения и умножения является кольцом.
4. Кольцо $\mathbb{Z}/m\mathbb{Z}$ остатков по модулю m; оно является полем тогда и только тогда, когда m — простое число.

2.2 Гомоморфизмы колец

Теперь посмотрим на отображения колец, сохраняющие операции.

Определение 2.2.1. Пусть R, S — кольца. Отображение $f\colon R \to S$ называется **гомоморфизмом (колец)**, если выполняются следующие условия:

1. $f(a + b) = f(a) + f(b)$ для любых $a, b \in R$;
2. $f(a \cdot b) = f(a) \cdot f(b)$ для любых $a, b \in R$;
3. $f(1) = 1$.

Заметим, что мы требуем, чтобы f переводил 1 в 1, но не требуем, чтобы f переводил 0 в 0. Дело в том, что отображение колец (и даже абелевых групп), удовлетворяющее первому условию ($f(a+b) = f(a) + f(b)$), автоматически переводит 0 в 0. Действительно, $f(0) = f(0+0) = f(0) + f(0)$, и, поскольку S — абелева группа, можно вычесть из обеих частей $f(0)$ и получить $0 = f(0)$. Если бы мы попытались аналогично показать, что $f(1) = 1$, ничего бы не вышло, поскольку в S не обязаны существовать обратные элементы по умножению. Поэтому условие $f(1) = 1$ включается в определение гомоморфизма. Кроме того, несложно показать, что $f(-a) = -f(a)$ для гомоморфизма колец f: мы уже знаем, что $f(0) = 0$ и $a + (-a) = 0$, откуда $0 = f(0) = f(a + (-a)) = f(a) + f(-a)$, и, прибавляя к обеим частям $-f(a)$, получаем требуемое. Таким образом, альтернативное определение гомоморфизма колец — это отображение, сохраняющее *все* операции (включая неявно определенную унарную операцию взятия противоположного элемента и 0-арную операции взятия 0 и 1).

Посмотрим на несложные примеры гомоморфизмов колец.

Примеры 2.2.2.

1. Мы знаем, что $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Эти три отображения включения являются гомоморфизмами колец (фактически это означает, что сложение и умножение в этих числовых множествах «устроено одинаково»).

2. Похожим образом, любое кольцо k вкладывается в кольцо многочленов $k[x]$: при этом отображении элемент $a \in k$ переходит в «постоянный многочлен» $a \in k[x]$ степени 0.

3. С каждым кольцом остатков $\mathbb{Z}/m\mathbb{Z}$ связано отображение $\pi\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, сопоставляющее целому числу $a \in \mathbb{Z}$ его остаток $\overline{a}$ по модулю m. Основное свойство арифметики остатков как раз состоит в том, что это отображение является гомоморфизмом.

Определение 2.2.3. Пусть $f\colon R \to S$ — гомоморфизм колец. Множество $\mathrm{Ker}(f) = \{x \in R \mid f(x) = 0\}$ называется **ядром** гомоморфизма f, а множество $\mathrm{Im}(f) = \{y \in S \mid y = f(x) \text{ для некоторого } x \in R\}$ — его **образом**. Иными словами, ядро гомоморфизма — это прообраз нуля, а образ — обычный (теоретико-множественный) образ отображения.

Заметим, что ядро гомоморфизма f тривиально (состоит из одного 0) тогда и только тогда, когда f инъективно. В одну сторону это очевидно (если f инъективно, то в 0 может переходить только 0). Обратно, если $\mathrm{Ker}(f) = 0$ и $f(a) = f(b)$, то $f(a-b) = f(a) - f(b) = 0$, откуда $a - b = 0$ и $a = b$.

Во всех приведенных выше примерах гомоморфизмов, кроме последнего, ядра тривиальны. Посмотрим на последний пример, $\pi\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Прообраз 0 — это те целые числа, которые дают остаток 0 при делении на m, то есть в точности целые числа, делящиеся на m; это множество обозначается через $m\mathbb{Z}$.

2.3 Идеалы и фактор-кольца

Посмотрим, какими могут быть ядра гомоморфизмов колец.

Определение 2.3.1. Пусть R — кольцо. Подмножество $I \subseteq R$ называется **идеалом** кольца R, если оно удовлетворяет следующим условиям:

1. если $a, b \in I$, то $a - b \in I$;
2. если $a \in I$, $r \in R$, то $r \cdot a \in I$.

Обозначение: $I \trianglelefteq R$.

Первое свойство на самом деле эквивалентно тому, что подмножество I а) содержит 0; б) вместе с любыми двумя элементами содержит их сумму; в) вместе с каждым элементом содержит противоположный к нему. Позднее мы узнаем, что такое подмножество называется *подгруппой* (абелевой группы R с операцией сложения). Упражнение: докажите эту эквивалентность! Второе свойство означает, что I выдерживает умножение на элементы R.

Несложно привести тривиальные примеры идеалов: в любом кольце R множества $\{0\}$ и R являются идеалами (их называют **нулевым** и **единичным** соответственно). Не так тривиален идеал $m\mathbb{Z} \trianglelefteq \mathbb{Z}$ целых чисел, делящихся на m. Действительно, сумма двух чисел, делящихся на m, также делится на m; и если число делящееся на m, умножить на любое целое, результат также будет делиться на m. Заметим, что m здесь может быть любым натуральным числом или нулем. В случае $m = 0$ получаем нулевой идеал 0, а в случае $m = 1$ — единичный идеал $\mathbb{Z}$.

Мы уже встречали множества $m\mathbb{Z}$ как ядра гомоморфизмов в кольца остатков; оказывается, это не простое совпадение.

Предложение 2.3.2. *Пусть* $f\colon R \to S$ *— гомоморфизм колец. Ядро* f *является идеалом в* R*:* $\operatorname{Ker}(f) \trianglelefteq R$.

Доказательство. Проверим первое условие из определения идеала: пусть $a, b \in \operatorname{Ker}(f)$; это означает, что $f(a) = f(b) = 0$. Нам нужно показать, что $a - b \in \operatorname{Ker}(f)$. Но $f(a - b) = f(a) - f(b) = 0 + 0 = 0$, что и требовалось. Второе свойство: пусть $a \in \operatorname{Ker}(f)$ (то есть $f(a) = 0$) и $r \in R$; тогда $f(r \cdot a) = f(r) \cdot f(a) = f(r) \cdot 0 = 0$, поэтому $r \cdot a \in \operatorname{Ker}(f)$. □

Таким образом, ядро любого гомоморфизма является идеалом. Наша ближайшая цель — показать, что верно и обратное: любой идеал является ядром некоторого гомоморфизма колец. Для этого мы по кольцу и его идеалу построим специальное кольцо, куда и будет действовать этот гомоморфизм.

Итак, пусть R — кольцо, $I \trianglelefteq R$ — идеал в нем. Определим отношение $\sim$ на R следующим образом: $a \sim b$ тогда и только тогда, когда $a - b \in I$.

Упражнение 2.3.3. *Проверьте, что* $\sim$ *является отношением эквивалентности. Указание: для этого достаточно того, что* I *является аддитивной подгруппой в* R.

Как мы знаем, каждое отношение эквивалентности на множестве R порождает разбиение R на классы эквивалентности; класс, в который попал элемент $a \in R$ мы будем обозначать через $a + I$ или через $\overline{a}$ (внимание! В этом обозначении не указан идеал, который мы взяли для определения отношения). Обозначение $a + I$ вполне обосновано: $a + I = \{a + x \mid x \in I\}$. Полученное множество всех классов эквивалентности мы будем обозначать через R/I.

Введем теперь операции сложения и умножения на R/I. Определим сумму двух классов как $\overline{a} + \overline{b} = \overline{a + b}$, а произведение как $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. То есть, для того, чтобы сложить или перемножить два класса, нужно сложить или перемножить любых представителей этих классов и посмотреть, в какой класс попал результат. Прежде всего нужно показать, что это определение корректно, то есть не зависит от выбора представителей. Действительно, если $\overline{a} = \overline{a'}$ и $\overline{b} = \overline{b'}$, то $a - a' \in I$ и $b - b' \in I$, откуда $(a + a') - (b + b') = (a - a') + (b - b') \in I$, поскольку I является идеалом. Но это означает, что $a + a' \sim b + b'$, то есть, $\overline{a + a'} = \overline{b + b'}$. Кроме того, $ab - a'b' = a(b - b') + (a - a')b' \in I$ по определению идеала. Поэтому $ab \sim a'b'$ и $\overline{ab} = \overline{a'b'}$.

Теперь несложно проверить, что R/I является кольцом относительно введенных операций: все нужные свойства напрямую следуют из аналогичных свойств кольца R и определения операций. Заметим, что роль нуля в кольце R/I играет класс $\overline{0}$, а роль единицы — класс $\overline{1}$. Это кольцо называется **фактор-кольцом** кольца R по идеалу I.

Вместе с кольцом R/I естественным образом строится отображение $\pi\colon R \to R/I$ по формуле $\pi(a) = \overline{a}$. Из определения операций немедленно вытекает, что π является гомоморфизмом колец. Этот гомоморфизм называется **канонической проекцией** кольца R на факторкольцо R/I.

Классический (и, пожалуй, самый простой из нетривиальных) пример фактор-кольца — кольцо остатков $\mathbb{Z}/m\mathbb{Z}$ по модулю m, которое является, как подсказывает обозначение, фактор-кольцом кольца $\mathbb{Z}$ по идеалу $m\mathbb{Z}$ целых чисел, делящихся на m. Аналогии с этим случаем полезно иметь в виду и в общей ситуации: элементы R/I удобно представлять как «остатки» по модулю идеала I, а отношение эквивалентности на R — как «сравнение» по модулю I.

Приведем еще примеры идеалов. Прежде всего заметим, что если R является полем, то в R нет идеалов, кроме нулевого и единичного. Действительно, если $I \trianglelefteq R$ и $a \in I$, $a \neq 0$, то по определению идеала $1 = a \cdot a^{-1} \in I$. Ну, а если $1 \in R$, то и любой элемент $b = 1 \cdot b$ также лежит в R. Верно и обратное:

Предложение 2.3.4. *Кольцо является полем тогда и только тогда, когда в нем нет идеалов, кроме нулевого и единичного.*

Доказательство. Осталось доказать, что если в кольце нет идеалов, кроме нулевого и единичного, то оно является полем. Пусть R такое кольцо и $a \in R$ — ненулевой элемент. Рассмотрим множество $aR = \{ax \mid x \in R\}$. Нетрудно видеть, что оно является идеалом в R. Кроме того, этот идеал содержит a и потому ненулевой. Значит, он совпадает с R и, в частности, содержит 1. Но это означает, что 1 имеет вид $1 = ax$ для некоторого x; этот x и является обратным элементом к a. □

Для любого кольца R и $a \in R$ множество $aR = \{ax \mid x \in R\}$ является идеалом в R. Такой идеал называется **главным идеалом**, порожденным элементом a и обозначается через (a), если из контекста ясно, какое кольцо имеется в виду. Заметим, что единичный и нулевой идеал являются главными, как и обсуждавшиеся выше идеалы вида $m\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Более общо, можно рассмотреть идеалы, порожденные не одним элементом R, а произвольным подмножеством $X \subset R$. А именно, рассмотрим наименьший идеал в R, содержащий X. Такой идеал действительно существует — его можно описать как пересечение всех идеалов в R, содержащих X (нетрудно видеть, что пересечение любого семейства идеалов кольца R также является идеалом в R). Такой идеал часто обозначается через (X). Если множество $X = \{a_1, \ldots, a_n\}$ конечно, то идеал, порожденный X, часто обозначается через $a_1R + \cdots + a_nR$, поскольку он состоит из элементов вида $a_1x_1 + \cdots + a_nx_n$, $x_1, \ldots, x_n \in R$. В кольцах $\mathbb{Z}$ и $k[x]$ любой идеал является главным, однако, скажем, в кольце $k[x, y]$ многочленов от двух переменных идеал, порожденный двумя элементами x, y не является главным. Действительно, если он порожден одним элементом d, то и x, и y должны делиться на d; поэтому d может быть только константой и $(d) = k[x, y]$. Однако идеал (x, y) не совпадает с $k[x, y]$, поскольку у всех многочленов из него свободный член равен нулю.

Биективный гомоморфизм колец называется **изоморфизмом колец**, а кольца, между которыми существует биективный гомоморфизм (и тогда обратное к нему отображение также является гомоморфизмом), называются **изоморфными** (обозначение: $\cong$).

Теорема 2.3.5. *[О гомоморфизме] Пусть* $f\colon R \to S$ *— гомоморфизм колец. Тогда* $R/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$.

Доказательство. Построим отображение $\varphi\colon R/\operatorname{Ker}(f) \to \operatorname{Im}(f)$. Элемент $R/\operatorname{Ker}(f)$ — это класс эквивалентности элементов из R, поэтому его можно записать в виде $\overline{a}$ для некоторого $a \in R$. Положим $\varphi(\overline{a}) = f(a)$. Заметим, что результат действительно лежит в $\operatorname{Im}(f)$, а не

просто в S. Перед тем, как доказывать, что φ является изоморфизмом колец, необходимо проверить корректность определения φ, то есть, его независимость от выбора представителя класса эквивалентности. Пусть $\overline{a} = \overline{b}$, то есть, a и b — два представителя одного класса. Вспоминая определение отношения эквивалентности из конструкции фактор-кольца, заключаем, что $a - b = k$, где $k \in \mathrm{Ker}(f)$. Но тогда $f(a - b) = f(k) = 0$, поскольку k лежит в ядре f, откуда $f(a) - f(b) = 0$ и $f(a) = f(b)$. Таким образом, $\varphi(\overline{a})$ определено корректно.

Проверим теперь, что φ является гомоморфизмом колец. Действительно, если $a, b \in R$, то $\varphi(\overline{a}+\overline{b}) = \varphi(\overline{a+b})$ по определению операций в фактор-кольце. Теперь по определению φ это выражение равно $f(a+b)$, в то время как сумма $\varphi(\overline{a}) + \varphi(\overline{b})$ равна $f(a) + f(b)$. Но полученные выражения равны, поскольку f является гомоморфизмом колец. Совершенно аналогично показывается, что φ сохраняет умножение.

Наконец, проверим, что φ биективно. Для доказательства инъективности гомоморфизма колец достаточно проверить, что его ядро тривиально. Но если $\varphi(\overline{a}) = 0$, то $f(a) = 0$, откуда $a \in \mathrm{Ker}(f)$ и, значит, $\overline{a} = \overline{0}$. Наконец, φ сюръективно, поскольку любой элемент $\mathrm{Im}(f)$ имеет вид $f(a)$ для некоторого $a \in R$, то есть, имеет вид $\varphi(\overline{a})$. □

2.4 Фактор-кольца кольца многочленов

Посмотрим теперь на кольцо $k[x]$ многочленов от одной переменной. Пусть $f \in k[x]$ — некоторый многочлен степени n. Рассмотрим фактор-кольцо $k[x]/(f)$ по идеалу, порожденному f, и постараемся описать его. Как мы говорили выше, его элементы — это в каком-то смысле «остатки» по модулю f. А именно, любой многочлен $a \in k[x]$ можно поделить с остатком на f: $a = fq + r$, где $r \in k[x]$ — многочлен степени меньше n. Мы видим, что $a \sim r$, то есть, в каждом классе эквивалентности по модулю f есть многочлен степени меньше n. Более того, такой многочлен только один: если r_1 и r_2 лежат в одном классе, то $r_1 - r_2$ делится на f и является многочленом степени меньше n; поэтому $r_1 = r_2$. Наконец, очевидно, что любой многочлен степени меньше n лежит в каком-то классе эквивалентности. Мы получили, что элементы $k[x]/(f)$ биективно соответствуют многочленам степени меньше n (иными словами, в каждом классе эквивалентности можно выбрать канонического представителя — многочлен степени меньше n). Для того, чтобы сложить два класса, достаточно сложить их представителей; для того, чтобы перемножить два класса, нужно перемножить два представителя и (если степень результата больше или равна n) поделить на f с остатком.

Например, пусть $k = \mathbb{R}$ и $f = x^2+1 \in \mathbb{R}[x]$. В фактор-кольце $\mathbb{R}[x]/(x^2+1)$ у каждого класса есть канонический представитель степени меньше 2, то есть, имеющий вид $a+bx$, $a, b \in \mathbb{R}$. Посмотрим, как выглядит сложение и умножение классов. Сумма двух классов, представленных многочленами $a+bx$ и $a'+b'x$, содержит многочлен $(a+a')+(b+b')x$. Произведение же этих классов содержит многочлен $(a+bx)(a'+b'x) = aa'+(ab'+a'b)x+bb'x^2$ и, значит, его остаток от деления на x^2+1. Нетрудно видеть, что $aa'+(ab'+a'b)x+bb'x^2 = aa'+(ab'+a'b)x+bb'(x^2+1)-bb'$, поэтому результат эквивалентен многочлену $(aa'-bb')+(ab'+a'b)x$ степени меньше 2. Пристальный взгляд на эти формулы приводит нас к мысли, что полученное кольцо очень похоже на поле комплексных чисел. И действительно, отображение $\mathbb{R}[x]/(x^2+1) \to \mathbb{C}$, $\overline{a+bx} \mapsto a+bi$ является биективным гомоморфизмом колец (проверьте это утверждение!). Итак, мы показали, что $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

Теперь пусть k — произвольное поле и $a \in k$. Рассмотрим фактор-кольцо $k[x]/(x-a)$ кольца многочленов над k по линейному многочлену $x-a$. Аналогичные рассуждения показывают, что в каждом классе из фактор-кольца найдется единственный многочлен степени не выше 1, то есть, фактически, элемент k. Для того, чтобы найти этот представитель в классе $\overline{g}$ для произвольного $g \in k[x]$, нужно поделить g на $(x-a)$ с остатком;

но остаток от деления g на $(x-a)$ по теореме Безу равен $g(a)$. Иными словами, у всех многочленов из одного класса эквивалентности одинаковое значение в точке a. Нетрудно видеть, что сложение и умножение классов соответствует сложению и умножению этих значений.

Этот пример можно описать по-другому, используя теорему о гомоморфизме. Для поля k и элемента $a \in k$ рассмотрим **гомоморфизм эвалюации** $\mathrm{ev}_a \colon k[x] \to k$, сопоставляющий каждому многочлену $g \in k[x]$ его значение $g(a)$ в точке a. Это действительно гомоморфизм — значение суммы многочленов в точке равно сумме значений, а значение произведения — произведению значений. По теореме о гомоморфизме $k[x]/\operatorname{Ker}(\mathrm{ev}_a) \cong \operatorname{Im}(\mathrm{ev}_a)$. Но ядро гомоморфизма эвалюации состоит из всех многочленов, обращающихся в 0 в точке a, то есть (по теореме Безу), из всех многочленов, делящихся на $(x-a)$. Стало быть, $\operatorname{Ker}(\mathrm{ev}_a) = (x-a)$. С другой стороны, гомоморфизм эвалюации сюръективно (нетрудно придумать многочлен, принимающий любой наперед заданное значение в точке a; например, многочлен нулевой степени), поэтому $\operatorname{Im}(\mathrm{ev}_a) = k$. Получили, что $k[x]/(x-a) \cong k$.

В двух рассмотренных примерах фактор-кольцо $k[x]/(f)$ оказалось полем. Нетрудно понять, что в общем случае оно совершенно не обязано быть полем. Например, если профакторизовать $\mathbb{R}[x]$ по идеалу, порожденному многочленом $x^2-1 = (x-1)(x+1)$, то классы $\overline{x-1}$ и $\overline{x+1}$ ненулевые, однако же их произведение равно $\overline{(x-1)(x+1)} = \overline{0}$. В поле такого точно не бывает. Неприятности в этом примере возникают из-за того, что многочлен x^2-1 раскладывается на множители над исходным полем $\mathbb{R}[x]$. Оказывается, это единственное препятствие, из-за которого фактор-кольцо $k[x]/(f)$ не может быть полем.

Определение 2.4.1. Многочлен $f \in k[x]$ называется **неприводимым**, если его нельзя представить в виде произведения $f = gh$ двух многочленов, ни один из которых не является константой (то есть, многочленом степени 0).

Теорема 2.4.2. *Пусть k — поле, $f \in k[x]$. Фактор-кольцо $k[x]/(f)$ является полем тогда и только тогда, когда f неприводим.*

Доказательство. Как мы уже заметили, если f приводим, то в $k[x]/(f)$ есть делители нуля (а именно, если $f = gh$, то ненулевые классы $\overline{g}$ и $\overline{h}$ дают в произведении $\overline{0}$), поэтому оно не может быть полем.

Обратно, предположим, что f неприводим. Нам нужно показать, что у каждого ненулевого класса есть обратный. Пусть $a \in k[x]$ — канонический представитель этого класса, то есть, ненулевой многочлен степени меньшей, чем степень f. Заметим, что a и f взаимно просты. Действительно, если d — какой-то их общий делитель, то, во-первых, степень d меньше, чем степень f (поскольку a делится на d) и, во-вторых, f делится на d. Из неприводимости f следует, что d имеет степень 0.

По теореме о линейном представлении наибольшего общего делителя теперь найдутся многочлены s и t такие, что $as + ft = 1$. Но это означает, что $as \sim 1$, то есть, $\overline{a} \cdot \overline{s} = \overline{1}$, и $\overline{s}$ есть искомый обратный остаток к классу $\overline{a}$. □

Упражнение 2.4.3. *Пусть $x^2 + px + q$ — многочлен над $\mathbb{R}$ с отрицательным дискриминантом (то есть, $p^2 - 4q < 0$). Докажите, что $\mathbb{R}[x]/(x^2+px+q) \cong \mathbb{C}$.*

Теорема 2.4.4 (Универсальное свойство фактор-кольца). *Пусть $f \colon R \to S$ — гомоморфизм колец, $I \trianglelefteq R$ — некоторый идеал в R, и $f(I) = 0$ (иными словами, $I \subseteq \operatorname{Ker}(f)$). Тогда существует единственный гомоморфизм колец $\widetilde{f} \colon R/I \to S$ такой, что композиция $R \to R/I \to S$ совпадает с f: $\widetilde{f} \circ \pi_I = f$. Иными словами, любой гомоморфизм f с $I \subseteq \operatorname{Ker}(f)$ пропускается через каноническую проекцию π_I.*

Доказательство. Положим $\widetilde{f}(\overline{a}) = f(a)$; это определение корректно, так как если $\overline{a} = \overline{b}$, то $a - b \in I \subseteq \mathrm{Ker}(f)$, откуда $f(a) = f(b)$. Нетрудно проверить (упражнение!), что $\widetilde{f}$ является гомоморфизмом колец, и очевидно, что $\widetilde{f} \circ \pi_I = f$. Более того, последнее условие означает, что $\widetilde{f}(\overline{a}) = f(a)$, поэтому $\widetilde{f}$ единственный. □

2.5 Поле частных

Проведем конструкцию, аналогичную построению рациональных чисел по целым, для широкого класса колец. Пусть R — кольцо без делителей нуля (то есть, для $x, y \in R$ из $xy = 0$ следует, что $x = 0$ или $y = 0$). Рассмотрим множество пар (a, b) элементов из R таких, что $b \neq 0$: пусть $T = R \times (R \setminus \{0\}) = \{(a, b) \mid b \neq 0\}$. Эти пары мы сейчас превратим в [формальные] дроби a/b с помощью естественного отношения эквивалентности: пусть $(a, b) \sim (c, d)$ если и только если $ad = bc$. Нетрудно проверить, что это действительно отношение эквивалентности. К примеру, если $(a, b) \sim (c, d)$ и $(c, d) \sim (e, f)$, то $ad = bc$ и $cf = de$, откуда $adf = bcf = bde$, поэтому $d(af - be) = 0$, и, пользуясь отсутствием делителей нуля, получаем, что $af = be$, то есть, $(a, b) \sim (e, f)$.

Теперь можно рассмотреть фактор-множество множества T по этому отношению эквивалентности: положим $\mathrm{Frac}(R) = T/\sim$. Пока это просто множество, но нетрудно понять, как ввести на нем операции, чтобы оно превратилось в поле. Нужно вспомнить, как выглядят арифметические операции над дробями: $\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(ac, bd)}$ и $\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)}$; и $bd \neq 0$, поскольку $b \neq 0$, $d \neq 0$, и в R нет делителей нуля.

Упражнение 2.5.1. *Проверьте, что эти операции превращают* $\mathrm{Frac}(R)$ *в поле.* **Указание:** $0 = (0, b)$, $1 = (b, b)$, $-\overline{(a, b)} = \overline{(-a, b)}$, $\overline{(a, b)}^{-1} = \overline{(b, a)}$.

Построенное поле $\mathrm{Frac}(R)$ называется **полем частным** кольца R. Заметим, что отображение $R \to \mathrm{Frac}(R)$, $x \mapsto \overline{(x, 1)}$ задает инъективный гомоморфизм колец, называемый **каноническим вложением**. Сформулируем его универсальное свойство.

Теорема 2.5.2 (Универсальное свойство поля частных). *Пусть* R *— кольцо без делителей нуля. Обозначим через* i *каноническое вложение* R *в его поле частных* $\mathrm{Frac}(R)$*. Для любого гомоморфизма колец* $f\colon R \to S$ *такого, что образ любого ненулевого элемента* R *обратим в* S*, существует единственный гомоморфизм колец* $\widetilde{f}\colon \mathrm{Frac}(R) \to S$ *такой, что* $f = \widetilde{f} \circ i$*. Иными словами, любой гомоморфизм* f *с указанным свойством пропускается через* i*.*

Доказательство. Для $a, b \in R$ с $b \neq 0$ положим $\widetilde{f}(\overline{(a, b)}) = f(a)f(b)^{-1}$. Это можно сделать, поскольку по условию на f у элемента $f(b)^{-1}$ есть обратный в S. Это определение не зависит от выбора представителя в классе пар: если $\overline{(a, b)} = \overline{(c, d)}$, то $ad = bc$, откуда $f(a)f(d) = f(b)f(c)$ и, стало быть, $f(a)f(b)^{-1} = f(c)f(d)^{-1}$. После этого рутинная проверка показывает, что $\widetilde{f}$ является гомоморфизмом с необходимыми свойствами. □

Классический пример конструкции поля частных — построение рациональных чисел из целых: $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$. Нам понадобится еще один пример: возьмем $R = k[t]$ — кольцо многочленов над полем k от одной переменной. Его поле частных обозначается через $k(t)$ и называется **полем рациональных дробей** над k. Его элементы — формальные дроби вида f/g, где $f, g \in k[t]$, $g \neq 0$, и дроби можно сокращать на общие делители.

3 Расширения полей

3.1 Характеристика поля

В первом приближении теория Галуа изучает поля и гомоморфизмы между ними (говоря современным языком, категорию полей).

Заметим, что любой гомоморфизм колец $f\colon R\colon S$ между полями инъективен: действительно, его ядро должно быть идеалом в R, которых всего два; оно не может совпадать со всем R (иначе 1 переходит в 0, а не в 1), поэтому ядро нулевое. Значит, по теореме о гомоморфизме R можно отождествить с подполем $\mathrm{Im}(f)$ в S. В ситуации, когда одно поле, k, содержится в другом поле, F, мы будем говорить, что F является **расширением** k, или k является **подполем** в F. Эта ситуация будет обозначаться так: $k \subseteq F$ (иногда пишут F/k, но это чересчур похоже на факторизацию).

Самым грубым инвариантом полей является характеристика. Очевидно, что для любого поля (и даже для любого кольца с 1) k существует единственный гомоморфизм из кольца целых чисел в него: $i\colon \mathbb{Z} \to k$. Ядро этого гомоморфизма — идеал в $\mathbb{Z}$, то есть, множество вида $m\mathbb{Z}$ для некоторого $m \in \mathbb{N} \cup \{0\}$. Это число m называется **характеристикой** поля k и обозначается через $\operatorname{char} k$. Если $m = 0$, ядро тривиально, и i — вложение. Заметим, что $m \neq 1$ — иначе мы имели бы $i(1) = 0$, что невозможно по определению гомоморфизма.

Иными словами, мы смотрим на суммы 1, $1+1$, $1+1+1$, ... в поле k. Если оказалось так, что первая нулевая сумма в этой последовательности состоит из m единиц, то m — характеристика поля k; если же в этой последовательности вообще нет 0, считают, что характеристика равна нулю. Нетрудно понять, что если $k \subseteq F$, то $\operatorname{char} k = \operatorname{char} F$ (упражнение?).

Предложение 3.1.1. *Характеристика любого поля — простое число или 0.*

Доказательство. Пусть составное число $m = ab$ — характеристика поля k; это означает, что $1 + 1 + \cdots + 1 = 0$. Нетрудно видеть, что сумма из m единиц, стоящая в левой части, равна $(1 + 1 + \cdots + 1) \cdot (1 + 1 + \cdots + 1)$. Все происходит в поле, а там нет делителей нуля; поэтому хотя бы одна из скобок равна 0, а это означает, что характеристика k на самом деле меньше m. □

Посмотрим на наименьшее подполе поле k; оно должно содержать 0, 1, и, следовательно, все суммы вида $1 + 1 + \cdots + 1$. Если $\operatorname{char} k = p > 0$, то таких сумм конечное число и они образуют подполе в k, изоморфное полю из p элементов, которое мы будем обозначать через $\mathbb{F}_p$ (а не $\mathbb{Z}/p\mathbb{Z}$. Если же $\operatorname{char} k = 0$, то кроме всех сумм $1+1+\cdots+1$, соответствующих натуральным числам, должны быть еще их разности (и, стало быть, целые числа) и их частные (рациональные числа). В этом случае можно считать, что k содержит подполе, изоморфное полю рациональных чисел $\mathbb{Q}$. Полученное подполе (изоморфное $\mathbb{Q}$ в случае характеристики 0 и $\mathbb{F}_p$ в случае характеристики p) называется **простым подполем** поля k.

Сказанное можно уточнить: если $\operatorname{char} k = 0$, то отображение $i\colon \mathbb{Z} \to k$ инъективно, поэтому образ любого ненулевого элемента обратим. Значит, можно применить к нему универсальное свойство поля частных и получить гомоморфизм $\widetilde{i}\colon \mathbb{Q} \to k$. Поскольку $\mathbb{Q}$ и k — поля, $\widetilde{i}$ является вложением. Если же $\operatorname{char} k = p > 0$, то ядро отображения i равно $p\mathbb{Z}$ и к нему можно применить универсальное свойство фактор-кольца $\mathbb{Z}/p\mathbb{Z}$. Получаем гомоморфизм $\widetilde{i}\colon \mathbb{Z}/p\mathbb{Z}$, который и в этом случае оказывается вложением.

Простое подполе, таким образом, является *минимальным* (по включению) подполем k: понятно, что любое поле обязано содержать 1, $1+1$, $1+1+1$, ..., и, стало быть, все простое подполе.

3.2 Степень расширения

В любом расширении полей $k \subseteq F$ поле F является векторным пространством над полем k, поэтому интересно посмотреть на его размерность. Говорят, что расширение $k \subseteq F$ является **конечным** и имеет **степень** n, если размерность F как векторного пространства над k равна n. Обозначение: $[F : k] = n$. В случае бесконечной степени мы пишем $[F : k] = \infty$.

Самый главный пример конечного расширения — фактор-кольцо $k[t]/(f(t))$ кольца многочленов по идеалу, порожденному одним многочленом $f(t)$. Его элементы — «остатки» по модулю $f(t)$. Если многочлен $f(t)$ *неприводим*, то $k[t]/(f(t))$ является полем, расширением k. Его ценность состоит в том, что в этом поле исходный многочлен f имеет корень (класс многочлена t). Степень этого расширения равна степени многочлена f: действительно, если $n = \deg(f)$, то классы элементов $1, t, t^2, \dots, t^{n-1}$ образуют его базис, поскольку любой остаток можно единственным образом представить как их линейную комбинацию. При некоторых условиях *любое* конечное расширение k имеет такой вид (однако, это не всегда так).

Пусть $k \subseteq F$ — расширение полей, и $\alpha \in F$. Наименьшее подполе F, содержащее одновременно поле k и элемент α, обозначается через $k(\alpha)$. Как всегда в аналогичных ситуациях, несложно показать его существование: это просто пересечение *всех* подполей F, содержащих k и α. Расширение $k \subseteq F$ называется **простым**, если существует элемент $\alpha \in F$ такой, что $F = k(\alpha)$.

Приведенное выше расширение $k[t]/(f(t))$ для неприводимого многочлена f является простым: положим $\alpha = \bar{t}$ — класс элемента t; тогда $k[t]/(f(t)) = k(\alpha)$, поскольку любое поле, содержащее k и $\bar{t}$, должно содержать и все многочлены от t с коэффициентами из k, то есть, совпадать со всем $k[t]/(f(t))$.

Предложение 3.2.1. *Пусть* $k \subseteq k(\alpha)$ *— простое расширение. Рассмотрим* **гомоморфизм эвалюации** $\mathrm{ev}_\alpha \colon k[t] \to k(\alpha)$*, определенный формулой* $f \mapsto f(\alpha)$*. Тогда*

1. ev_α *инъективно тогда и только тогда, когда расширение* $k(\alpha)$ *бесконечно. В этом случае* $k(\alpha)$ *изоморфно полю рациональных функций* $k(t)$ *от одной переменной* t*.*

2. ev_α *не инъективно тогда и только тогда, когда расширение* $k(\alpha)$ *конечно. В этом случае существует единственный (с точностью до скалярного множителя) неприводимый многочлен* $p \in k(t)$ *степени* $n = [k(\alpha) : k]$ *такой, что* $k(\alpha) \cong k[t]/(p(t))$*. При этом изоморфизме* α *переходит в класс многочлена* t*. Многочлен* p *можно охарактеризовать как многочлен наименьшей степени такой, что* $p(\alpha) = 0$ *в* $k(\alpha)$*.*

Доказательство. По теореме о гомоморфизме образ отображения ev_α изоморфен $k[t]/\operatorname{Ker}(\mathrm{ev}_\alpha)$; при этом $\operatorname{Ker}(\mathrm{ev}_\alpha)$ является идеалом в $k[t]$. Он, как и любой идеал в $k[t]$, порождается одним элементом $p \in k[t]$.

Предположим сначала, что этот идеал (и порождающий его элемент) нулевой. Тогда отображение ev_α можно продолжить до гомоморфизма $k(t) \to k(\alpha)$ из поля частных кольца $k[t]$. Образ $k(t)$ при этом гомоморфизме является полем, содержащим k и α; поэтому он совпадает с $k(\alpha)$. При этом в силу инъективности ev_α степени α^0, α^1, ... линейно независимы над k. Значит, расширение $k \subseteq F$ бесконечно.

Пусть теперь p ненулевой. Мы знаем, что если многочлен p приводим, то в факторе $k[t]/(p)$ есть делители нуля. Однако, в $k(\alpha)$ нет делителей нуля, поэтому p — неприводимый многочлен. Тогда фактор-кольцо $k[t]/(p)$ является полем, изоморфным образу

ev_α в $k(\alpha)$. Это поле содержит k и α, поэтому совпадает со всем $k(\alpha)$. В этом случае $[k(\alpha) : k] = \deg(p)$, в частности, расширения конечно. □

Многочлен p из второй части предложения называется **минимальным многочленом** элемента α над k. Сразу заметим, что минимальный многочлен элемента может зависеть от базового поля k: например, элемент $\sqrt{2} \in \mathbb{C}$ имеет минимальный многочлен $t^2 - 2$ над $\mathbb{Q}$, и $t - \sqrt{2}$ над $\mathbb{R}$.

Вообще, чтобы задать гомоморфизм из кольца многочленов $k[t]$ в произвольное кольцо R, достаточно задать образ одного многочлена t. После этого образы всех остальных многочленов определяются однозначно из условия гомоморфизма. Рассмотрим, к примеру, гомоморфизм $f\colon \mathbb{Q}[t] \to \mathbb{R}$, переводящий t в $\sqrt{2}$. При этом гомоморфизме многочлен $t^2 - 2$ переходит в $0 \in \mathbb{R}$, поэтому идеал, порожденный $t^2 - 2$, лежит в ядре f. По теореме 2.4.4 гомоморфизм f пропускается через $\mathbb{Q}[t]/(t^2 - 2)$: существует $\widetilde{f}\colon \mathbb{Q}[t]/(t^2 - 2) \to \mathbb{R}$, композиция которого с проекцией равна f. Теперь это гомоморфизм полей, поэтому $\widetilde{f}$ инъективен, и образ отображения $\widetilde{f}$ равен $\mathbb{Q}(\sqrt{2})$.

Заметим, что существует и другое вложение $\mathbb{Q}[t]/(t^2 - 2) \to \mathbb{R}$: достаточно отправить t в $-\sqrt{2}$. Дело в том, что у многочлена $t^2 - 2$ два корня в $\mathbb{R}$. Впрочем, в нашем случае образы этих гомоморфизмов совпадают (и равны $\mathbb{Q}(\sqrt{2})$). В общем случае и это не обязано выполняться: рассмотрим многочлен $t^3 - 2$, имеющий в $\mathbb{C}$ три корня. Каждый из них задает вложение $\mathbb{Q}[t]/(t^3 - 2) \to \mathbb{C}$, образы которых — три *различных* подполя в $\mathbb{C}$, каждое из которых изоморфно $\mathbb{Q}[t]/(t^3 - 2)$.

3.3 Продолжение изоморфизма для простых расширений

Предложение 3.3.1. *Пусть $k_1 \subseteq k_1(\alpha_1)$, $k_2 \subseteq k_2(\alpha_2)$ — два простых конечных расширения полей, $p_1 \in k_1[t]$, $p_2 \in k_2[t]$ — минимальные многочлены элементов α_1, α_2 соответственно. Пусть $i\colon k_1 \to k_2$ — изоморфизм полей такой, что $i(p_1) = p_2$ (то есть, соответствующие коэффициенты многочленов p_1 и p_2 переводятся друг в друга при изоморфизме i). Тогда существует единственный изоморфизм $j\colon k_1(\alpha_1) \to k_2(\alpha_2)$ такой, что $j|_{k_1} = i$ и $j(\alpha_1) = \alpha_2$.*

Доказательство. Изоморфизм i продолжается до изоморфизма $k_1[t] \to k_2[t]$. Рассмотрим композицию $k_1[t] \to k_2[t] \to k_2[t]/(p_2)$, где второе отображение — каноническая проекция на фактор-кольцо. Очевидно, что ядро этой композиции совпадает с идеалом $(p_1) \trianglelefteq k_1[t]$. По универсальному свойству фактор-кольца она пропускается через отображение $k_1[t] \to k_1[t]/(p_1)$. Мы построили гомоморфизм $k_1[t]/(p_1) \to k_2[t]/(p_2)$. Он автоматически инъективный, и сюръективный, поскольку второе поле порождается классом многочлена t, который лежит в образе гомоморфизма. Поэтому это изоморфизм; кроме того, очевидно, что при нем класс $\bar{t}$ соответствует классу $\bar{t}$. Но по предложению 3.2.1 $k_1[t]/(p_1)$ изоморфно $k_1(\alpha_1)$, а $k_2[t]/(p_2)$ изоморфно $k_2(\alpha_2)$, причем при этих изоморфизмах $\bar{t}$ соответствует α_1, и $\bar{t}$ соответствует α_2. Композиция трех изоморфизмов теперь дает нужный изоморфизм j. Единственность следует из того, что любой гомоморфизм $k_1(\alpha_1)$ в $k_2(\alpha_2)$, совпадающий с i на k_1, задается выбором образа α_1. □

Определение 3.3.2. Пусть $k \subseteq F$ — расширение полей, и $\alpha \in F$. Элемент α называется **алгебраическим над k, степени n**, если $n = [k(\alpha) : k]$ конечно; в противном случае α называется **трансцендентным над k**.

Расширение $k \subseteq F$ называется **алгебраическим**, если любой его элемент алгебраичен над k.

По предложению 3.2.1 элемент $\alpha \in F$ алгебраичен над k тогда и только тогда, когда существует ненулевой многочлен $f \in k[x]$ такой, что $f(\alpha) = 0$. Минимальный многочлен α — это многочлен наименьшей степени, для которого выполнено это условие, и со старшим коэффициентом 1; он обязан быть неприводимым. Заметим, что если α алгебраичен над k, то любой элемент $k(\alpha)$ может быть записан как многочлен от α с коэффициентами из k.

3.4 Теорема о размерности башни

Конечные расширения являются алгебраическими:

Лемма 3.4.1. *Пусть расширение $k \subseteq F$ конечно. Тогда любой элемент $\alpha \in F$ алгебраичен над k, степени $\leqslant [F : k]$.*

Доказательство. В цепочке расширений $k \subseteq k(\alpha) \subseteq F$ размерность $k(\alpha)$ как векторного пространства над k ограничена сверху числом $\dim_k(F) = [F : k]$. □

Иными словами, если расширение $k \subseteq F$ конечно и $\alpha \in F$, то степени $1, \alpha, \alpha^2, \dots$ обязаны быть линейно зависимыми, и любая их нетривиальная линейная комбинация, равная 0, дает ненулевой многочлен $f \in k[x]$, для которого $f(\alpha) = 0$.

Постараемся найти адекватное «обратное» к утверждению «любое конечное расширение алгебраично».

Предложение 3.4.2. *Пусть $k \subseteq E \subseteq F$ — расширения полей. Расширение $k \subseteq F$ конечно тогда и только тогда оба расширения $k \subseteq E$ и $E \subseteq F$ конечны; в этом случае $[F : k] = [F : E] \cdot [E : k]$.*

Доказательство. Если F — конечномерное векторное пространство над k, то E — его подпространство, поэтому тоже конечномерно. Кроме того, любая линейная зависимость элементов F над k является и линейной зависимостью над E. Поэтому из конечности $k \subseteq F$ следует конечность $k \subseteq E$ и $E \subseteq F$.

Обратно, предположим, что $k \subseteq E$ и $E \subseteq F$ — конечные расширения. Пусть $(e_1, \dots, e_m)$ — базис E над k, а $(f_1, \dots, f_n)$ — базис F над E. Покажем, что mn произведений $(e_i f_j)_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n} = (e_1 f_1, e_1 f_2, \dots, e_m f_n)$ образуют базис F над k. Возьмем $g \in F$. Найдутся $d_1, \dots, d_n \in E$ такие, что $g = \sum_{j=1}^{n} d_j f_j$, поскольку f_j порождают F над E. Кроме того, E порождается элементами e_i над k, поэтому для каждого j найдутся элементы $c_{1j}, \dots, c_{mj}$ такие, что $d_j = \sum_{i=1}^{m} c_{ij} e_i$. Подставляя эти равенства в выражения для g, получаем, что $g = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} e_i f_j$, поэтому $e_i f_j$ — система образующих F над k.

Теперь покажем, что они линейно независимы. Пусть $\sum_{i,j} l_{ij} e_i f_j = 0$ для некоторых $l_{ij} \in k$. Тогда $\sum_j (\sum_i l_{ij} e_i) f_j = 0$. Из этого следует, что $\sum_i l_{ij} e_i = 0$ для каждого j, поскольку f_j линейно независимы над E. Но e_i линейно независимы над k, поэтому из этих равенств следует, что все l_{ij} равны 0. □

Пример 3.4.3. Пусть $k \subseteq F$ — расширение полей, и $\alpha \in F$ — алгебраический над k элемент нечетной степени. Тогда α можно записать как многочлен от α^2 с коэффициентами из k.

Действительно, $\alpha^2 \in k(\alpha)$, поэтому $k \subseteq k(\alpha^2) \subseteq k(\alpha)$. Чему может равняться степень $k(\alpha)$ над $k(\alpha^2)$? Элемент α является корнем многочлена $t^2 - \alpha^2$ с коэффициентами из $k(\alpha^2)$, поэтому $[k(\alpha) : k(\alpha^2)] \leqslant 2$. С другой стороны, произведенеие $[k(\alpha^2) : k] \cdot [k(\alpha) : k(\alpha^2)]$ нечетно, поэтому степень $k(\alpha)$ над $k(\alpha^2)$ равна 1, и $k(\alpha) = k(\alpha^2)$. В частности, $\alpha \in k(\alpha^2)$.

3.5 Конечно порожденные расширения

Определение 3.5.1. Расширение полей $k \subseteq F$ называется **конечно порожденным**, если существуют $\alpha_1, \ldots, \alpha_n \in F$ такие, что $F = k(\alpha_1)(\alpha_2)\ldots(\alpha_n)$.

Часто мы будем писать $k(\alpha_1, \ldots, \alpha_n)$ вместо $k(\alpha_1)(\alpha_2)\ldots(\alpha_n)$. Если $k \subseteq F$ и $\alpha_1, \ldots, \alpha_n \in F$, то $k(\alpha_1, \ldots, \alpha_n)$ — наименьшее подполе в F, содержащее поле k и все элементы $\alpha_1, \ldots, \alpha_n$. Другими словами, это наименьшее подполе в F, содержащее поля $k(\alpha_1)$, $k(\alpha_2)$, $\ldots$, $k(\alpha_n)$. Очевидно, что порядок элементов $\alpha_1, \ldots, \alpha_n$ не имеет значения.

Предложение 3.5.2. *Пусть $k \subseteq F = k(\alpha_1, \ldots, \alpha_n)$ — конечно порожденное расширение полей. Тогда следующие три условия эквивалентны:*

1. *расширение $k \subseteq F$ конечно;*
2. *расширение $k \subseteq F$ алгебраично;*
3. *каждое α_i алгебраично над k.*

Если эти условия выполнены, то $[F : k]$ не превосходит произведения степеней элементов α_i над k.

Доказательство. $(1) \Longrightarrow (2)$ — по лемме 3.4.1; $(2) \Longrightarrow (3)$ — очевидно. Докажем $(3) \Longrightarrow (1)$. Пусть каждый элемент α_i алгебраичен над k степени d_i. Тогда расширение $k(\alpha_1, \ldots, \alpha_{i-1}) \subseteq k(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i)$ конечное степени не выше d_i: действительно, мы знаем, что α_i является корнем многочлена степени d_i с коэффициентами из k, поэтому его минимальный многочлен над $k(\alpha_1, \ldots, \alpha_{i-1})$ имеет степень не выше d_i. Теперь применим теорему о размерности башни к последовательности расширений $k \subseteq k(\alpha_1) \subseteq k(\alpha_1, \alpha_2) \subseteq \cdots \subseteq k(\alpha_1, \ldots, \alpha_n) = F$. Получаем, что $k \subseteq F$ конечно и $[F : k] \leqslant d_1 \ldots d_n$. □

3.6 Алгебраические расширения

Из этого предложения следуют замечательные вещи: например, если α и β алгебраичны над k, то $\alpha + \beta$, $\alpha\beta$ и α/β также алгебраичны над k. Отсюда немедленно следует, что множество всех алгебраических элементов в любом расширении образует поле.

Таким образом, для конечно порожденных расширений конечность равносильна алгебраичности.

Пример 3.6.1. Рассмотрим расширение $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. По предыдущему предложению оно алгебраично. В частности, число $\sqrt{2} + \sqrt{3}$ должно являться корнем какого-то многочлена с рациональными коэффициентами. Можно найти этот многочлен так: обозначим $\alpha = \sqrt{2} + \sqrt{3}$, тогда $\alpha^2 = 5 + 2\sqrt{6}$, $\alpha^3 = 11\sqrt{2} + 9\sqrt{3}$, $\alpha^4 = 49 + 20\sqrt{6}$. Видно, что появилась линейная зависимость: $\alpha^4 - 10\alpha^2 + 1 = 0$, поэтому $t^4 - 10t^2 + 1$ — искомый многочлен. На самом деле это минимальный многочлен элемента α: легко проверить, что все его корни — это $\pm\sqrt{2} \pm \sqrt{3}$. Теперь рассмотрим башню расширений $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Мы поняли, что степень $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ над $\mathbb{Q}$ равна 4. Но по предыдущему предложению степень $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ не превосходит 4. Значит, обе эти степени равны 4 и $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Кроме того, алгебраическое расширение алгебраического расширения является алгебраическим (даже без условия конечной порожденности):

Предложение 3.6.2. *Пусть $k \subseteq E \subseteq F$ — расширения полей. Тогда $k \subseteq F$ алгебраично если и только если $k \subseteq E$ и $E \subseteq F$ алгебраичны.*

Доказательство. Если $k \subseteq F$ алгебраично, то любой элемент F алгебраичен над k; в частности, любой элемент E алгебраичен над k, поэтому E алгебраично над k. Кроме того, любой элемент F является корнем многочлена с коэффициентами из k, следовательно, и корнем многочлена с коэффициентами из E. Поэтому и F алгебраично над E.

Обратно, пусть E алгебраично над k и F алгебраично над E. Возьмем $\alpha \in F$. По предположению он является корнем некоторого многочлена с коэффициентами из E. Запишем этот многочлен: $x^n + e_{n-1}x^{n-1} + \cdots + e_1x + e_0$. Значит, α алгебраичен уже над подполем $k(e_0, \ldots, e_{n-1}$ в E. Получаем, что расширение $k(e_0, \ldots, e_{n-1}) \subseteq k(e_0, \ldots, e_{n-1}, \alpha)$ является конечным. Далее, расширение $k \subseteq k(e_0, \ldots, e_{n-1})$ алгебраическое, поскольку каждый его элемент содержится в E, и, следовательно, также конечное. Применим теперь теорему а размерности башни к цепочке конечных расширений $k \subseteq k(e_0, \ldots, e_{n-1}) \subseteq k(e_0, \ldots, e_{n-1}, \alpha)$; получим, что расширение $k(e_0, \ldots, e_{n-1}, \alpha)$ конечно, и, следовательно, алгебраично над k. Это означает, что α алгебраичен над k, что и требовалось. □

Для доказательства неприводимости многочленов над $\mathbb{Q}$ часто используется следующий критерий.

Теорема 3.6.3 (Критерий Эйзенштейна). *Пусть $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ — многочлен с целыми коэффициентами, и p — простое число такое, что a_i делится на p для всех i и a_0 не делится на p^2. Предположим, что $f = gh$ для некоторых многочленов g и h с целыми коэффициентами. Тогда g или h имеет степень 0.*

Доказательство. Пусть $\deg(g) = k$, $\deg(h) = n - k$, и $k, n - k < n$. Запишем $g = b_kx^k + \cdots + b_0$, $h = c_{n-k}x^{n-k} + \cdots + c_0$. По условию $b_0c_0 = a_0$ делится на p, но не делится на p^2. Значит, ровно одно из чисел b_0, c_0 делится на p. Без ограничения общности можно считать, что b_0 делится на p, а c_0 не делится на p. Посмотрим, сколько младших коэффициентов многочлена g делится на p: пусть l — натуральное число такое, что $b_0, \ldots, b_{l-1}$ делятся на p, а b_l не делится на p. Такое число l найдется (на самом деле, $l \leqslant k$) поскольку $b_kc_{n-k} = 1$, и, следовательно, b_k не делится на p. Теперь посмотрим на $a_l = b_0c_l + \cdots + b_{l-1}c_1 + b_lc_0$. По условию a_l делится на p (поскольку $l \leqslant k < n$), и в правой части все слагаемые, кроме последнего, делятся на p. Но последнее слагаемое, b_lc_0, не делится на p — противоречие. □

Приведем пример бесконечного алгебраического расширения. Рассмотрим множество всех комплексных чисел, алгебраических над $\mathbb{Q}$: $\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid z \text{ алгебраично над } \mathbb{Q}\}$. Мы знаем, что сумма, разность, произведение и частное алгебраических чисел алгебраичны, поэтому $\overline{\mathbb{Q}}$ является полем (подполем в $\mathbb{C}$). Расширение $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$, очевидно, алгебраично, но не может быть конечным. Действительно, предположим, что $[\overline{\mathbb{Q}} : \mathbb{Q}] = n$ и рассмотрим число $\sqrt[p]{2}$ для простого p. Очевидно, что это алгебраическое число, поэтому $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[p]{2}) \subseteq \overline{\mathbb{Q}}$ — цепочка расширений полей. Нетрудно видеть, что $\sqrt[p]{2}$ является корнем многочлена $t^p - 2 \in \mathbb{Q}[t]$, неприводимого по критерию Эйзенштейна, поэтому $[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = p$, и по теореме о размерности башни n делится на p. Но натуральное число n не может делиться на все простые числа p — получаем противоречие.

Поле $\overline{\mathbb{Q}}$ называется **полем алгебраических чисел**.

Определение 3.6.4. Пусть $k \subseteq F$ — расширение полей. Множество гомоморфизмов $j\colon F \to F$ таких, что $j|_k = \mathrm{id}_k$ (то есть, $j(a) = a$ для всех $a \in k$), называется **группой автоморфизмов расширения** и обозначается через $\mathrm{Aut}_k(F)$.

Замечание 3.6.5. Мы пока не знаем, что такое «группа», но $\mathrm{Aut}_k(F)$ действительно будет группой относительно композиции гомоморфизмов.

3.7 Приложение: построения циркулем и линейкой

Одним из первых достижений теории расширений полей стало решение (отрицательное) трех классических задач древности на построение циркулем и линейкой. Это квадратура круга, трисекция угла и удвоение куба:

1. **квадратура круга**: построить квадрат, площадь которого равна площади данного круга;
2. **трисекция угла**: разделить данный угол на три данных части;
3. **удвоение куба**; построить отрезок, равный стороне куба, объем которого вдвое больше объема куба с данной стороной.

Для того, чтобы показать, что эти операции невозможно выполнить циркулем и линейкой, необходимо прежде всего формализовать само понятие построения циркулем и линейкой. **Алгоритмом** построения циркулем и линейкой будем называть описание конечной последовательности действий, каждое из которых является одним из **элементарных построений**. Опишем теперь, какие бывают элементарные построения:

1. *Провести прямую через две точки*: если на плоскости уже отмечены две точки, разрешается провести через них прямую.
2. *Найти точку пересечения двух прямых*: если на плоскости уже проведены две прямые, разрешается отметить их точку пересечения (если она есть).
3. *Провести окружность с центром в данной точке заданным радиусом*: если на плоскости отмечены точки A и B, разрешается построить окружность с центром в точке A и радиусом AB.
4. *Найти точку пересечения прямой и окружности*: если на плоскости проведены прямая и окружность, разрешается отметить их точки пересечения.
5. *Найти точку пересечения двух окружностей*: если на плоскости проведены две окружности, разрешается отметить их точки пересечения.

Предположим, что на плоскости выбрана декартова система координат, то есть построены две перпендикулярные оси и на одной из них отмечен единичный отрезок. Посмотрим на координаты всех точек, которые отмечаются в процессе выполнения алгоритма построения.

Когда мы отмечаем точку пересечения двух прямых, каждая из этих прямых построена посредством операции 1, поэтому можно считать, что мы отмечаем точку пересечения прямых AB и CD, где A, B, C, D — ранее отмеченные точки. Пусть их координаты — (x_A, y_A), (x_B, y_B), (x_C, y_C), (x_D, y_D) соответственно. Тогда прямая AB задается уравнением $x(y_A - y_B) - y(x_A - x_B) + (x_A y_B - y_A x_B) = 0$. Для сокращения обозначений будем считать, что это уравнение $ax + by + c = 0$. Аналогично, прямая CD задается уравнением $x(y_C - y_D) - y(x_C - x_D) + (x_C y_D - y_C x_D) = 0$, и мы будем считать, что это уравнение $a'x + b'y + c' = 0$. Точка пересечения (x, y) этих прямых имеет координаты, удовлетворяющие системе уравнений

$$\begin{cases} ax + by + c = 0; \\ a'x + b'y + c' = 0. \end{cases}$$

Решение выглядит так: $x = (bc' - b'c)/(ab' - a'b)$, $y = (a'c - ac')/(ab' - a'b)$. Нам важно только то, что координаты (x, y) новой отмеченной точки есть рациональные функции

от a, b, c, a', b', c'. В свою очередь, a, b, c, a', b', c' есть рациональные функции (и даже многочлены) от координат точек A, B, C, D. Поэтому координаты новой точки являются рациональными выражениями от координат точек A, B, C, D.

Теперь разберем случай пересечения прямой и окружности. Как и раньше, пусть прямая AB задается уравнением $ax + by + c = 0$, где a, b, c — многочлены от координат точек A и B. Окружность с центром в отмеченной точке C и радиусом CD (D — также отмеченная точка) задается уравнением $(x-x_C)^2+(y-y_C)^2 = (x_D-x_C)^2+(y_D-y_D)^2$. Нас интересует решение полученной системы

$$\begin{cases} ax + by + c = 0; \\ (x - x_C)^2 + (y - y_C)^2 = (x_D - x_C)^2 + (y_D - y_D)^2. \end{cases}$$

Если $b \neq 0$, в первом уравнении можно выразить y через x (иначе $a \neq 0$, и можно выразить x через y — этот случай симметричен нашему). Подставляя полученное выражение во второе уравнение, мы получаем одно квадратичное уравнение $kx^2 + lx + m = 0$ относительно x, коэффициенты k, l, m которого, как нетрудно видеть, являются рациональными функциями от координат исходных точек A, B, C, D. Корни этого уравнения имеют вид $x = (-l \pm \sqrt{l^2 - 4km})/(2k)$, и y после этого линейно выражается через x (коэффициенты этого выражения — также рациональные функции от координат точек A, B, C, D). Мы видим, что в этом случае координаты новой отмеченной точки уже не являются рациональными функциями от координат исходных; однако они являются рациональными функциями от координат исходных точек и от $\sqrt{\alpha}$, где $\alpha = l^2 - 4km$ — снова рациональная функция от координат точек A, B, C, D. При этом $\alpha \geqslant 0$ (иначе точек пересечения вовсе нет).

Осталось рассмотреть случай пересечения двух окружностей. Пусть окружности заданы уравнениями

$$\begin{cases} (x - x_A)^2 + (y - y_A)^2 = (x_B - x_A)^2 + (y_B - y_A)^2, \\ (x - x_C)^2 + (y - y_C)^2 = (x_D - x_C)^2 + (y_D - y_C)^2. \end{cases}$$

Нетрудно видеть, что разность этих двух уравнений является линейным уравнением относительно x и y, коэффициенты которого — рациональные функции от координат точек A, B, C, D; поэтому система из этих двух уравнений эквивалентная системе, в которой одно из уравнений такое же, как и прежде, а второе — линейное. Таким образом, этот случай сводится к предыдущему, и вывод остается таким же — координаты новой точки рационально выражаются через координаты исходных и квадратный корень от рациональной функции тех же координат.

Рассмотрим теперь минимальное поле K_i, в котором лежат координат всех точек, отмеченных после выполнения i шагов алгоритма. Наш разбор показал, что с каждым шагом это поле либо не изменяется, либо расширяется посредством добавления квадратного корня из элемента прежнего поля. Первоначально отмечены только точки $(0, 0)$ и $(1, 0)$, поэтому $K_0 = \mathbb{Q}$.

На самом деле, мы пропустили еще одно элементарное построение, которое не так просто формализовать — это возможность отметить «произвольную» точку на плоскости. Более того, можно потребовать, чтобы эта точка удовлетворяла каким-то ограничениям — например, лежала вне или внутри построенной окружности, или по заданную сторону от построенной прямой, или на заданном отрезке (с концами в отмеченных точках), или на заданной дуге построенной окружности, или даже каким-то комбинациям этих ограничений. Покажем, что это новое построение не добавляет ничего нового к нашему выводу относительно строения полей K_i. Ключевое соображение состоит в том, что точки с рациональными координатами всюду плотны на плоскости (и в любой открытой области

плоскости), а прямые, уравнения которых имеют рациональные коэффициенты, также в некотором смысле всюду плотны: их пересечения с заданным отрезком или дугой окружности образуют всюду плотное множество точек (на отрезке или дуге). Поскольку алгоритм должен работать независимо от того, какую именно «произвольную» точку мы взяли, будем считать, что при выборе произвольной точки нам всегда попадается та, координаты которой либо рациональны, либо задаются пересечением какой-то уже построенной кривой (прямой или окружности) с прямой, уравнение которой имеет рациональные коэффициенты. Поскольку $K_0 = \mathbb{Q}$ содержится в каждом K_i, выбор такой точки не изменяет нашего заключения: каждое K_i либо совпадает с K_{i-1}, либо является его квадратичным расширением.

Наконец, будем говорить, что вещественное число α можно **построить циркулем и линейкой**, если существует алгоритм построения такой, что в результате его работы на декартовой плоскости окажется отмеченной точка с координатами $(\alpha, 0)$.

Теорема 3.7.1. *Вещественное число α можно построить циркулем и линейкой тогда и только тогда, когда существует конечная цепочка расширений полей*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n,$$

в которой для каждого i либо $K_i = K_{i-1}$, либо $K_i = K_{i-1}(\alpha_i)$ для некоторого $\alpha_i \in K_{i-1}$, $\alpha_i > 0$, и в которой $\alpha \in K_n$.

Доказательство. Предыдущие рассуждения показывают, что если α можно построить циркулем и линейкой, то такая цепочка существует (нужно взять в качестве K_i поле, порожденное координатами всех точек, отмеченных после i-го шага). Обратно, если задана такая цепочка, покажем, что α можно построить циркулем и линейкой. Это немедленно следует из того, что если мы умеем строить числа s и t, то мы умеем строить и числа $s \pm t$, st, s/t и $\sqrt{s}$. Построение суммы и разности тривиально, произведение и частное строятся с помощью теоремы Фалеса (и с учетом того, что у нас с самого начала есть отрезок длины 1). а $\sqrt{s}$ можно построить, например, как среднее геометрическое s и 1 (высота в прямоугольном треугольнике является средним геометрическим длин отрезков, на которые основание высоты делит гипотенузу). Поэтому любое наперед заданное число $\alpha \in K_n$ для такой цепочки расширений строится циркулем и линейкой за конечное число шагов. □

Теперь остается формализовать три классические задачи древности. Нетрудно видеть, что квадратура круга сводится к построению числа $\sqrt{\pi}$, удвоение куба — к построению числа $\sqrt[3]{2}$. Трисекция угла говорит о делении *произвольного* угла на три части. Мы знаем, что некоторые углы все-таки можно поделить циркулем и линейкой на три равные части — например, угол 90°, поскольку возможно построить угол в 30°. Но, к примеру, уже для угла в 30° трисекцию провести невозможно: достаточно доказать, что невозможно построить число $\sin(10^\circ)$.

Примем на веру, что число π трансцендентно. Из этого сразу следует невозможность квадратура круга: если бы могли построить $\sqrt{\pi}$, то могли бы построить и π. Однако, из теоремы 3.7.1 следует, что любое число, построимое циркулем и линейкой, является алгебраическим, поскольку расширение K_n алгебраично (поскольку все расширения $K_{i-1} \subseteq K_i$ конечны, следовательно, алгебраичны).

Пусть теперь $\alpha = \sqrt[3]{2}$. Предположим, что α можно построить циркулем и линейкой; по теореме 3.7.1 существует цепочка $\mathbb{Q} = K_0 \subseteq K_2 \subseteq \ldots \subseteq K_n$ не более чем квадратичных расширений такая, что $\alpha \in K_n$. Заметим, что степень каждого расширения в цепочке

равна 1 или 2. Значит, по теореме о размерности башни степень расширения $\mathbb{Q} \subseteq K_n$ равна 2^l. С другой стороны, если $\alpha \in K_n$, то имеется цепочка $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K_n$, в которой степень расширения $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ равна 3: действительно, α является корнем неприводимого многочлена $t^3 - 2$ степени 3 над $\mathbb{Q}$. По теореме о размерности башни $2^l = [K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(\alpha)] \cdot 3$, что невозможно, поскольку степень двойки не может делиться на 3.

Наконец, пусть $\alpha = \sin(10^\circ)$. По формуле синуса тройного угла $3\sin(10^\circ) - 4(\sin(10^\circ))^3 = \sin(30^\circ) = 1/2$. Значит, α является корнем уравнения $8t^3 - 6t + 1 = 0$. Несложные рассуждения показывают, что многочлен $8t^3 - 6t + 1$ неприводим (если бы он был приводим, у него был бы линейный множитель, то есть, существовал бы рациональный корень, а возможные рациональные корни данного многочлена легко перебрать — они должны иметь вид ± 1, $\pm 1/2$, $\pm 1/4$ или $\pm 1/8$). Поэтому расширение $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ снова имеет степень 3, и можно действовать, как в предыдущем случае.

Заметим, что некоторые углы все-таки можно построить циркулем и линейкой: к примеру,

$$\cos 3^\circ = \frac{1}{8}(\sqrt{3}+1)\sqrt{5+\sqrt{5}} + \frac{1}{16}(\sqrt{6}-\sqrt{2})(\sqrt{5}-1).$$

Из этого следует, что для целого числа n угол в n градусов можно построить циркулем и линейкой тогда и только тогда, когда n делится на 3: указанное выражение позволяет построить угол в 3 градуса, и, следовательно, все кратные ему, а если бы можно было построить угол в n градусов для n не кратного трем, то можно было бы и построить угол в 1°, и, стало быть, угол в 10°, что невозможно.

Традиционно рассматривалась и задача построения циркулем и линейкой правильного n-угольника, или, что то же самое, построения угла $2\pi/n$. На этот вопрос получен такой ответ: угол $2\pi/n$ можно построить циркулем и линейкой тогда и только тогда, когда $n = 2^l p_1 p_2 \dots p_s$, где l — некоторое натуральное число или 0, а $p_1, \dots, p_s$ — различные **простые числа Ферма**, то есть простые числа вида $p = 2^{2^k} + 1$. Известно, что для $k = 0, 1, 2, 3, 4$ эти числа (3, 5, 17, 257, 65537) действительно простые. Для $k = 5$ число $2^{32} + 1 = 4294967297$ не является простым, а равно $641 \cdot 6700417$. На сегодняшний день (март 2012) неизвестно, существуют ли другие простые числа Ферма, помимо перечисленных. Гаусс в возрасте 19 лет разработал построение циркулем и линейкой правильного 17-угольника на основе того факта, что

$$\cos(\tfrac{2\pi}{17}) = \frac{\sqrt{17}-1+\sqrt{2}\sqrt{34+6\sqrt{17}+\sqrt{2}(\sqrt{17}-1)\sqrt{17-\sqrt{17}}-8\sqrt{2}\sqrt{17+\sqrt{17}}}+\sqrt{2}\sqrt{17-\sqrt{17}}}{16}$$

Видно, что запись этого числа включает в себя только квадратные корни (хотя и вложенные), поэтому, по теореме 3.7.1, построимо циркулем и линейкой.

4 Нормальность и сепарабельность

4.1 Алгебраическое замыкание

Определение 4.1.1. Пусть $k \subseteq L$ — расширение полей. Говорят, что L является **алгебраическим замыканием** поля k, если расширение $k \subseteq L$ алгебраично и поле L алгебраически замкнуто, то есть любой многочлен степени > 0 с коэффициентами из L имеет корень в L. Такое поле L часто обозначается через $\overline{k}$.

Нам понадобятся некоторые факты, которые мы приведем без доказательства.

Теорема 4.1.2. *У любого поля k есть алгебраическое замыкание $k \subseteq \overline{k}$, единственное с точностью до изоморфизма.*

Полезное свойство алгебраического замыкания: любое алгебраическое расширение поля вкладывается в его алгебраическое замыкание (и, на самом деле, в любое алгебраически замкнутое расширение основного поля).

Предложение 4.1.3. *Пусть* $k \subseteq L$ — *расширение полей, и* L *алгебраически замкнуто. Пусть* $k \subseteq F$ — *алгебраическое расширение. Тогда существует (инъективный) гомоморфизм полей* $F \to L$ *такой, что композиция его с вложением* $k \subseteq F$ *совпадает с вложением* $k \subseteq L$.

Отметим, что описанный гомоморфизм, как правило, не является единственным: положим $k = \mathbb{Q}$, $L = \mathbb{C}$, $F = \mathbb{Q}[t]/(t^3 - 2)$; мы уже обсуждали, что есть три различных гомоморфизма $\mathbb{Q}[t]/(t^3 - 2) \to \mathbb{C}$.

Нам уже знакомы примеры алгебраических замыканий: $\overline{\mathbb{R}} = \mathbb{C}$ и замыкание поля рациональных чисел, которое мы обозначали через $\overline{\mathbb{Q}}$. Конечно, можно рассмотреть и вложение $\mathbb{Q} \subseteq \mathbb{C}$ поля рациональных чисел в алгебраически замкнутое поле $\mathbb{C}$, но оно не является алгебраическим. В $\mathbb{C}$ много трансцендентных над $\mathbb{Q}$ элементов (например, π). Более того, $\overline{\mathbb{Q}}$ счетно, в отличие от $\mathbb{C}$, поэтому в башне расширений $\mathbb{Q} \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}$ верхний этаж значительно больше нижнего.

4.2 Поле разложения

Итак, в алгебраическом замыкании поля k любой многочлен из $k[x]$ раскладывается на линейные. Предположим, что у нас есть некоторый набор многочленов $\mathcal{F} \subseteq k[x]$ и нас интересуют расширения, в которых каждый многочлен из $\mathcal{F}$ раскладывается на линейные. Конечно, $\overline{k}$ является таким расширением, но имеет смысл задача нахождения минимального расширения с этим свойством. Нам достаточно будет рассмотреть случай, когда $\mathcal{F}$ состоит из одного многочлена (на самом деле, случай конечного множества $\mathcal{F}$ сводится к этому).

Определение 4.2.1. Пусть k — поле, $f \in k[x]$ — многочлен степени d. **Полем разложения** многочлена f над k называется расширение $k \subseteq F$ такое, что $f(x) = c\prod_{i=1}^{d}(x - \alpha_i)$ в $F[x]$ и, кроме того, F порождается над k корнями многочлена f, то есть, $F = k(\alpha_1, \ldots, \alpha_d)$.

Предложение 4.2.2. *Пусть* k — *поле,* $f \in k[x]$. *Поле разложения* F *многочлена* f *существует и единственно с точностью до изоморфизма; степень расширения* $[F : k]$ *не превосходит* $(\deg(f))!$. *Более того, если* $i\colon k \to k'$ — *изоморфизм полей и* $g \in k'[x]$ *таков, что* $i(f) = g$, *то* i *продолжается до изоморфизма [любого] поля разложения* f *над* k *и [любого] поля разложения* g *над* k'.

Доказательство. Доказываем индукцией по степени многочлена f. Пусть q — какой-нибудь неприводимый множитель многочлена f. Рассмотрим расширение $k \subseteq F' = k[t]/(q)$ степени $\deg(q) \leqslant \deg(f)$. Над полем F' у многочлена f появился корень, поэтому f стал делиться на линейный множитель $(x - \alpha)$. Рассмотрим многочлен $f/(x - \alpha) \in F'[x]$. Его степень равна $\deg(f) - 1$, поэтому можно применить предположение индукции и найти расширение $F' \subseteq F$ такое, что над F многочлен $f/(x - \alpha)$ раскладывается на линейные множители. Кроме того, $[F : F'] \leqslant (\deg(f)-1)!$. Посмотрим на башню расширений $k \subseteq F' \subseteq F$; очевидно, что над F многочлен f раскладывается на $(x - \alpha)$ и на множители многочлена $f/(x - \alpha)$, то есть, целиком на линейные множители. По теореме о размерности башни имеем $[F : k] = [F : F'] \cdot [F' : k] \leqslant (\deg(f) - 1)! \cdot (\deg f) = (\deg(f))!$, что и требовалось. □

Примеры 4.2.3.

1. Легко видеть, что $\mathbb{Q}(i)$ является полем разложения многочлена $x^2 + 1$ над $\mathbb{Q}$, а $\mathbb{C}$ — полем разложения того же многочлена над $\mathbb{R}$.

2. Поле разложения многочлена $x^8 - 1$ над $\mathbb{Q}$ порождается элементом $\zeta := \cos(2\pi/8) + \sin(2\pi/8)$, поскольку корнями этого многочлена являются все корни восьмой степени из 1, и все они — степени ζ. Заметим, что ζ является корнем неприводимого над $\mathbb{Q}$ многочлена $x^4 + 1$; поэтому $F = \mathbb{Q}(\zeta)$ является полем разложения и многочлена $x^4 + 1$ над $\mathbb{Q}$. Степень расширения $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ равна 4, в то время как предыдущее предложение дает оценки 8! и 4!.

   Заметим теперь, что $i = \zeta^2 \in F$ и $\sqrt{2} = \zeta + \zeta^7 \in F$. Поэтому поле F содержит $\mathbb{Q}(i, \sqrt{2})$. Обратно, $\zeta = \sqrt{2}(1 + i)/2 \in \mathbb{Q}(i, \sqrt{2}$. Мы получили, что поле разложения $x^4 + 1$ (и поле разложения $x^8 - 1$) равно $\mathbb{Q}(i, \sqrt{2})$.

3. Посмотрим теперь на многочлен $x^4 - 1$. Он раскладывается над $\mathbb{Q}$: $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$, поэтому его поле разложения такое же, как поле разложения $x^2 + 1$, то есть, $\mathbb{Q}(i)$.

4. Различие между предыдущими двумя примерами связано не с приводимостью: посмотрим на многочлен $x^4 + 2$. Его корни — $\sqrt[4]{2}\zeta$, $\sqrt[4]{2}\zeta^3$, $\sqrt[4]{2}\zeta^5$, $\sqrt[4]{2}\zeta^7$, поэтому $K = \mathbb{Q}(\sqrt[4]{2}\zeta, \sqrt[4]{2}\zeta^3, \sqrt[4]{2}\zeta^5, \sqrt[4]{2}\zeta^7)$ — поле разложения x^4+2. Легко видеть, что $K \subseteq \mathbb{Q}(\zeta, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt{2}, \sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2}$. С другой стороны, $\sqrt{2} = (\sqrt[4]{2})\zeta)^3/(\sqrt[4]{2}\zeta^3) \in K$, поэтому $i = (\sqrt[4]{2}\zeta)^2/\sqrt{2} \in K$, $\zeta = \sqrt{2}(1+i)/2 \in K$ и $\sqrt[4]{2} = (\sqrt[4]{2}\zeta)/\zeta \in K$. Стало быть, $\mathbb{Q}(i, \sqrt[4]{2}) \subseteq K$, и поэтому поле разложения x^4+2 равно $K = \mathbb{Q}(i, \sqrt[4]{2})$. Можно убедиться (упражнение!), что степень расширения K над $\mathbb{Q}$ равна 8; в частности, поэтому поле разложения многочлена $x^4 + 2$ не может быть изоморфно полю разложения $x^4 + 1$.

4.3 Нормальные расширения

Поля разложения играют большую роль в теории Галуа: дело в том, что они не только расщепляют данный многочлен на линейные множители, но и автоматически расщепляют любой неприводимый многочлен, у которого появляется хотя бы один корень в этом поле.

Определение 4.3.1. Расширение $k \subseteq F$ называется **нормальным**, если для любого неприводимого многочлена $f \in k[x]$ f имеет корень в F тогда и только тогда, когда f расщепляется в произведение линейных множителей в $F[x]$.

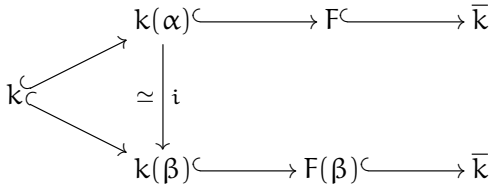
Теорема 4.3.2. *Расширений полей $k \subseteq F$ является конечным и нормальным тогда и только тогда, когда F является полем разложения некоторого многочлена $f \in k[x]$.*

Доказательство. Пусть $k \subseteq F$ — конечное нормальное расширение. Тогда F конечно порождено: $F = k(\alpha_1, \ldots, \alpha_r)$, где каждый α_i алгебраичен над k. Пусть p_i — минимальный многочлен α_i над k. Из определения нормальности следует, что каждый $p_i(t)$ раскладывается над F на линейные множители, поэтому и их произведение $f = p_1 \ldots p_r$ раскладывается над F на линейные множители. Следовательно, F является полем разложения многочлена f.

Обратно, предположим, что F — поле разложения многочлена $f \in k[x]$, и пусть $p \in k[x]$ — неприводимый многочлен, у которого появляется корень α в F. Можно считать, что F — подполе алгебраического замыкания $\overline{k}$. Пусть $\beta \in \overline{k}$ — любой другой корень многочлена p; мы хотим доказать, что $\beta \in F$. Из этого будет следовать, что F содержит все корни p, то есть, F нормально. Расширение $k \subseteq F$ конечно по предложению 4.2.2.

Существует изоморфизм $i\colon k(\alpha) \to k(\beta)$, ограничение которого на k тождественно, такой,

что $i(\alpha) = \beta$. Рассмотрим также подполе $F(\beta) \subseteq \overline{k}$, являющееся расширением $k(\beta)$:



Теперь рассмотрим F как поле разложения многочлена f не над k, а над $k(\alpha)$. Это можно сделать, поскольку F содержит все корни f и, кроме того, F порождается над k (и, следовательно, над $k(\alpha)$) этими корнями. Аналогично, $F(\beta)$ можно рассмотреть как поле разложения многочлена f над $k(\beta)$. Теперь можно применить вторую часть предложения 4.2.2 к изоморфизму i и получить изоморфизм полей разложения $j\colon F \to F(\beta)$, продолжающий i. В частности, j является изоморфизмом векторных пространств над k, поэтому $\dim_k(F) = \dim_k(F(\beta))$, и обе этих размерности конечны (поскольку поле разложения F конечномерно над k). Теперь рассмотрим вложение $F \to F(\beta)$, являющееся, несомненно, линейным отображением векторных пространств одинаковой конечной размерности. Получаем, что $F = F(\beta)$, то есть, $\beta \in F$, что и требовалось. □

Пример 4.3.3. Мы знаем, что расширение $\mathbb{Q}(i, \sqrt[4]{2})$ является полем разложения многочлена $x^4 + 2$. Поэтому если корень неприводимого многочлена $p \in \mathbb{Q}[x]$ выражается как рациональная функция от i и $\sqrt[4]{2}$ с рациональными коэффициентами, то *все* корни p выражаются таким образом.

4.4 Сепарабельные многочлены

Пример 4.4.1. Пусть p — простое число. Рассмотрим поле $\mathbb{F}_p(t)$ рациональных функций от переменной t. Многочлен $x^p - t$ над этим полем неприводим. Действительно, он неприводим в $\mathbb{F}_p[t][x]$ по критерию Эйзенштейна (t является простым элементом $\mathbb{F}_p[t]$), поэтому по лемме Гаусса (перекрестное сокращение знаменателей) он неприводим и в $\mathbb{F}_p(t)[x]$. Пусть u — корень этого многочлена в каком-нибудь расширении L поля $\mathbb{F}_p(t)$ (например, в качестве L можно взять алгебраическое замыкание поля $\mathbb{F}_p(t)$). Тогда $x^p - t = x^p - u^p = (x-u)^p$ в $L[x]$, поскольку в поле характеристики p выполнено тождество $(a+b)^p = a^p + b^p$. Поэтому u оказался кратным корнем неприводимого многочлена $x^p - t$.

Следующее определение выделяет многочлены, для которых подобных патологий не происходит.

Определение 4.4.2. Многочлен $f \in k[x]$ называется **сепарабельным**, если он не имеет кратных корней в своем поле разложения. В противном случае многочлен называется **несепарабельным**

Очевидно, что можно рассматривать корни многочлена не в поле разложения, а в любом расширении, в котором данный многочлен раскладывается на линейные множители. Позже мы увидим, что несепарабельные многочлены существуют только над полями положительной характеристики.

Следующая лемма показывает, что несепарабельность можно обнаружить, не выходя за пределы исходного поля.

Лемма 4.4.3. *Многочлен $f \in k[x]$ сепарабелен тогда и только тогда, когда f и f' взаимно просты.*

Доказательство. Сразу заметим, что условие взаимной простоты сохраняется при расширениях полей: наибольший общий делитель можно искать с помощью алгорифма Эвклида, а он не выводит за пределы данного поля. Пусть $\gcd(f, f') = 1$; предположим, что f несепарабелен. Рассмотрим расширение, в котором у f есть кратный корень α. Запишем $f = (x-\alpha)^m \cdot g$, где $m \geqslant 2$. Тогда $f' = m(x-\alpha)^{m-1}g + (x-\alpha)^m g'$, и $m - 1 \geqslant 1$. Значит, и f, и f' делятся на $x - \alpha$, поэтому они не многут быть взаимно просты. Обратно, пусть многочлен f сепарабелен, а $\gcd(f, f') = d \neq 1$. Рассмотрим расширение L, в котором у многочлена d есть корень α. Тогда f, f' делятся на $x - \alpha$ в $L[x]$. Запишем $f = (x-\alpha) \cdot g$ и продифференцируем это равенство: $f' = (x-\alpha)g' + g$. В этом равенстве f' делится на $x-\alpha$ и $(x-\alpha)g'$ делится на $x-\alpha$, поэтому и g делится на $x-\alpha$. Получаем, что $f = (x-\alpha)^2 \cdot h$, и, стало быть, у f есть кратный корень в L. □

Таким образом, несепарабельность многочлена $x^p - t$ из нашего примера можно увидеть сразу из того, что $(x^p - t)' = px^{p-1} = 0$ над полем $\mathbb{F}_p[t]$, поэтому $\gcd(x^p - t, 0) = x^p - t \neq 1$.

Лемма 4.4.4. *Пусть* k *— поле,* $f \in k[x]$ *— несепарабельный неприводимый многочлен. Тогда* $f' = 0$.

Доказательство. Если f несепарабелен, то по лемме 4.4.3 у f и f' есть общий множитель q положительной степени. Поскольку f неприводим и f делится на q, f должен отличаться от q на константу. Степень f' строго меньше степени f, но f' делится на q — это возможно только если $f' = 0$. □

Из этой леммы сразу видно, что в характеристике 0 любой неприводимый многочлен сепарабелен: в этом случае $\deg(f') = \deg(f) - 1$. Более того, если характеристика k равна простому числу p и $f' = 0$, нетрудно понять, что в многочлене f возможны только мономы вида x^{pl}. Иными словами, если $f' = 0$, то f является многочленом от x^p.

Определение 4.4.5. Пусть k — поле характеристики $p > 0$. Отображение $k \to k$, $x \mapsto x^p$, называется **гомоморфизмом Фробениуса**.

Нетрудно понять, что гомоморфизм Фробениуса действительно является гомоморфизмом колец; он инъективен, как и любой гомоморфизм между полями, но не всегда сюръективен.

4.5 Совершенные поля

Определение 4.5.1. Поле k называется **совершенным**, если любой неприводимый многочлен над k сепарабелен.

Предложение 4.5.2. *Пусть* k *— поле.* k *совершенно тогда и только тогда, когда либо* $\mathrm{char}\, k = 0$*, либо* $\mathrm{char}\, k > 0$ *и гомоморфизм Фробениуса сюръективен.*

Доказательство. Мы уже заметили, что если $\mathrm{char}\, k = 0$, то все неприводимые многочлены сепарабельны, поэтому k совершенно. Если же $\mathrm{char}\, k = p$, мы знаем, что несепарабельный многочлен должен иметь вид $f = \sum_i a_i (x^p)^i$. Из сюръективности Фробениуса следует, что найдутся b_i такие, что $b_i^p = a_i$. Тогда $f = \sum_i b_i^p (x^p)^i = \sum_i (b_i x^i)^p = (\sum_i b_i x^i)^p$, что противоречит неприводимости f.

Обратно, пусть k совершенно, то есть, любой неприводимый многочлен над k сепарабелен. Нам нужно доказать, что если $\mathrm{char}\, k = p$, то гомоморфизм Фробениуса сюръективен. Возьмем $a \in k$ и посмотрим на многочлен $f = x^p - a$. Если он неприводим, то он сепарабелен. По лемме 4.4.3 это бы означало, что f и f' взаимно просты; но $f' = px^{p-1} = 0$. Значит, f

приводим: $f = gh$ над полем k. С другой стороны, в поле разложения многочлена f у f есть корень b и $f = x^p - a = x^p - b^p = (x-b)^p$, поэтому b — корень кратности p. Значит, множители g и h многочлена f имеют вид $(x-b)^l$ и $(x-b)^{p-l}$ для некоторого l: $0 < l < p$. Мы знаем, что коэффициенты многочлена $g = (x-b)^l$ лежат в k; $(x-b)^l = x^l - bl(x-b)^{l-1} + \dots$, поэтому $bl \in k$. Но l взаимно просто с p, поэтому обратимо в k. Значит, на самом деле $b \in k$. Но $b^p = a$, поэтому a лежит в образе гомоморфизма Фробениуса. □

Следствие 4.5.3. *Конечные поля совершенны.*

Доказательство. Гомоморфизм Фробениуса инъективен (поскольку это гомоморфизм полей), и для конечного поля он сюръективен по принципу Дирихле. □

4.6 Конечные поля

Пусть F — конечное поле характеристики $p > 0$. Можно считать, что F является расширением $\mathbb{F}_p \subseteq$ своего простого подполя $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Обозначим $d = [F : \mathbb{F}_p]$. Тогда F изоморфно $\mathbb{F}_p^d$ как векторное пространство; в частности, $|F| = p^d$ — степень p. В этом разделе мы увидим, что для каждой степени q простого числа p существует ровно одно поле F с q элементами (с точностью до изоморфизма).

Теорема 4.6.1. *Пусть $q = p^d$. Тогда поле разложения многочлена $x^q - x$ над $\mathbb{F}_p$ — поле из q элементов. Обратно, если F — поле из q элементов, то F является полем разложения $x^q - x$ над $\mathbb{F}_p$. Многочлен $x^q - x$ сепарабелен над $\mathbb{F}_p$.*

Доказательство. Пусть F — поле разложения многочлена $f = x^q - x$ над $\mathbb{F}_p$. Обозначим через E множество всех корней E в F. $f' = qx^{q-1} - 1 = -1$, поэтому f и f' взаимно просты, и f сепарабелен. Стало быть, в E ровно q элементов. Докажем, что E является полем: пусть $a, b \in E$; тогда $a^q = a$, $b^q = b$, поэтому $(a-b)^q = a^q + (-1)^q b^q = a - b$. Если $b \neq 0$, то $(ab^{-1})^q = a^q (b^q)^{-1} = ab^{-1}$. Значит, E замкнуто относительно операций вычитания и деления на ненулевой элемент. Поэтому E — поле. Кроме того, F порождается корнями f над $\mathbb{F}_p$, поэтому $F = E$.

Обратно, если F — поле и $|F| = q$, то ненулевые элементы F образуют группу из $q-1$ элемента относительно умножения. Порядок каждого $a \in F^*$ в этой группе делит $q-1$. Значит, для ненулевых a выполнено $a^{q-1} = 1$. Поэтому $a^q - a = 0$ для всех a. Значит, у многочлена $x^q - x$ оказалось q корней в F (а именно, все элементы F). Поэтому F является полем разложения $x^q - x$, что и требовалось. □

Следствие 4.6.2. *Для каждого q, являющегося степенью простого числа, существует единственное (с точностью до изоморфизма) поле из q элементов.*

Доказательство. Немедленно следует из теоремы 4.6.1 вместе с единственностью поля разложения. □

Следствие 4.6.3. *Пусть p — простое число, $d \leqslant e$ — натуральные числа. Расширение $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^e}$ существует тогда и только тогда, когда e делится на d. Более того, если e делится на d, то существует ровно одно такое расширение; точнее, поле $\mathbb{F}_{p^e}$ содержит единственную копию поля $\mathbb{F}_{p^d}$. Все расширения $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^e}$ — простые.*

Доказательство. Если такое расширение существует, то $\mathbb{F}_p \subseteq \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^e}$ — башня расширений, и по теореме о размерности башни степень $[\mathbb{F}_{p^e} : \mathbb{F}]$ делится на степень $[\mathbb{F}_{p^d} : \mathbb{F}]$, то есть, e делится на d. Обратно, если e делится на d, то $p^e - 1 = (p^d - 1)((p^d)^{e/d-1} + \dots + 1)$,

поэтому $p^e - 1$ делится на $p^d - 1$, и $x^{p^e-1} - 1$ делится на $x^{p^d-1} - 1$. Значит, $x^{p^e} - x$ делится на $x^{p^d} - x$. По теореме 4.6.1 $\mathbb{F}_{p^e}$ является полем разложения многочлена $x^{p^e} - x$. Нетрудно видеть, что корни многочлена $x^{p^d} - x$ порождают в нем единственное подполе, являющееся полем разложения многочлена $x^{p^d} - x$, то есть, подполе, изоморфное $\mathbb{F}_{p^d}$. Для доказательства простоты расширения $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^e}$ достаточно вспомнить, что мультипликативная группа конечного поля является циклической. Если $\alpha \in \mathbb{F}_{p^e}$ порождает эту группу, то α порождает все поле $\mathbb{F}_{p^e}$ над любым подполем, поэтому $\mathbb{F}_{p^e} = \mathbb{F}_{p^d}(\alpha)$. □

5 Теория Галуа

5.1 Группа автоморфизмов расширения

Определение 5.1.1. Пусть $k \subseteq F$ — расширение полей. Группа автоморфизмов $j\colon F \to F$ таких, что $j|_k = \mathrm{id}_k$, называется **группой автоморфизмов расширения** и обозначается через $\mathrm{Aut}_k(F)$.

Предложение 5.1.2. *Пусть* $k \subseteq F = k(\alpha)$ *— простое конечное расширение, и* $p \in k[x]$ *— минимальный многочлен* α *над* k*. Тогда* $|\mathrm{Aut}_k(F)|$ *равняется числу различных корней многочлена* p*; в частности,* $|\mathrm{Aut}_k(F)| \leqslant [F : k]$*. Равенство выполняется тогда и только тогда, когда* p *раскладывается над* F *в произведение различных линейных многочленов.*

Доказательство. Пусть $j \in \mathrm{Aut}_k(F)$. Кождый элемент F является многочленом от α с коэффициентами из k, и j тождественно на k, поэтому j полностью определяется заданием $j(\alpha)$. В частности, $p(j(\alpha)) = j(p(\alpha)) = j(0) = 0$, поэтому $j(\alpha)$ является корнем p. Значит, $|\mathrm{Aut}_k(F)|$ не больше, чем число корней p. Обратно, как только мы выбрали корень многочлена p, мы можем продолжить тождественное отображение на k до автоморфизма F, переводящего α в выбранный корень. □

Примеры 5.1.3. 1. Мы уже считали $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}))$: это циклическая группа C_2.

2. Группа $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) = F$ состоит из четырех элементов. Действительно, мы уже знаем, что минимальный многочлен элемента $\sqrt{2} + \sqrt{3}$ — это $t^4 - 10t^2 + 1$. Все его корни — это $\pm\sqrt{2} \pm \sqrt{3}$. У F есть автоморфизм, оставляющий на месте $\mathbb{Q}(\sqrt{2})$ и переводящий $\sqrt{3} \mapsto -\sqrt{3}$. С другой стороны, есть автоморфизм, оставляющий на месте $\mathbb{Q}(\sqrt{3})$ и переводящий $\sqrt{2} \mapsto -\sqrt{2}$. Мы нашли два различных элемента порядка 2; поэтому группа $\mathrm{Aut}_{\mathbb{Q}}(F)$ не может быть циклической. Значит, это группа $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. Пусть F — поле разложения $x^4 + 1$ над $\mathbb{Q}$; мы видели, что $F = \mathbb{Q}(i, \sqrt{2})$. Аналогично предыдущему случаю мы видим, что группа $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(i, \sqrt{2}))$ изоморфна $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Упражнение 5.1.4. *Найдите группу* $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2 + \sqrt{2}}))$.

Таким образом, группа $\mathrm{Aut}_k(F)$ отождествляется с некоторой подгруппой группы перестановок корней неприводимого многочлена p в F.

5.2 Автоморфизмы конечных полей

Предложение 5.2.1. *Пусть* F *— конечное поле. Тогда для любого натурального* n *существует неприводимый многочлен степени* n *в* $F[x]$.

Доказательство. Мы знаем, что $F = \mathbb{F}_{p^d}$ для некоторого простого p и $d \geqslant 1$. По следствию 4.6.3 существует расширение $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^{dn}}$, порожденное элементом α. Тогда $[\mathbb{F}_{p^{dn}} : \mathbb{F}_{p^d}] = n$, и поэтому минимальный многочлен элемента α над $\mathbb{F}^{p^d}$ является неприводимым многочленом степени n в $F[x]$. □

Предложение 5.2.2. *Пусть $F = \mathbb{F}_q$ — конечное поле, n — натуральное число. Тогда в разложение многочлена $x^{q^n} - x$ в $F[x]$ входят все неприводимые многочлены (со старшим коэффициентом 1) степени d, где d пробегает все натуральные делители n. В частности, все эти многочлены полностью раскладываются над полем $\mathbb{F}_{q^n}$.*

Доказательство. По теореме 4.6.1 поле $\mathbb{F}_{q^n}$ является полем разложения $x^{q^n} - x$ над $\mathbb{F}_p$, поэтому и над $\mathbb{F}_q = F$. Если f — неприводимый многочлен степени d со старшим коэффициентом 1, то $F[x]/(f) = F(\alpha)$ является расширением степени d над F и, следовательно, изоморфно $\mathbb{F}_{q^d}$. По следствию 4.6.3 существует вложение $\mathbb{F}_{q^d}$ в $\mathbb{F}_{q^n}$. Но поле F_{q^n} состоит из корней многочлена $x^{q^n} - x$, поэтому α должно быть корнем этого многочлена. Минимальным многочленом α является f, значит, $x^{q^n} - x$ делится на f. Мы показали, что любой неприводимый многочлен степени d (где d — делитель n) является множителем многочлена $x^{q^n} - x$. Обратно, если f — неприводимый множитель в $x^{q^n} - x$, то $\mathbb{F}_{q^n}$ содержит некоторый корень α многочлена f. Поэтому $F = \mathbb{F}_q \subseteq \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^n}$, и $\mathbb{F}_q(\alpha) \simeq \mathbb{F}_{q^d}$, где $d = \deg(\alpha)$. По следствию 4.6.3 тогда n делится на d. □

Пример 5.2.3. Пусть $q = 2$, то есть, $F = \mathbb{F}_2$.

- $n = 1$: многочлен $x^2 - x$ раскладывается в произведение x и $x - 1$. Это все неприводимые многочлены степени 1 над $\mathbb{F}_2$.
- $n = 2$: многочлен $x^4 - x$ должен раскладываться в произведение всех неприводимых многочленов степеней 1 и 2. Действительно, $x^4 - x = x(x-1)(x^2 + x + 1)$, поэтому существует только один неприводимый многочлен степени 2 над $\mathbb{F}_2$, а именно, $x^2 + x + 1$.
- $n = 3$: многочлен $x^8 - x$ делится на $x(x-1)$ и частное имеет стемень 6. Оно должно быть произведением всех неприводимых многочленов степени 3 над $\mathbb{F}_2$, поэтому таких многочленов ровно две штуки. Несложно понять, что это многочлены $x^3 + x^2 + 1$ и $x^3 + x + 1$. Поэтому $\mathbb{F}_8$ можно представить как фактор $\mathbb{F}_2[x]$ по модулю неприводимого многочлена двумя способами: $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ и $\mathbb{F}_2[x]/(x^3 + x + 1)$. Эти поля изоморфны по теореме 4.6.1. Упражнение: постройте явный изоморфизм между ними.
- $n = 6$: разложение $x^{64} - x$ должно включать в себя множители x, $x - 1$, $x^2 + x + 1$, $x^3 + x^2 + 1$ и $x^3 + x + 1$. Остается многочлен степени 54, то есть, девять неприводимых многочленов степени 6. Таким образом, $\mathbb{F}_{64}$ можно представить как фактор $\mathbb{F}_2[x]$ по неприводимому многочлену степени 6 девятью разными способами, и все они приводят к изоморфным полям.

Вычислим теперь группу автоморфизмов $\mathbb{F}_{p^d}$ над $\mathbb{F}_p$ для простого p. Мы знаем, что расширение $\mathbb{F}_p \subseteq \mathbb{F}_{p^d}$ является простым, и минимальный многочлен порождающего элемента имеет степень d. Этот многочлен сепарабелен (поскольку конечное поле $\mathbb{F}_p$ совершенно), следовательно, по предложению 5.1.2, $|\operatorname{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^d})| = d$.

Предложение 5.2.4. *Группа $\operatorname{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^d})$ является циклической и порождается автоморфизмом Фробениуса.*

Доказательство. Обозначим гомоморфизм Фробениуса $\mathbb{F}_{p^d} \to \mathbb{F}_{p^d}$ через φ: $\varphi(x) = x^p$. По принципу Дирихле φ является изоморфизмом и ограничение его на $\mathbb{F}_p$ тождественно (поскольку $\mathbb{F}_p$ состоит из корней многочлена $x^p - x$). Мы уже знаем, что порядок группы $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^d})$ равен d, поэтому достаточно доказать, что φ имеет порядок d.

Пусть порядок φ равен e. Тогда $\varphi^e = \mathrm{id}$, то есть, $x^{p^e} = x$ для всех $x \in \mathbb{F}_{p^d}$. Это означает, что у ненулевого многочлена $x^{p^e} - x$ нашлось p^d корней в поле $\mathbb{F}_{p^d}$; отсюда немедленно следует, что $p^d \leqslant p^e$, то есть, $d \leqslant e$. С другой стороны, порядок группы всегда делится на порядок ее элемента, поэтому d делится на e. Значит, $d = e$. □

5.3 Сепарабельность и вложения в алгебраическое замыкание

Пусть $k \subseteq F$ — расширение полей. Элемент $\alpha \in F$ называется **сепарабельным над** k, если минимальный многочлен α над k сепарабелен; в противном случае α называется **несепарабельным над** k. Алгебраическое расширение полей $k \subseteq F$ называется **сепарабельным**, если каждый его элемент сепарабелен над k.

Теперь можно переформулировать определение совершенного поля так: поле k называется совершенным, если каждое алгебраическое расширение k сепарабельно. В дальнейшем мы будем в основном ограничиваться рассмотрением лишь сепарабельных расширений.

Мы знаем, что каждое алгебраическое расширение $k \subseteq F$ можно вложить в алгебраическое замыкание поля k: $k \subseteq F \subseteq \overline{k}$. Вообще говоря, это можно сделать разными способами. Количество различных гомоморфизмов $F \to \overline{k}$, тождественных на k, обозначается через $[F : k]_s$ и называется **сепарабельной степенью** расширения F над k.

Лемма 5.3.1. *Пусть $k \subseteq k(\alpha)$ — простое алгебраическое расширение. Тогда $[k(\alpha) : k]_s$ равно числу различных корней в $\overline{k}$ минимального многочлена элемента α. В частности, $[k(\alpha) : k]_s \leqslant [k(\alpha) : k]$, и равенство выполнено тогда и только тогда, когда α сепарабелен над k.*

Доказательство. (Вспомните доказательство предложения 5.1.2.) Сопоставим каждому гомоморфизму $i\colon k(\alpha) \to \overline{k}$, тождественному на k, образ $i(\alpha)$ элемента α. Элемент $i(\alpha)$ должен быть корнем минимального многочлена α. Это сопоставление (отображение из множества гомоморфизмов $k(\alpha) \to \overline{k}$, тождественных на k, в множество корней минимального многочлена α) инъективно: если известно $i(\alpha)$, то известно значение i на всех элементах $k(\alpha)$. Кроме того, оно сюръективно: если $\beta \in \overline{k}$ — корень этого минимального многочлена, можно рассмотреть расширение $k(\beta) \subseteq \overline{k}$; по предложению 3.3.1 существует изоморфизм $k(\alpha) \to k(\beta)$, отправляющий α в β. В композиции с вложением $k(\beta) \subseteq \overline{k}$ получаем нужное отображение $i\colon k(\alpha) \to \overline{k}$. □

Таким образом, для простых расширений сепарабельная степень действительно связана с сепарабельностью. Кроме того, сепарабельная степень мультипликативна:

Лемма 5.3.2. *Пусть $k \subseteq E \subseteq F$ — алгебраические расширения. Тогда $[F : k]_s$ конечна тогда и только тогда, когда обе $[F : E]_s$ и $[E : k]_s$ конечны. В этом случае $[F : k]_s = [F : E]_s[E : k]_s$.*

Доказательство. Различные вложения E в $\overline{k}$ продолжаются до различных вложений F в $\overline{k}$ по предложению 4.1.3; при этом если вложение F в $\overline{E} = \overline{k}$ тождественно на E, то оно тем более тождественно на k. Значит, если одна из степеней $[F : E]_s$, $[E : k]_s$ бесконечна, то и $[F : k]_s$ бесконечна.

Обратно, каждое вложение $F \subseteq \overline{k}$, тождественное на k, можно получить в два шага: сначала построить вложение $E \subseteq \overline{k}$, тождественное на k (это можно сделать $[E : k]_s$ способами), а потом продолжить выбранное вложение $E \subseteq \overline{k} = \overline{E}$ до вложения $F \subseteq \overline{E} = \overline{k}$ (что

можно сделать $[F : E]_s$ способами). Получили в точности $[F : E]_s \cdot [E : k]_s$ способов, что и требовалось. □

Теперь мы можем переформулировать сепарабельность конечных расширений в терминах подсчета вложений в алгебраическое замыкание:

Предложение 5.3.3. *Пусть $k \subseteq F$ — конечное расширение. Тогда $[F : k]_s \leqslant [F : k]$, и следующие три условия равносильны:*

1. *$F = k(\alpha_1, \ldots, \alpha_r)$, где каждый α_i сепарабелен над k;*
2. *расширение $k \subseteq F$ сепарабельно;*
3. *$[F : k]_s = [F : k]$.*

Доказательство. Поскольку F конечно над k, оно конечно порождено. Пусть $F = k(\alpha_1, \ldots, \alpha_r)$. Тогда в силу предыдущих двух лемм и теоремы о башне расширений получаем

$$\begin{aligned}[F : k]_s &= [k(\alpha_1, \ldots, \alpha_{r-1})(\alpha_r) : k(\alpha_1, \ldots, \alpha_{r-1})]_s \cdot \cdots \cdot [k(\alpha_1) : k]_s \\ &\leqslant [k(\alpha_1, \ldots, \alpha_{r-1})(\alpha_r) : k(\alpha_1, \ldots, \alpha_{r-1})] \cdot \cdots \cdot [k(\alpha_1) : k] \\ &= [F : k].\end{aligned}$$

(1) $\Longrightarrow$ (3): если α_i сепарабелен над k, то он сепарабелен и над $k(\alpha_1, \ldots, \alpha_{i-1})$ (это несложное упражнение), поэтому неравенство $[F : k]_s \leqslant [F : k]$ превращается в равенство по лемме 5.3.1.

(3) $\Longrightarrow$ (2): пусть $[F : k]_s = [F : k]$, $\alpha \in F$. Тогда $k \subseteq k(\alpha) \subseteq F$, откуда по лемме 5.3.2 имеем $[F : k(\alpha)]_s \cdot [k(\alpha) : k]_s = [F : k]_s = [F : k] = [F : k(\alpha)] \cdot [k(\alpha) : k]$. Поскольку сепарабельная степень не превосходит обычной, мы получаем $[k(\alpha) : k]_s = [k(\alpha) : k]$, и α сепарабелен по лемме 5.3.1. По определению это означает, что расширение $k \subseteq F$ сепарабельно.

(2) $\Longrightarrow$ (2) немедленно следует из определения (конечное расширение является конечно порожденным). □

5.4 Сепарабельность и простые расширения

Все примеры расширений полей, которые мы видели до сих пор, являлись простыми расширениями. Это неспроста: дело в том, что мы видели в основном сепарабельные расширения, и сейчас мы покажем, что любое конечное сепарабельное расширение является простым.

Предложение 5.4.1. *Алгебраическое расширение $k \subseteq F$ является простым тогда и только тогда, когда количество промежуточных полей $k \subseteq E \subseteq F$ конечно.*

Доказательство. Пусть $F = k(\alpha)$ — простое алгебраическое расширение; $q_k(x)$ — минимальный многочлен α над k. Вложим F в алгебраическое замыкание $\overline{k}$ поля k. Если E — промежуточное поле, что $F = E(\alpha)$ — снова простое алгебраическое расширение; пусть $q_E(x)$ — минимальный многочлен α над E. Заметим, что $q_k(x)$ делится на $q_E(x)$. Докажем, что E однозначно определяется многочленом $q_E(x)$. Поскольку у $q_k(X)$ лишь конечное число множителей в $\overline{k}$, мы докажем, что имеется лишь конечное количество промежуточных полй.

Покажем, что E порождается над k коэффициентами многочлена $q_E(x)$. Пусть $E' \subseteq E$ — подполе E, порожденное k и коэффициентами $q_E(x)$. Тогда $q_E(x) \in E'[x]$, и, поскольку $q_E(x)$ неприводим над E, он остается неприводимым над E'. Кроме того, $E'(\alpha) = F = E(\alpha)$.

Рассмотрим башню расширений $E' \subseteq E \subseteq F$; видим, что $\deg(q_E(x)) = [F : E'] = [F : E] \cdot [E : E'] = \deg(q_E(x))[E : E']$, поэтому $[E : E'] = 1$ и $E = E'$.

Обратно, пусть имеется лишь конечное число промежуточных полей $k \subseteq E \subseteq F$. Расширение $k \subseteq F$ конечно порождено (иначе мы легко построили бы бесконечную цепочку подрасширений $k \subseteq k(\alpha_1) \subseteq k(\alpha_1, \alpha_2) \subseteq \ldots \subseteq F$) и алгебраично, поэтому оно конечно. Если k конечно, то F конечно, и просто по следствию 4.6.3. Теперь считаем, что k бесконечно. Можно считать, что $F = k(\alpha, \beta)$ (дальше — индукция по числу порождающих элементов). Для каждого $c \in k$ рассмотрим промежуточное поле $k \subseteq k(c\alpha + \beta) \subseteq k(\alpha, \beta) = F$. Их конечное число, в то время как k бесконечно; поэтому для некоторых $c \neq c' \in k$ выполнено $k(c'\alpha+\beta) = k(c\alpha+\beta)$. Тогда $\alpha = \frac{(c'\alpha+\beta)-(c\alpha+\beta)}{c'-c} \in k(c\alpha+\beta)$ и $\beta = (c\alpha+\beta)-c\alpha \in k(c\alpha+\beta)$, поэтому $k(\alpha, \beta) \subseteq k(c\alpha+\beta)$ и, следовательно, $k(\alpha, \beta) = k(c\alpha+\beta)$ — простое расширение. □

Предложение 5.4.2. *Всякое конечное сепарабельное расширение является простым.*

Доказательство. Можно предполагать, что $F = k(\alpha, \beta)$ (дальше индукция по числу порождающих элементов), и α, β сепарабельны над k. В частности, α, β алгебраичны над k. Можно предполагать, что поле k бесконечно.

Рассмотрим множество I вложений $i\colon F \to \overline{k}$ поля F в алгебрическое замыкание поля k, которые индуцируют тождественное отображение на k: $i|_k = \mathrm{id}_k$. Если $i \neq i'$ — два таких вложения, и x — переменная, то многочлены $i(\alpha)x+i(\beta)$ и $i'(\alpha)x+i'(\beta)$ различны — иначе $i'(\alpha) = i(\alpha)$ и $i'(\beta) = i(\beta)$, откуда $i = i'$ на всем $k(\alpha, \beta) = F$. Рассмотрим многочлен $f(x) = \prod_{i \neq i'}((i(\alpha)x + i(\beta)) - (i'(\alpha)x + i'(\beta))) \in \overline{k}[x]$. Он не равен тождественно нулю, а поле k бесконечно, поэтому найдется точка $c \in k$, в которой он не равен нулю. То есть, разные элементы $i \in I$ переводят элемент $\gamma = c\alpha+\beta$ в разные элементы $i(\gamma) = i(\alpha)c+i(\beta)$. Мы знаем, что в множестве I ровно $[F : k]_s$ элементов, и каждый $i(\gamma)$ является корнем минимального многочлена элемента γ над k, поэтому $[F : k]_s \leqslant [k(\gamma) : k] \leqslant [F : k]$. По предположению расширение является сепарабельным, значит, $[F : k]_s = [F : k]$, поэтому $[k(\gamma) : k] = [F : k]$, откуда $F = k(\gamma)$, что и требовалось. □

Следствие 5.4.3. *Пусть $k \subseteq F$ — конечное сепарабельное расширение. Тогда $|\mathrm{Aut}_k(F)| \leqslant [F : k]$, и равенство выполнено тогда и только тогда, когда расширение $k \subseteq F$ нормально.*

Доказательство. Расширение $k \subseteq F$ конечно и сепарабельно. По предложению 5.4.2 оно является простым: $F = k(\alpha)$ для некоторого $\alpha \in F$. Неравенство немедленно следует из предложения 5.1.2; а равенство выполнено тогда и только тогда, когда минимальный многочлен f элемента α раскладывается на различные линейные множители над полем F. В этом случае F является полем разложения многочлена f, поэтому оно нормально (теорема 4.3.2). Обратно, если F нормально над k, то f раскладывается на линейные множители над F, и все его корни различны, поскольку α сепарабелен над k. Поэтому $|\mathrm{Aut}_k(F)| = [F : k]$ по предложению 5.1.2. □

5.5 Соответствие Галуа и расширения Галуа

Пусть $k \subseteq F$ — расширение полей, $G \leqslant \mathrm{Aut}_k(F)$ —группа, состоящая из некоторых автоморфизмов этого расширения. Промежуточное поле $F^G = \{\alpha \in F \mid \forall g \in G, g\alpha = \alpha\}$ называется **неподвижным полем** группы G. Очевидно, что оно действительно является подполем в F и содержит k. Мы получаем соответствие между промежуточными полями E: $k \subseteq E \subseteq F$ и подгруппами группы $\mathrm{Aut}_k(F)$. Это соответствие сопоставляет каждой подгруппе $G \leqslant \mathrm{Aut}_k(F)$ ее поле неподвижных точек F^G, а каждому промежуточному полю E подгруппу $\mathrm{Aut}_E(F)$ группы $\mathrm{Aut}_k(F)$. Это соответствие называется **соответствием Галуа**.

Лемма 5.5.1. *Соответствие Галуа обращает включение. Более того, для всех подгрупп* $G \leqslant \mathrm{Aut}_k(F)$ *и для всех промежуточных полей* $k \subseteq E \subseteq F$ *выполнено* $E \subseteq F^{\mathrm{Aut}_E(F)}$ *и* $G \leqslant \mathrm{Aut}_{F^G}(F)$. *Обозначим через* E_1E_2 *наименьшее подполе* F, *содержащее промежуточные подполя* E_1, E_2, *а через* $\langle G_1, G_2\rangle$ — *наименьшую подгруппу в* $\mathrm{Aut}_k(F)$, *содержащую подгруппы* G_1 *и* G_2. *Тогда* $\mathrm{Aut}_{E_1E_2}(F) = \mathrm{Aut}_{E_1}(F) \cap \mathrm{Aut}_{E_2}(F)$ *и* $F^{\langle G_1, G_2\rangle} = F^{G_1} \cap F^{G_2}$.

Доказательство. Упражнение. □

Конечно же, возникает естественный вопрос — когда указанные в Лемме включения превращаются в равенства (и, таким образом, соответствие Галуа становится биективным). Заметим, что не всегда:

Пример 5.5.2. Рассмотрим расширение $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$. Его степень равна простому числу 3, поэтому промежуточными полями являются только $\mathbb{Q}$ и $\mathbb{Q}(\sqrt[3]{2})$. Посмотрим на группу $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$. Заметим, что $\sqrt[3]{2}$ является вещественным числом, поэтому $\mathbb{Q}(\sqrt[3]{2}$ содержится в $\mathbb{R}$. У минимального многочлена $t^3 - 2$ элемента $\sqrt[3]{2}$ есть только один вещественный корень, поэтому $\sqrt[3]{2}$ — единственный его корень, лежащий в $\mathbb{Q}(\sqrt[3]{2})$. Поэтому $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})$ состоит из одного (тривиального) элемента. Стало быть, в этом случае соответствие Галуа действует между двухэлементным множеством $\{\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2})\}$ и одноэлементным множеством $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}) = \{e\}$.

Этот пример показывает, что включение $E \subseteq F^{\mathrm{Aut}_E(F)}$ из Леммы 5.5.1 не обязано быть равенством: возьмем $E = \mathbb{Q}$, которое не совпадает с $\mathbb{Q}(\sqrt[3]{2})$ (неподвижным полем единственной подгруппы в $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$.

Предложение 5.5.3. *Пусть* $k \subseteq F$ — *конечное расширение,* $G \leqslant \mathrm{Aut}_k(F)$. *Тогда* $|G| = [F : F^G]$ *и* $G = \mathrm{Aut}_{F^G}(F)$. *В частности, для конечного расширения соответствие Галуа, сопоставляющее каждому промежуточному полю* E *подгруппу* $\mathrm{Aut}_E(F)$ *в* $\mathrm{Aut}_k(F)$, *является сюръективным.*

Для доказательства этого предложения нам понадобится следующая лемма:

Лемма 5.5.4. *Пусть* $k \subseteq F$ — *конечное расширение, и* G — *подгруппа в* $\mathrm{Aut}_k(F)$. *Тогда расширение* $F^G \subseteq F$ *является конечным, простым, нормальным и сепарабельным.*

Доказательство. Заметим, что если $\alpha \in F$ и $g \in G$, то $g\alpha$ должен быть корнем минимального многочлена элемента α над k. Число таких корней конечно, поэтому орбита α под действием группы G состоит из конечного числа элементов $\alpha = \alpha_1, \ldots, \alpha_n$. Группа G действует на этой орбите, переставляя элементы, поэтому каждый элемент G оставляет многочлен $q_\alpha(t) = (t - \alpha_1)\ldots(t - \alpha_n)$ на месте. Значит, коэффициенты этого многочлена лежат в поле F^G. Кроме того, $\deg q_\alpha(t) \leqslant |G|$, и $q_\alpha(t)$ сепарабелен (так как все его корни различны). Значит, α сепарабелен над F^G; поэтому расширение $F^G \subseteq F$ сепарабельно. Оно конечно, поскольку $k \subseteq F$ конечно.

Конечное сепарабельное расширение является простым по Предложению 5.4.2. Пусть α порождает F над F^G. Многочлен $q_\alpha(t)$ раскладывается над F на линейные множители, и F порожден над F^G корнями $q_\alpha(t)$ (достаточно даже $\alpha = \alpha_1$). Поэтому F является полем разложения многочлена $q_\alpha(t)$ над F^G и нормально по теореме 4.3.2. □

Доказательство Предложения 5.5.3. По лемме 5.5.1 G является подгруппой в $\mathrm{Aut}_{F^G}(F)$, в частности, $|G| \leqslant |\mathrm{Aut}_{F^G}(F)|$. Докажем обратное неравенство. По лемме 5.5.4 $F = F^G(\alpha)$ для некоторого $\alpha \in F$. Поэтому $|\mathrm{Aut}_{F^G}(F)|$ равно числу различных корней в F минимального многочлена элемента α над F^G. Как и в доказательстве Леммы 5.5.4 пусть $\alpha = \alpha_1, \ldots, \alpha_n$ —

орбита элемента α под действием G; тогда многочлен $q_\alpha(t) = (t-\alpha_1)\dots(t-\alpha_n)$ имеет своим корнем α. Поэтому $q_\alpha(t)$ делится на минимальный многочлен элемента α. Число n корней многочлена q_α не превосходит $|G|$, откуда $|\operatorname{Aut}_{F^G}(F)| \leqslant |G|$, что и требовалось. Осталось заметить, что $[F : F^G] = |\operatorname{Aut}_{F^G}(F)|$ по следствию 5.4.3, поэтому $[F : F^G] = |G|$. □

Теорема 5.5.5. *Пусть $k \subseteq F$ — конечное расширение полей. Следующие условия равносильны:*

1. *F является полем разложения сепарабельного многочлена $f \in k[t]$ над k;*
2. *$k \subseteq F$ нормально и сепарабельно;*
3. *$|\operatorname{Aut}_k(F)| = [F : k]$;*
4. *$k = F^{\operatorname{Aut}_k(F)}$ является полем неподвижных элементов группы $\operatorname{Aut}_k(F)$;*
5. *соответствие Галуа для $k \subseteq F$ биективно;*
6. *$k \subseteq F$ сепарабельно, и если $F \subseteq K$ — некоторое алгебраическое расширение, $\sigma \in \operatorname{Aut}_k(K)$, то $\sigma(F) = F$.*

Доказательство. Большая часть теоремы уже была доказана ранее. Например, (1) ⇔ (2) по теореме 4.3.2, (2) ⇔ (3) по следствию 5.4.3. Применим предложение 5.5.3 к расширению $F^{\operatorname{Aut}_k(F)} \subseteq F$: видим, что $[F : F^{\operatorname{Aut}_k(F)}] = |\operatorname{Aut}_k(F)|$. Поскольку $k \subseteq F^{\operatorname{Aut}_k(F)} \subseteq F$, получаем, что $k = F^{\operatorname{Aut}_k(F)}$ тогда и только тогда, когда $|\operatorname{Aut}_k(F)| = [F : k]$, то есть, (3) ⇔ (4).

(2) ⇔ (6): заметим, что конечное сепарабельное расширение является простым, поэтому можно считать, что $F = k(\alpha)$. Предположим, что $k \subseteq F$ нормально и пусть $\sigma \in \operatorname{Aut}_k(K)$ — автоморфизм некоторого расширения $F \subseteq K$ такой, что $\sigma(F) \neq F$. Можно считать, что существует $x \in F$ такой, что $\sigma(x) \notin F$. Пусть p — минимальный многочлен элемента x над k; тогда $\sigma(x)$ тоже является корнем p. Поскольку $x \in F$ и F нормально, все корни p тоже лежат в F, то есть, $\sigma(x) \in F$. Обратно, если выполнено (6), докажем, что F нормально. Пусть $p \in k[x]$ — неприводимый многочлен такой, что $\alpha \in F$ является корнем p, и β — другой его корень в K — поле разложения многочлена p. Тогда существует автоморфизм K над k, переводящий α в β. По условию этот автоморфизм переводит F в F, поэтому и $\beta \in F$.

Докажем, что из (5) следует (4). Положим $E = F^{\operatorname{Aut}_k(F)}$. По предложению 5.5.3 $\operatorname{Aut}_E(F) = \operatorname{Aut}_k(F)$. Из биективности соответствия Галуа тогда следует, что $k = E = F^{\operatorname{Aut}_k(F)}$.

Наконец, докажем, что из (1) следует (5). Поскольку расширение $k \subseteq F$ конечно, мы уже знаем из предложения 5.5.3, что у соответствия Галуа есть обратное справа. Докажем существование обратного слева, то есть, что любое промежуточное поле E совпадает с неподвижным полем подгруппы $\operatorname{Aut}_E(F)$. По (1) F является полем разложения сепарабельного многочлена $f \in k[t] \subseteq E[t]$. Поэтому (1) выполняется не только для расширения $k \subseteq F$, но и для $E \subseteq F$. Мы уже доказали, что (1) ⇔ (4), поэтому $E = F^{\operatorname{Aut}_E(F)}$, что и требовалось. □

Определение 5.5.6. Конечное расширение называется **расширением Галуа**, если оно удовлетворяет одному из условий теоремы 5.5.5. В этом случае группа автоморфизмов $\operatorname{Aut}_k(F)$ называется **группой Галуа** этого расширения.

Следствие 5.5.7. *Пусть $k \subseteq F$ — расширение Галуа. Соответствие Галуа устанавливает биекцию между промежуточными подполями в расширении $k \subseteq F$ и подгруппами в $\operatorname{Aut}_k(F)$. Если при этой биекции подполям E_1, E_2 соответствует подгруппы G_1, G_2, то подполю $E_1 \cap E_2$ соответствует подгруппа $\langle G_1, G_2\rangle$, а подполю E_1E_2 (см. лемму 5.5.1) — подгруппа $G_1 \cap G_2$.*

Доказательство. Сразу следует из теоремы 5.5.5 и леммы 5.5.1. □

Мы видели уже много примеров расширений Галуа (поля разложения различных многочленов). Конечные поля являются расширениями Галуа своих простых подполей. С другой стороны, расширение $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ не является расширением Галуа.

5.6 Действие группы на множестве

Основная причина полезности теории групп состоит в том, что на свете много примеров групп вида «множество преобразований *чего-то*, сохраняющих *что-то*». К примеру, группу $\mathrm{GL}(n, k)$ можно рассматривать как множество преобразований векторного пространства k^n, сохраняющих сложение и умножение на скаляр — то есть, структуру векторного пространства. Если на пространстве k^n ввести (скажем, стандартное) скалярное произведение, то появляется группа $\mathrm{O}(n, k)$ ортогональных матриц, то есть, группа преобразований векторного пространства k^n, сохраняющих наше скалярное произведение. Все подобные примеры на самом деле можно рассматривать в некотором более широком контексте *действия группы на множестве*.

Определение 5.6.1. Пусть G — группа, X — множество. **(Действием** G **на** X называется отображение

$$a\colon G \times X \to X$$

(мы будем писать $g \cdot x$ или просто gx вместо $a(g, x)$), удовлетворяющее следующим условиям:

1. $g \cdot (h \cdot x) = (gh) \cdot x$ для всех $g, h \in G$, $x \in X$;
2. $e \cdot x = x$ для всех $x \in X$.

Как всегда, через e мы обозначаем нейтральный элемент группы G. Если на множестве X задано действие группы G, говорят, что X является G-множеством.

Пример 5.6.2. Группа $\mathrm{GL}(n, k)$ действует на k^n посредством умножения матрицы на вектор:

$$\begin{aligned} \mathrm{GL}(n, k) \times k^n &\to k^n, \\ (A, v) &\mapsto Av. \end{aligned}$$

Условия из определения 5.6.1 сводятся к ассоциативности умножения матриц и свойству единичной матрицы.

Пример 5.6.3. На любом множестве X можно завести **тривиальное** действие любой группы G:

$$\begin{aligned} G \times X &\to X, \\ (g, x) &\mapsto x. \end{aligned}$$

Пример 5.6.4. На множестве $X = \{1, \ldots, n\}$ естественно действует симметрическая группа S_n:

$$\begin{aligned} S_n \times \{1, \ldots, n\} &\to \{1, \ldots, n\}, \\ (\pi, i) &\mapsto \pi(i). \end{aligned}$$

Пример 5.6.5. Каждая группа G действует на себе **левыми сдвигами**:

$$G \times G \to G,$$
$$(g, x) \mapsto gx.$$

Есть и другое действие G на себе — сопряжениями:

$$G \times G \to G,$$
$$(g, x) \mapsto gxg^{-1}.$$

Пример 5.6.6. Пусть G — группа, $H \leqslant G$ — подгруппа. Рассмотрим множество G/H правых смежных классов G по H:

$$G/H = \{gH \mid g \in G\}.$$

Группа G действует на этом множестве левыми сдвигами:

$$G \times G/H \to G/H,$$
$$(g_1, g_2H) \mapsto (g_1g_2)H.$$

Нетрудно проверить, что это корректно определенное отображение: если g_2 заменить на другой представитель g_2' того же класса смежности, то $g_1g_2H = g_1g_2'H$. Проверить условия из определения 5.6.1 тоже несложно.

Отметим, что действие левыми сдвигами из примера 5.6.5 является частным случаем примера 5.6.6 для случая тривиальной подгруппы $H = \{e\}$.

Мы покажем, что любое действие группы на множестве в некотором смысле сводится к описанному в примере 5.6.6.

Определение 5.6.7. Пусть группа G действует на множестве X, и $x \in X$. Множество $G \cdot x = \{gx \mid g \in G\}$ называется **орбитой** элемента x.

Оказывается, если G действует на X, все множество X разбивается на непересекающиеся орбиты. Это неудивительно: действие группы на множестве задает на нем следующее отношение эквивалентности: будем говорить, что элемент $x \in X$ эквивалентен элементу $y \in X$, если y лежит в орбите x, то есть, найдется элемент $g \in G$ такой, что $gx = y$. Нетрудно проверить, что это отношение эквивалентности:

- $x = e \cdot x$, поэтому наше отношение рефлексивно;
- если $x = gy$, то $y = g^{-1}x$, поэтому оно симметрично;
- если $x = gy$ и $y = hz$, то $x = gy = g(hz) = (gh)z$, поэтому оно транзитивно.

Обратите внимание, что при доказательстве мы использовали в точности определение действия группы на множестве.

Как мы знаем, полученное отношение эквивалентности на множестве X приводит к разбиению X на классы эквивалентности — это и есть орбиты действия. Другими словами, два элемента эквивалентны тогда и только тогда, когда они лежат в одной орбите.

Определение 5.6.8. Пусть G действует на X. Элемент $x \in X$ называется **неподвижным** (или **неподвижной точкой** этого действия), если $gx = x$ для всех $g \in G$, то есть, если его орбита состоит из одного элемента.

Например, в действии группы G на себе сопряжениями единичный элемент является неподвижной точкой, поскольку $geg^{-1} = e$ для всех $g \in G$. А вот при действии G на себе сдвигами неподвижных точек нет (если G отлична от тривиальной группы из одного элемента), поскольку из равенства $gx = x$ в группе G следует, что $g = e$.

Случай, в некотором смысле противоположный одноэлементным орбитам, возникает, когда все элементы X оказываются в одной орбите.

Определение 5.6.9. Говорят, что действие группы G на множестве X **транзитивно**, если у него ровно одна орбита, то есть, для любых $x, y \in X$ найдется элемент $g \in G$ такой, что $y = gx$.

Действие на множестве смежных классов из примера 5.6.6 является транзитивным. Сейчас мы докажем, что на самом деле любое транзитивное действие имеет такой вид. Осталось понять, что значит «имеет такой вид».

Определение 5.6.10. Пусть заданы два действия: группы G на множестве X, и группы G на другом множестве Y. Отображение $\varphi\colon X \to Y$ называется **изоморфизмом** между G-множествами X и Y, если φ биективно, и $g \cdot \varphi(x) = \varphi(g \cdot x)$ для всех $x \in X$, $g \in G$. В этом случае говорят, что X, Y — **изоморфные** G-множества.

Замечание 5.6.11. Мы могли бы определить **морфизм** G-множеств как произвольное отображение $\varphi\colon X \to Y$, для которого $g \cdot \varphi(x) = \varphi(g \cdot x)$ (при всех $x \in X$, $g \in G$), и потом определить **изоморфизм** как отображение $\varphi\colon X \to Y$, для которого найдется морфизм G-множеств $\psi\colon Y \to X$, обратный к φ (то есть, такой, что $\psi \circ \varphi = \mathrm{id}_X$ и $\varphi \circ \psi = \mathrm{id}_Y$). Нетрудно понять, что такое определение эквивалентно определению 5.6.10, точно так же как изоморфизм групп можно определять как биективный гомоморфизм, а можно как гомоморфизм, для которого существует обратный гомоморфизм.

Определение 5.6.12. Пусть группа G действует на множестве X, и $x \in X$. Множество

$$\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}$$

называется **стабилизатором точки** x. Упражнение: покажите, что $\mathrm{Stab}_G(x)$ является подгруппой в G.

Теорема 5.6.13. *Пусть группа G действует на множестве X, и это действие транзитивно. Пусть $x \in X$. Тогда существует изоморфизм между G-множествами X и $G/\mathrm{Stab}_G(x)$ (с действием левыми сдвигами, описанным в примере 5.6.6).*

Доказательство. Обозначим $H = \mathrm{Stab}_G(x)$ и определим морфизм G-множеств

$$\begin{aligned} \varphi\colon G/H &\to X, \\ gH &\mapsto g \cdot x. \end{aligned}$$

Нужно проверить, что это отображение корректно определено: если $g' \in G$ — другой представитель класса gH (то есть $g' = gh$ для некоторого $h \in H$), нам хочется знать, что $g \cdot x = g' \cdot x$. Но, действительно, $g' \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x$ поскольку $h \cdot x = x$ по определению стабилизатора.

Из транзитивности действия сразу следует, что наше построенное отображение φ сюръективно. Осталось показать инъективность: пусть $\varphi(gH) = \varphi(g'H)$, то есть, $g \cdot x = g' \cdot x$. Это означает, что $(g^{-1}g') \cdot x = x$, и потому $g^{-1}g' = \mathrm{Stab}_G(x)$. Но это в точности означает, что g и g' лежат в одном правом смежном классе по модулю $H = \mathrm{Stab}_G(x)$, то есть, что $gH = g'H$. □

Лемма 5.6.14. *Пусть группа* G *действует на множестве* X. *Если* $x, y \in X$ — *две точки, лежащие в одной орбите этого действия, то их стабилизаторы* $\mathrm{Stab}_G(x)$, $\mathrm{Stab}_G(y)$ *сопряжены, то есть, найдется элемент* $g \in G$ *такой, что* $g\,\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(y)$.

Доказательство. По определению найдется $g \in G$, переводящий x в y: $gx = y$. Заметим, что при этом $g^{-1}y = x$. Покажем для начала, что $g\,\mathrm{Stab}_G(x)g^{-1} \subseteq \mathrm{Stab}_G(y)$. Возьмем элемент $g' \in g\,\mathrm{Stab}_G(x)g^{-1}$ и покажем, что он лежит в стабилизаторе точки y, то есть, что $g'y = y$. Ну, действительно, g' можно записать в виде $gg''g^{-1}$ для некоторого $g'' \in \mathrm{Stab}_G(x)$, и тогда $g'y = gg''g^{-1}y = gg''x = gx = y$.

Теперь поменяем местами x с y (и g с $g{-}1$); рассуждение выше показывает, что $g^{-1}\,\mathrm{Stab}_G(y)g \subseteq \mathrm{Stab}_G(x)$, то есть, что $\mathrm{Stab}_G(y) \subseteq g\,\mathrm{Stab}_G(x)g^{-1}$, а это и есть нужное включение в обратную сторону. □

5.7 Основная теорема теории Галуа

Замечание 5.7.1. Отметим, что если $k \subseteq F$ — расширение Галуа, и E — некоторое промежуточное подполе, то расширение $E \subseteq F$ также является расширением Галуа: это сразу следует, например, из условия (1) теоремы 5.5.5. А вот расширение $k \subseteq E$ не обязано быть расширением Галуа. Например, $\mathbb{Q}(\sqrt[3]{2})$ является промежуточным полем между $\mathbb{Q}$ и полем разложения многочлена $t^3 - 2$; это поле разложения имеет степень 6 над $\mathbb{Q}$.

Теорема 5.7.2. *Пусть* $k \subseteq F$ — *расширение Галуа, и* E — *промежуточное поле. Расширение* $k \subseteq E$ *является расширением Галуа тогда и только тогда, когда подгруппа* $\mathrm{Aut}_E(F)$ *нормальна в* $\mathrm{Aut}_k(F)$. *В этом случае имеется изоморфизм* $\mathrm{Aut}_k(E) \cong \mathrm{Aut}_k(F)/\mathrm{Aut}_E(F)$.

Зафиксируем вложение $F \subseteq \overline{k}$ поля F в алгебраическое замыкание поля k. Пусть I — множество вложений $i\colon E \to \overline{k}$, тождественных на k. Заметим, что $i(E) \subseteq F$ для всех $i \in I$. Действительно, расширение $k \subseteq E$ является простым, $E = k(\alpha)$, поэтому i полностью определяется значением $i(\alpha)$, которое должно быть корнем минимального многочлена элемента α над k. Но расширение $k \subseteq F$ нормально и содержит какой-то корень этого многочлена; поэтому F содержит все его корни: $i(\alpha) \in F$ для всех $i \in I$, откуда $i(E) \subseteq F$ для всех $i \in I$.

Определим действие группы $\mathrm{Aut}_k(F)$ на множестве $i \in I$: для $g \in \mathrm{Aut}_k(F)$ и $i \in I$ положим $g(i) = g \circ i \in I$. Заметим, что это действие транзитивно. Действительно, если $i_1, i_2 \in I$, то $i_1(E)$ и $i_2(E)$ содержат k. Поле F является полем разложения некоторого многочлена над k (теорема 5.5.5), поэтому оно является полем разложения того же многочлена над $i_1(E)$ и над $i_2(E)$. Тогда по Предложению 4.2.2 существует автоморфизм $g\colon F \to F$, продолжающий изоморфизм $i_2 \circ i_1^{-1}\colon i_1(E) \to i_2(E)$. Видим, что $g \in \mathrm{Aut}_k(F)$ и $g \circ i_1 = i_2$.

Выберем теперь одно $i \in I$ и отождествим с его помощью E с промежуточным полем в $k \subseteq F$. Тогда $\mathrm{Aut}_E(F) = \mathrm{Aut}_{i(E)}(F)$ является подгруппой в $\mathrm{Aut}_k(F)$, состоящей из таких элементов $\mathrm{Aut}_k(F)$, которые тождественны на $E = i(E)$. Иными словами, $\mathrm{Aut}_E(F)$ является стабилизатором элемента $i \in I$. Значит, I изоморфно множеству левых смежных классов подгруппы $\mathrm{Aut}_E(F)$ в $\mathrm{Aut}_k(F)$ (как множество с действием группы $\mathrm{Aut}_k(F)$).

Доказательство теоремы 5.7.2. Выше мы заметили, что стабилизатором точки $i \in I$ при действии $\mathrm{Aut}_k(F)$ на I является подгруппа $\mathrm{Aut}_{i(E)}(F)$. Стабилизаторы различных точек i сопряжены друг с другом; если $\mathrm{Aut}_E(F)$ нормальна, то $\mathrm{Aut}_{i(E)}(F) = \mathrm{Aut}_E(F)$, откуда по биективности соответствия Галуа следует, что $i(E) = E$ для всех $i \in I$. Значит, расширение $k \subseteq E$ удовлетворяет условию (6) из Теоремы 5.5.5. Поэтому $k \subseteq E$ является расширением Галуа.

Обратно, пусть $k \subseteq E$ — расширение Галуа. Снова по условию (6) Теоремы 5.5.5 получаем, что $i(E) = E$ для всех $i \in I$. Получаем гомоморфизм $\rho\colon \mathrm{Aut}_k(F) \to \mathrm{Aut}_k(E)$ путем ограничения каждого автоморфизма из $\mathrm{Aut}_k(F)$ на $E = i(E)$. Из транзитивности действия $\mathrm{Aut}_k(F)$ на I следует, что этот гомоморфизм сюръективен. Его ядро состоит в точности из тех $g \in \mathrm{Aut}_k(F)$, которые тождественны на E, то есть, совпадает с $\mathrm{Aut}_E(F)$. Значит, подгруппа $\mathrm{Aut}_E(F)$ нормальна и по первой теореме об изоморфизме фактор по ней равен образу ρ, то есть, $\mathrm{Aut}_k(E)$. □

6 Примеры

6.1 Конечные поля

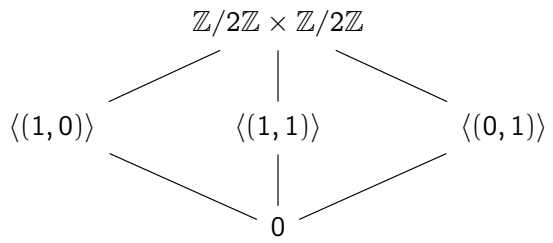
Фактически мы проверили основную теорему теории Галуа «вручную» для конечных полей в разделах 4.6 и 5.2. А именно, любое расширение конечных полей имеет вид $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$, где q — степень простого, $m \geqslant 1$. Это расширение является расширением Галуа, его группа Галуа — циклическая группа C_m порядка m, порожденная автоморфизмом Фробениуса. Несложное упражнение по элементарной теории групп: любая подгруппа циклической группы C_m является циклической и изоморфна группе вида C_d, где $d|m$. Более того, для каждого делителя d числа m есть ровно одна подгруппа вида C_d в C_m: если x — образующая C_m, то $\langle x^{m/d}\rangle \cong C_d$. Это соответствует тому, что в $\mathbb{F}_{q^d}$ является подполем в $\mathbb{F}_{q^m}$ тогда и только тогда, когда $d|m$ (и такое подполе единственно) — см. следствие 4.6.3.

6.2 Некоторые расширения $\mathbb{Q}$

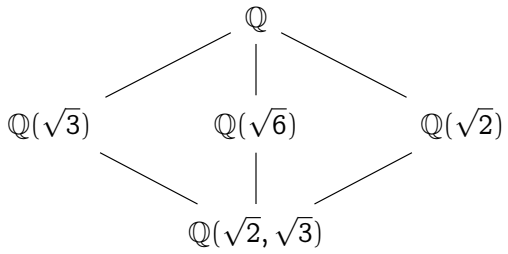
Расширение $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, изученное в примере 3.6.1, является полем разложением многочлена $t^4 - 10t^2 + 1$ над $\mathbb{Q}$, и потому является расширением Галуа. Его группа Галуа состоит из четырех элементов:

- тождественное отображение;
- отображение, переводящее $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ в $a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$;
- отображение, переводящее $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ в $a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$;
- отображение, переводящее $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ в $a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$.

Говоря неформально, второй из перечисленных элементов переводит $\sqrt{2}$ в $-\sqrt{2}$, третий переводит $\sqrt{3}$ в $-\sqrt{3}$, а четвертый является их композицией. Таким образом, группа Галуа этого расширения изоморфна $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, и указанные элементы можно представить как $(0,0), (1,0), (0,1), (1,1)$, соответственно. У группы $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ есть три нетривиальные подгруппы, каждая из которых изоморфна $\mathbb{Z}/2\mathbb{Z}$:



Решетка промежуточных полей, стало быть, выглядит так:



Например, группа, порожденная элементом, который мы обозначили через $(1,0)$, оставляет на месте $\sqrt{3}$ (поскольку ее единственный нетривиальный элемент «меняет знак у $\sqrt{2}$»). Поэтому ей соответствует некоторое расширение степени 2, содержащее $\mathbb{Q}(\sqrt{3})$ — значит, это и есть $\mathbb{Q}(\sqrt{3})$.

6.3 Круговые расширения

Пусть n — натуральное число, $\zeta_n = e^{2\pi i/n}$. У многочлена $x^n - 1$ есть ровно n корней в $\mathbb{C}$, являющихся различными степенями ζ_n. Они образуют циклическую подгруппу порядка n в группе $\mathbb{C}^*$ всех ненулевых комплексных чисел относительно умножения. Эту подгруппу мы будем обозначать через μ_n. Корень n-ой степени из 1, порождающий эту группу, называется **первообразным** корнем степени n из 1. Таким образом, ζ_n^m является первообразным корнем степени n из 1 тогда и только тогда, когда m и n взаимно просты. В частности, первообразных корней степени n равно $\varphi(n)$ штук.

Определение 6.3.1. Многочлен $\Phi_n(x) = \prod(x - \zeta)$, где произведение берется по всем первообразным корням ζ степени n из 1, называется **многочленом деления круга**. Иными словами, $\Phi_n(x) = \prod_{1 \leqslant m \leqslant n, (m,n)=1}(x - \zeta_n^m)$.

Легко видеть, что Φ_n — многочлен степени $\varphi(n)$ со старшим коэффициентом 1. Оказывается, его коэффициенты являются целыми числами, и он неприводим над $\mathbb{Q}$.

Пример 6.3.2. Если $n = p$ — простое число, то любой неединичный элемент μ_p является порождающим; то есть, любой корень степени p из 1 является первообразным, кроме 1. Значит, $\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + \cdots + 1$.

Лемма 6.3.3. *Для всех натуральных n имеем $x^n - 1 = \prod_{1 \leqslant d|n} \Phi_d(x)$.*

Доказательство. Если $n = de$, то любой корень ζ степени d из 1 является и корнем степени n из 1: $\zeta^n = \zeta^{de} = (\zeta^d)^e = 1$. В частности, любой первообразный корень степени d из 1 является корнем степени n из 1. С другой стороны, каждый элемент $\zeta \in \mu_n$ порождает некоторую подгруппу $H \leqslant \mu_n$, и $H = \mu_d$, где d — порядок элемента ζ — является делителем n. Поэтому любой элемент $\zeta \in \mu_n$ является первообразным корнем какой-то степени d из 1, и $d|n$. Это значит, что множество всех корней степени n из 1 совпадает с объединением множеств первообразных корней степени d из 1, где d пробегает все натуральные делители n. □

Следствие 6.3.4. *Коэффициенты многочлена деления круга $\Phi_n(x)$ являются целыми числами.*

Доказательство. Индукция по n. Начнем с $n = 1$: $\Phi_1(x) = x - 1$. Пусть мы уже доказали, что у всех $\Phi_m(x)$ при $m < n$ целые коэффициенты. Перемножим все $\Phi_d(x)$ по всем

делителям n, кроме самого n: $f(x) := \prod_{d|n, 1 \leqslant d < n} \Phi_d(x)$ — это тоже многочлен с целыми коэффициентами и со старшим коэффициентом 1. Поделим $x^n - 1$ с остатком на $f(x)$: $x^n - 1 = f(x)q(x) + r(x)$ для некоторых $q(x), r(x) \in \mathbb{Z}[x]$. С другой стороны, по Лемме 6.3.3 имеем $x^n - 1 = f(x) \cdot \Phi_n(x)$ в $\mathbb{C}[x]$. Значит, $f(x) \cdot (\Phi_n(x) - q(x)) = r(x)$, откуда $r(x) = 0$ (иначе степень $r(x)$ была бы не меньше степени $f(x)$), поэтому $\Phi_n(x) = q(x) \in \mathbb{Z}[x]$. □

Предложение 6.3.5. *Многочлен $\Phi_n(x) \in \mathbb{Z}[x]$ неприводим над $\mathbb{Q}$ (и, следовательно, над $\mathbb{Z}$, поскольку старший коэффициент Φ_n равен 1).*

Доказательство. Без доказательства. □

Определение 6.3.6. Поле разложения $\mathbb{Q}(\zeta_n)$ многочлена $x^n - 1$ над $\mathbb{Q}$ называется **n-ым круговым полем**.

По предложению 6.3.5 поле $\mathbb{Q}(\zeta_n)$ является расширением $\mathbb{Q}$ степени $\varphi(n)$, а $\Phi_n(x)$ — минимальный многочлен элемента ζ_n.

Предложение 6.3.7. *Группа $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ изоморфна группе обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$.*

Доказательство. Мы знаем, что мощность $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ равна $\varphi(n)$ (Предложение 5.1.2; корни различны, поскольку Φ_n сепарабелен). Поэтому достаточно построить инъективный гомоморфизм $j\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$. Возьмем элемент $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^*$ (то есть, обратимый остаток по модулю n) и пусть $j(\overline{m})$ — автоморфизм $\mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$, отправляющий ζ_n в ζ_n^m (образы остальных элементов определяются однозначно). Очевидно, что он не зависит от выбора представителя класса $\overline{m}$. Несложно проверить, что j инъективен и что $(j(\overline{m_1}) \circ j(\overline{m_2}))(\zeta_n) = j(\overline{m_1})(\zeta_n^{m_2}) = \zeta_n^{m_1 m_2} = j(\overline{m_1} \cdot \overline{m_2})(\zeta_n)$, поэтому j является гомоморфизмом. □