Введение в 12-ю проблему Гильберта.

М.Ю.Розенблюм.

Примерно в седьмом классе средней школы любознательный ученик начинает догадываться, что математика - это наука о решении уравнений. Специалисты по теории числел, как правило, продолжают исповедовать эту веру и на более поздних стадиях карьеры. Простейшие уравнения - алгебраические, а среди них - уравнения с одним неизвестным. Цель этого миникурса - ознакомить слушателей с некоторыми идеями и достижениями в этой области, так или иначе связанными с программой исследований, которую принято именовать 12-й проблемой Гильберта.

Рассмотрим сначала квадратное уравнение: $x^2 + px + q = 0$. Принято считать, что формулу, выражающую его корни через коэффициенты, в современном виде выглядящую как , $x_1 = -\frac{p}{2} + \frac{\sqrt{\Delta}}{2}$). $x_2 = -\frac{p}{2} - \frac{\sqrt{\Delta}}{2}$) где $\Delta = p^2 - 4q$ - дискриминант полинома, стоящего в левой части, изобрёл Мохаммед ибн Муса аль-Хорезми в начале IX века. По сути дела, она сводит решение квадратного уравнения к рациональным операциям и решению простейшего квадратного уравнения $y^2 = \Delta$. По причинам, скорее, мистическим, математики постепенно уверились, что для уравнения любой степени с одним неизвестным должна существовать формула, позволяющая выразить его решения, прибегая лишь к рациональным операциям и решению простейших уравнений (т.е. к "извлечению корней"). Если такая формула находилась, говорили, что уравнение решается в радикалах.
Трактат аль-Хорезми был переведен на латынь в XII веке, но очередного успеха пришлось ждать до XVI века. Исследования нескольких математиков, чьи взаимоотношения могли бы послужить сюжетом романисту, привели к так называемой формуле Кардано. Решения уравнения $x^3+px+q=0$, к которому общее кубическое уравнение сводится сдвигом переменой - в случае квадратного уравнения этого сдвига хватило для решения в радикалах -, задаются формулой $x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$, в которой слагаемые нужно выбирать так, чтобы их произведение было равно $-\frac{p}{3}$ (это оставляет как раз три варианта из девяти теоретически возможных).

Надо сказать, что комплексные числа (без которых в этом вычислении не обойтись как раз в случае, когда все три решения исходного уравнения вещественны) не вызвали у Кардано особого восторга, и лишь несколькими десятилетиями позже Рафаэль Бомбелли отнесся к ним всерьез.

Вскоре Феррари справился с уравнением степени 4 (мы разберем этот случай ниже), но затем что-то пошло не так. Подозрение, что в радикалах решается не любое уравнение, постепенно крепли, на рубеже XVIII и XIX веков превратились в уверенность, и наконец, в первой половине XIX века устоявшаяся мечта рухнула. Финальную точку в серии работ (Лагранж, Руффини, Абель) поставил Эварист Галуа. Он сделал нечто большее - открыл новую классификацию уравнений, отличную от очевидной классификации по степени. С обзора теории Галуа мы и начнем.

Бэкграунд.

Предполагается, что слушателям известно, что такое группа. По большей части группы будут выступать, как группы преобразований. Если группа G действует на множествеX, последнее превращается в объединение непересекающихся орбит. Два элемента лежат на одной орбите, если один можно перевести в другой действием группы. Любая подгруппа $H \subset G$ действует на множестве элементов G сдвигами как слева ($g \mapsto hg$), так и справа ($g \mapsto gh$), орбиты этих действий именуются, соответственно, правыми (левыми) смежными классами. Если каждый правый смежный класс является одновременно левым и наоборот, то подгруппа H именуется нормальной, в последнем случае на множестве смежных классов определена структура группы $g_1H \times g_2H = g_1g_2H$, она называется факторгруппой G/H. Далее, любая группа действует на множестве своих элементов $x \in G$ сопряжениями $x \mapsto gxg^{-1}$, орбиты этого действия называются классами сопряженных элементов. В коммутативной группе (иначе называемой абелевой) все подгруппы нормальны, а все классы сопряженных элементов содержат ровно по одному элементу. Нам пригодится теорема о структуре конечных коммутативных групп (доказательство несложно): любая такая группа представляется в виде конечной прямой суммы $G = \oplus\mathbf{Z}/(p_i^{k_i})$ групп вычетов по модулю степеней простых чисел (как числа, так и степени могут повторяться).

Также предполагается, что присутствующие знают, что такое кольцо. Все кольца, о которых пойдет речь, будут коммутативными с единицей. Модуль над кольцом состоит из элементов, которые можно складывать друг с другом и умножать на элементы кольца. Модуль, содержащийся строго внутри кольца, называется идеалом. Факторгруппа аддитивной группы кольца $\mathcal{O}$ по идеалу I имеет структуру кольца, оно называется факторкольцом $\mathcal{O}/I$. Идеал называется простым, если факторкольцо по нему не имеет делителей нуля (такое кольцо ещё называют целостным) и максимальным, если факторкольцо по нему является полем. Любой максимальный идеал, очевидно, прост. Из теоретико-множественной леммы Цорна следует, что любой идеал содержится в некотором максимальном идеале.

Осталось упомянуть про поле. Ядро стандартного гомоморфизма $i : \mathbf{Z} \to k$, при котором 1 переходит в единицу поля, - идеал в $\mathbf{Z}$, неотрицательная образующая этого идеала называется характеристикой поля. $\mathrm{im}\,(i) \simeq \mathbf{Z}/\ker(i)$ - подкольцо в k и, следовательно, не имеет делителей нуля, поэтому характеристика может равняться только нулю или простому числу. Из алгоритма Евклида следует, что в кольце полиномов $k[T]$ с коэффициентами в поле k все идеалы главные. Полином называется неприводимым, если он отличен от константы и не разлагается в произведение полиномов меньшей степени с коэффициентами из k. Поле называется совершенным, если любой неприводимый полином $P \in k[T]$ взаимно прост со своей производной. В частности, поле характеристики 0 совершенно. Мы будем предполагать, что все абстрактные поля, которые нам встретятся, совершенны. Наконец, поле алгебраически замкнуто, если любой неприводимый полином над ним имеет степень 1.

Теория Галуа.

Проще всего построить корень полинома (иными словами, "найти" одно решение уравнения с одной неизвестной) в абстрактной форме. Пусть $P \in k[T]$ - неприводимый полином. Тогда идеал, порожденный P в кольце $k[T]$, максимален. Положим $k_P \stackrel{\text{def}}{=} k[T]/(P)$. Тогда образ T в поле k_P есть корень полинома P.

Отметим, что эта конструкция никак не облегчает поиск решений уравнения внутри конкретного поля (исторически сложилось так, что главный интерес для математиков представляло сначала поле $\mathbf{Q}$ рациональных чисел, затем его пришлось расширить до поля $\mathbf{R}$ действительных чисел, и наконец, до поля $\mathbf{C}$ комплексных чисел). Однако они близко связаны. Пусть поле k содержится в некотором бОльшем поле K, и $\alpha \in K$. Среди всех полиномов $P \in k[T]$, удовлетворяющих условию $P(\alpha) = 0$, если таковые в природе существуют (в этом случае элемент α называется алгебраическим над k), имеется единственный унитарный неприводимый, он называется минимальным полиномом $P_{\alpha,\ K/k}$, а его степень - степенью α над k. Совсем лёгкая теорема говорит, что гомоморфизм $k[T] \to K,\ \ T \mapsto \alpha$ определяет изоморфизм поля k_{P_α} с кольцом $k[\alpha] \subset K$, которое, тем самым, совпадает с полем $k(\alpha) \subset K$.

Пользуясь конструкцией k_P, легко построить алгебраически замкнутое поле, содержащее произвольное поле k. Для этого нужно сначала построить поле K_0, применив конструкцию ко всем неприводимым полиномам одновременно. Иначе говоря, для каждого унитарного неприводимого полинома P выберем свою независимую переменную T_P, и рассмотрим

модуль $I \subset k[T_P]$, порожденный элементами $P(T_P)$. Почти очевидно, что I - идеал (т.е. $1 \notin I$), следовательно, он содержится в некотором максимальном идеале M, и ясно, что в поле $K_0 \stackrel{\text{def}}{=} k[T_P]/M$ любой полином с коэффициентами в k имеет хоть один корень. Затем из поля K_0 таким же образом надо построить K_1 и т.д. , после чего все построенные поля объединить. Очевидно, что получившееся поле будет алгебраически замкнуто. Оно обозначается $\overline{k}$. Чуть позже мы увидим, что поле $\overline{k}$ определено однозначно с точностью до изоморфизма.

Верно ли, что все элементы $\overline{k}$ алгебраичны над k? Чтобы это стало понятно, присмотримся к тому, как ведут себя расширения полей. Если фиксировано вложение полей $k \mapsto K$, будем говорить, что определено расширение K/k. Назовем расширение конечным, если K конечномерно как векторное пространство над k, эта размерность называется степенью расширения. Очевидно, что k_P/k конечно (его степень равна $\deg P$), и почти очевидно, что если K/k и L/K - конечные расширения, то и L/k конечно, и его степень равна произведению степеней "этажей". Простое, но важное замечание: если K/k - конечное расширение, то любой элемент $\alpha \in K$ алгебраичен над k (действительно, его степени не могут быть линейно независимы). Назовем расширение K/k алгебраическим, если все элементы K алгебраичны над k. Из предыдущего легко следует, что если K/k и L/K - алгебраические расширения, то и L/k алгебраично (если $\alpha \in L$ алгебраичен над K, то он алгебраичен и над подполем K. порожденным коэффициентами минимального полинома $P_{\alpha,\,K}$, а последнее конечно над k, поскольку может быть получено последовательным применением конечного числа k_P - конструкций). Теперь ясно, что расширение полей, порожденное произвольным количеством алгебраических элементов, алгебраично. В частности, таковы все этажи башни, использованной при построении алгебраического замыкания, и следовательно, оно само.

Пусть K/k и L/k - два расширения одного и того же поля. Назовем гомоморфизмом $K/k \to L/k$ вложение $K \to L$, оставляющее на месте элементы k. Основной объект изучения в теории Галуа алгебраических расширений - множество $\Sigma_{K/k}^{\overline{k}/k}$ гомоморфизмов $K/k \to \overline{k}/k$. Установим последовательно некоторые свойства этого множества.

1) $\Sigma_{K_P/k}^{\overline{k}/k}$ совпадает с множеством корней полинома P в $\overline{k}$.

2) Если L/K - алгебраическое расширение, то любой элемент $\Sigma_{K/k}^{\overline{k}/k}$ может быть продолжен до некоторого элемента $\Sigma_{L/k}^{\overline{k}/k}$.
Для случая, когда L получается из K применением K_P - конструкции это следует из 1), далее можно применить трансфинитную индукцию)

3) Если K/k и L/K - конечные расширения, то $\#\Sigma_{K/k}^{\overline{k}/k}\#\Sigma_{L/K}^{\overline{k}/K} = \#\Sigma_{L/k}^{\overline{k}/k}$ (здесь мы отождествили $\overline{k}$ и $\overline{K}$).
Для доказательства достаточно проверить, что слои отображения "ограничения на подполе K": $\Sigma_{L/k}^{\overline{k}/k} \mapsto \Sigma_{K/k}^{\overline{k}/k}$ имеют поровну элементов - столько же, сколько и слой над тем вложением $K \to \overline{k}$, которое мы выберем в качестве тождественного.
4) Для конечного расширения $\#\Sigma_{K/k}^{\overline{k}/k} = \deg K/k$.
Это следует из пп. 1) и 3), с учетом того, что поле k совершенно, поэтому полином в 1) не имеет кратных корней в поле $\overline{k}$.
5) Все элементы $\Sigma_{\overline{k}/k}^{\overline{k}/k}$ суть автоморфизмы. Это верно, даже если **оба** $\overline{k}/k$ поменять на произвольное алгебраическое расширение K/k. Действительно, при любом $\alpha \in K$ на корнях $P_{\alpha,k}$ гомоморфизм $\sigma \in \Sigma_{K/k}^{K/k}$ действует перестановками, поскольку не затрагивает коэффициенты полинома, следовательно, σ сюръективен).

Отступление.

Пусть поле k имеет характеристику p. Тогда имеется замечательный гомоморфизм Фробениуса $Fr : k \to k,\ x \mapsto x^p$. Это действительно гомоморфизм: операции умножения и взятия обратного элемента с ним, очевидно, коммутируют, а $(x-y)^p$ по формуле бинома Ньютона есть линейная комбинация выражений $\binom{p}{i}x^i y^{p-i}$, и все биномиальные коэффициенты, кроме первого и последнего, делятся на p.

Это позволило Галуа развить теорию конечных полей. Любой элемент кольца вычетов $\mathbf{Z}/(p)$ обратим, следовательно это поле (стандартное обозначение $\mathbf{F}_p$). Гомоморфизм Фробениуса действует на нём тождественно, значит, $Fr \in \Sigma_{\overline{\mathbf{F}_p}/\mathbf{F}_p}^{\overline{\mathbf{F}_p}/\mathbf{F}_p}$, и по п.5) выше это автоморфизм. Пусть $q = p^r, r \in \mathbf{Z}_{\geq 1}$. Положим $\mathbf{F}_q \stackrel{\text{def}}{=} \{x \in \overline{\mathbf{F}_p} \mid Fr^r(x) = x$ (иными словами, $x^q - x = 0$). Очевидно, это поле.

Пусть, напротив, K - некоторое конечное поле. Оно не может иметь характеристику 0, поскольку $i : \mathbf{Z} \to K$ обязан иметь нетривиальное ядро. Пусть $\operatorname{char} k = p$, тогда K содержит $\mathbf{F}_p$ и является конечномерным векторным пространством над ним размерности, скажем, r. Отсюда $\#K = p^r$, обозначим $q \stackrel{\text{def}}{=} p^r$. По предыдущему $\Sigma_{K/\mathbf{F}_p}^{\overline{\mathbf{F}_p}/\mathbf{F}_p}$ непусто, следовательно, K вкладывается в $\overline{\mathbf{F}_p}$. Поскольку $\#K^* = q - 1$, любой ненулевой элемент образа удовлетворяет уравнению $x^q = 1$, и мы пришли к предыдущей конструкции.

Группа $\mathbf{F}_q^*$ циклична. Это верно для любой конечной подгруппы Γ в мультипликативной группе поля. Действительно, по теореме Безу при любом l количество решений уравнения $x^l - 1 = 0$ не превосходит l. Следовательно, в сумме $\Gamma = \oplus \mathbf{Z}/(p_i^{k_i})$ одно и то же p не может повторяться два раза, поскольку в противном случае нашлось бы p^2 элементов порядка p.

Вернемся к теории Галуа и докажем теорему о примитивном элементе: если K/k - конечное расширение, то $\exists\, \alpha \in K \mid \deg \alpha = \deg K/k$. Это означает, что любое конечное расширение может быть порождено одним элементом или, что то же самое, представлено в виде k_P. Напомню, что речь идёт о совершенных полях. Если поле k конечно, то в качестве порождающего элемента можно выбрать образующую группы K^*. Пусть теперь k бесконечно, и $\deg K/k = n$. Гомоморфизмы $\sigma_i \in \Sigma_{K/k}^{\overline{k}/k} k$ - линейны, их попарные разности $\sigma_i - \sigma_j$ также k - линейны и отличны от нуля, следовательно, $\forall i \neq j \;\; \ker(\sigma_i - \sigma_j)$ - подпространство в K размерности строго меньше n. Поэтому найдется $\alpha \in K$, не лежащий ни в одном из ядер, и при $i \neq j \;\; \sigma_i(\alpha) \neq \sigma_j(\alpha)$. Тем самым, $P_{\alpha,\,k}$ имеет не менее, чем n различных корней, и $\deg \alpha \geq n$.

Осталось дать ключевое для теории Галуа определение: расширение K/k называется нормальным или расширением Галуа, если образы всех гомоморфизмов $\sigma \in \Sigma_{K/k}^{\overline{k}/k}$ совпадают. Нетрудно проверить, что это эквивалентно тому, что любой неприводимый полином $P \in k[T]$ либо не имеет корней в K, либо распадается в K в произведение линейных множителей.

По любому не обязательно неприводимому полиному $P \in k[T]$ можно построить нормальное расширение $k_{P,\,\mathrm{split}}/k$, которое называется полем разложения P. Для этого надо выбрать какое-нибудь алгебраическое замыкание $\overline{k}/k$ и рассмотреть его подполе, порожденное над k всеми корнями полинома P. Очевидно, что это расширение нормально, и легко проверить, что другой выбор алгебраического замыкания приведет к изоморфному расширению.

Любое конечное расширение можно вложить в конечное нормальное расширение: в качестве такового можно взять поле разложения минимального полинома примитивного элемента.

Если полином P неприводим, то его поле разложения $k_{P,\,\mathrm{split}}$ содержит несколько экземпляров поля k_P: по одному для каждого корня полинома. Все эти подполя

изоморфны, но они не обязаны совпадать. Иногда совпадают (например, если $\deg P = 2$), но это довольно редкое явление. Например, если $P \in \mathbf{Q}[T], P(T) = T^3 - 2$, то расширение, порожденное вещественным корнем, не может совпадать ни с одним из двух других. В отличие от случая k_P, никакой простой алгебраической конструкции расширения $k_{P,\,\mathrm{split}}$ не существует, и даже вычисление его степени является весьма нетривиальной задачей.

Отметим, что свойство нормальности не слишком хорошо ведет себя в башнях. Если $k \subset M \subset K$, и K/k нормально, то и K/M нормально, поскольку $\Sigma_{K/M}^{\overline{k}/k} \subset \Sigma_{K/k}^{\overline{k}/k}$. Однако легко привести примеры, когда K/k нормально, а M/k нет (например, если K/k - поле разложения полинома из предыдущего абзаца), а также когда оба этажа башни нормальны, а K/k нет (например, $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt[4]{2})$).

Ясно, что для нормального расширения множество $\Sigma_{K/k}^{\overline{k}/k} = \Sigma_{K/k}^{K/k}$ может быть снабжено структурой группы; её порядок равен $\deg K/k$. Эта группа называется группой Галуа расширения (обозначение $\mathrm{Gal}\,(K/k)$).

Если $H \subset \mathrm{Gal}\,(K/k)$ - подгруппа, то поле неподвижных элементов для неё определяется как $K^H \stackrel{\mathrm{def}}{=} \{x \in K \ , \mid \forall h \in H \ \ h(x) = x\}$.

Основная теорема. Пусть K/k - конечное расширение Галуа, $G = \mathrm{Gal}\,(K/k)$ - его группа Галуа. Тогда
1) Имеется взаимнооднозначное соответствие $\{$подгруппы $H \subset G\} \leftrightarrow \{$ подполя $k \subset M \subset K\}$, определенное при помощи отображений $H \mapsto K^H$, $\mathrm{Gal}\,(K/M) \leftarrow\shortmid M$.
2) M/k нормально $\Leftrightarrow$ $H \lhd G$ (т.е. H - нормальная подгруппа).

Для доказательства заметим, что $K^G = k$ (если $\alpha \in K^G$, то любой элемент $\Sigma_{k(\alpha)/k}^{\overline{k}/k}$ продолжается до элемента G и, следовательно, не действует на α, а это значит, что $\#\Sigma_{k(\alpha/k}^{\overline{k}/k} = 1$ и, тем самым, $k(\alpha)/k$ тривиально). Аналогично, для любого поля M между k и K $M = K^{\mathrm{Gal}\,(K/M)}$ - как отмечалось выше, K/M нормально. Осталось проверить, что $\mathrm{Gal}\,(K/K^H) = H$. По определению, $H \subset \mathrm{Gal}\,(K/K^H)$, так что нужно удостовериться в отсутствии в $\mathrm{Gal}\,(K/K^H)$ "лишних" элементов, то есть доказать неравенство $\deg K/K^H \leq \#H$. Пусть $\alpha \in K$, а $h_1 = \mathrm{Id}, \ldots, h_r$ - максимальный набор элементов H таких, что все $h_i(\alpha)$ различны. Пусть $P(T) \stackrel{\mathrm{def}}{=} \prod_{i=1}^{r}(T - h_i(\alpha))$.

Коэффициенты P *a priori* лежат в K, но на самом деле в K^H, ибо любой элемент из H (не обязательно входящий в список) просто переставляет его корни по предположению о максимальности набора $\{h_i\}$. Следовательно, над полем K^H α имеет степень $\leq \#H$. Применение этого вывода к примитивному элементу для расширения K/K^H завершает доказательство 1). Что касается 2), то достаточно заметить, что для произвольных промежуточного поля M и элемента $g \in \mathrm{Gal}\,(K/k)$ подгруппы $\mathrm{Gal}\,(K/g(M))$ и $g\,\mathrm{Gal}\,(K/M)g^{-1}$ совпадают.

Если расширение M/k нормально, то гомоморфизм ограничения на поле M отождествляет $\mathrm{Gal}\,(M/k)$ с факторгруппой $\mathrm{Gal}\,(K/k)/\mathrm{Gal}\,(K/M)$.

Проверим, что поле $\mathbf{C} \stackrel{\mathrm{def}}{=} \mathbf{R}_{T^2+1}$ алгебраически замкнуто. Пусть $K/\mathbf{R}$ - конечное расширение, при необходимости расширив ещё, будем считать, что оно нормально. По теореме из анализа о среднем значении любой полином нечётной степени над $\mathbf{R}$ имеет корень в $\mathbf{R}$, поэтому у $\mathbf{R}$ нет нетривиальных расширений нечетной степени, следовательно, группа $G = \mathrm{Gal}\,(K/\mathbf{R})$ не имеет собственных подгрупп нечетного индекса. Отсюда легко выводится, что G - 2 - группа, т.е. $\#G$ есть степень двойки, и столь же легко проверить, что любая 2 - группа содержит подгруппу индекса 2. Пусть $H \subset G$ - такая подгруппа. Отвечающее ей по основной теореме расширение $M/\mathbf{R}$ квадратично, и следовательно, изоморфно $\mathbf{C}/\mathbf{R}$. Подгруппа H - тоже 2 - группа, и она должна содержать подгруппу H_1 индекса 2, которой по основной теореме должно соответствовать нетривиальное квадратичное расширение $\mathbf{C}$, а их, как легко проверить, не существует.

Вооружившись теорией, вернемся к классификации уравнений с рациональными коэффициентами. Сопоставим уравнению $P(x) = 0$, где $P \in \mathbf{Q}[T]$ - неприводимый полином, группу Галуа $G = \mathrm{Gal}\,(k_{P,\mathrm{split}}/\mathbf{Q})$. Если $\deg P = n$, то G вкладывается в группу $\mathbf{S}_n$ перестановок корней полинома P в $\mathbf{C}$ (если $g \in G$ тривиально действует на корнях, то он тривиально действует и на всём $k_{P,\mathrm{split}}$, и следовательно, сам тривиален). Соответственно, $\#G$ может принимать значения от n ($\deg k_{P,\mathrm{split}} \geq \deg k_P$) до $n!$.

Нормальное расширение является полем разложения большого количества разных полиномов P. Классическая задача нахождения решений уравнения распадается на две:
1) вычислить какой-нибудь набор элементов, порождающих его поле разложения (мы уже знаем, что всегда можно ограничиться одним - примитивным - элементом, но он может быть слишком сложным, и мы не будем к этому стремиться), и затем

2) выразить решения исходного уравнения через эти образующие.

Мы преимущественно будем заниматься первой задачей, изредка уделяя внимание второй, и основным объектом будет нормальное расширение поля $\mathbf{Q}$ с группой Галуа G.

Но прежде, чем окончательно отвлечься от степени уравнений, посмотрим на то, как новая постановка задачи связана с предыдущей, на примерах уравнений степени $2, 3$ и 4 над произвольным полем. G будет обозначать группу Галуа поля разложения соответствующего полинома.

Если P - неприводимый полином степени 2, то по формуле Виета $k_{P,\,\mathrm{split}} \simeq k_{\mathfrak{p}}$, $G = \mathbf{Z}/(2)$.

Если P - неприводимый полином степени 3, то G - подгруппа $\mathbf{S}_3$, следовательно, $\deg k_{P,\,\mathrm{split}}/k \mid 6$. Но поскольку $k_{P,\,\mathrm{split}}$ содержит поле, изоморфное k_P, его степень равна 6 или 3. В первом случае $G = \mathbf{S}_3$, а во втором G совпадает с единственной подгруппой порядка 3 - подгруппой $\mathbf{A}_3$ четных перестановок.

Для того, чтобы довести вычисление до конца, рассмотрим дискриминант. Напомню, что дискриминант унитарного полинома $P \in k[T]$ задается формулой $\Delta_P \stackrel{\mathrm{def}}{=} \prod_{i<j}(\alpha_i - \alpha_j)^2$, где α_i - корни P в $\overline{k}$. Будучи симметричным относительно всех перестановок корней, дискриминант выражается через коэффициенты полинома P, которые, с точностью до знака, суть элементарные симметрические полиномы от корней. Поэтому $\Delta_P \in k$ и не зависит от выбора $\overline{k}$. Рассмотрим башню полей $k \subset k(\sqrt{\Delta}) \subset k_{P,\,\mathrm{split}}$. Ясно, что $\sqrt{\Delta} \in k \Leftrightarrow$ образ G в $\mathbf{S}_n$ содержится в подгруппе четных перестановок. Если уравнение было кубическим, то в последнем случае $G = \mathbf{A}_3 \simeq \mathbf{Z}/(3)$.
Таким образом, чтобы добраться до поля, содержащего все корни кубического уравнения, надо сначала при необходимости расширить k присоединением $\sqrt{\Delta}$, а затем перейти к циклическому расширению степени 3. Это весьма напоминает формулу Кардано, с двумя важными отличиями, причина которых прояснится ниже. Во первых, квадратный корень извлекают не из дискриминанта (он равен $\Delta = -4p^3 - 27q^2$), а из $-\frac{\Delta}{108}$. Пренебрегая полным квадратом, получаем множитель $\sqrt{-3}$, в котором опытные слушатели узнают иррациональность, входящую в кубический корень из единицы. Во-вторых, вместо перехода к циклическому расширению мы извлекаем кубический корень и пока что не можем сказать, как связаны эти процедуры.

Теперь обратимся к формуле Феррари. Она сводит решение уравнения четвертой степени к решению кубического уравнения. Пусть уравнение вглядит как $x^4 + px^2 + qx + r$. Назовем его резольвентой уравнение $y^3 - 2py^2 + (p^2 - 4r)y + q^2 = 0$. Название появилось тогда же, но в данном контексте не прижилось, поскольку у уравнений более высокой степени удобных резольвент в общем случае не оказалось. Тогда корни исходного уравнения связаны с корнями резольвенты формулами
$y_1 = (x_1 + x_2)(x_3 + x_4)$
$y_2 = (x_1 + x_3)(x_2 + x_4)$
$y_3 = (x_1 + x_4)(x_2 + x_3)$
Это отражение того факта, что подгруппа $\mathbf{V}_4 = \{1, (12)(34), (13)(24), (14)(23)\}$ нормальна в $\mathbf{S}_4$. Поле инвариантов её пересечения с группой Галуа совпадает с полем разложения резольвенты. Сама же подгруппа изоморфна $\mathbf{Z}/(2) + \mathbf{Z}/(2)$. Соответственно, чтобы получить набор x_i из набора y_i, нужно в общем случае дважды решить квадратное уравнение, что соответствует системе уравнений, приведённой выше, если учесть соотношение $\sum x_i = 0$.

Вернемся к общей проблеме решения в радикалах. Что такое извлечение корня? Иначе говоря, какова группа Галуа поля разложения полинома $T^n - b$? Изящный ответ на этот вопрос дал Эрнст Куммер (работа Галуа в этот момент ещё не была опубликована, хотя прошло почти 15 лет со дня его гибели, но, конечно, идеи уже были частью математического фольклора) при одном невинно выглядящем дополнительном условии, которое оказалось ключевым для обозначенной в названии курса проблемы.

Прежде, чем комментировать эту теорему, скажем несколько слов об авторе. Эрнст Эдуард Куммер (1810-1993) был, на мой взгляд, ключевой фигурой в развитии алгебраической теории чисел в XIX веке, и практически все тогдашние специалисты испытали влияние его работ, а Леопольд Кронекер, один из авторов теоремы, упомянутой в анонсе курса, был его непосредственным учеником.

Теорема. Пусть $\operatorname{char} k \nmid n$. Предположим, что полином $T^n - 1$ разлагается в k на линейные множители. Тогда
1) Если $\operatorname{Gal}(K/k) \simeq \mathbf{Z}/(n)$, то $\exists b \in k \mid K \simeq k_{T^n - b}$.
2) $\forall b \in k$ $k_{T^n - b,\ \mathrm{split}}$ - циклическое расширение некоторой степени d, $d|n$.

Пусть K/k - произвольное конечное расширение Галуа с группой G. Определим норму элемента $\alpha \in K$ формулой $N_{K/k}(\alpha) \stackrel{\text{def}}{=} \prod\limits_{g \in G} g(\alpha)$. Норма элемента лежит в k, и нетрудно проверить, что она совпадает с детерминантом линейного оператора

умножения на α в k - линейном пространстве K (в частности, если $\alpha \in k$, то $N_{K/k}(\alpha) = \alpha^{\deg K/k}$). Второе определение годится для любых конечных расширений. Утверждение, входящее в учебники под историческим названием "теорема Гильберта 90" гласит, что в случае, когда K/k - циклическое расширение, а σ - образующая G, то $N_{K/k}(\alpha) = 1 \Leftrightarrow \exists \beta$ такой, что $\alpha = \frac{\sigma(\beta)}{\beta}$. В одну сторону ($\Leftarrow$) она очевидна, а доказательство импликации $\Rightarrow$ мы опустим. Оно короткое и элементарное, но может вызвать вопросы, которые завели бы нас слишком далеко. Пусть теперь ζ - первообразный корень степени n из 1, то есть образующая группы корней из 1 степени n в $\overline{k}$ (эта группа, а) будучи подгруппой в $\overline{k}^*$, циклична; б) благодаря ограничению на характеристику поля, изоморфна $\mathbf{Z}/(n)$, и в) по условию теоремы целиком содержится в k). Применим теорему 90 к ζ (ясно, что $N_{K/k}(\zeta) = \zeta^n = 1$). Найдётся β такой, что $\sigma(\beta) = \zeta\beta$, тогда для $1 \leq i \leq n-1$ $\sigma^i(\beta) = \zeta^i\beta$, и все они различны, следовательно, $\deg_k \beta \geq \deg K/k$, и β порождает K/k. Однако $\sigma(\beta^n) = (\sigma(\beta))^n = (\zeta\beta)^n = \beta^n$, поэтому $\beta^n \in k$, и его можно выбрать в качестве b. Доказательство второй половины теоремы ещё проще, и мы его опустим.

Теперь можно ответить на вопрос о разрешимости уравнения в радикалах. Пусть $P \in \mathbf{Q}[T]$ - неприводимый полином. Будем говорить, что уравнение $P(x) = 0$ разрешимо в радикалах, если поле $\mathbf{Q}_{P,\,\mathrm{split}}$ можно вложить в некоторое поле L, получающееся из $\mathbf{Q}$ последовательным добавлением корней полиномов вида $T^{n_i} - b_i$

Теорема. Уравнение разрешимо в радикалах в том и только в том случае, когда группа $\mathrm{Gal}\,(\mathbf{Q}_{P,\,\mathrm{split}}/\mathbf{Q})$ разрешима (напомню, что конечная группа G называется разрешимой, если существует ряд подгрупп $(1) = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_r = G$ такой, что все факторгруппы H_{i+1}/H_i цикличны).

Действительно, пусть уравнение разрешимо в радикалах. Добавим к полю $\mathbf{Q}$ первообразный корень ζ из 1 степени (НОК всех n_i). Разумеется, $L(\zeta)$ получается из $\mathbf{Q}(\zeta)$ при помощи той же процедуры. По предыдущей теореме расширение $L(\zeta)/\mathbf{Q}(\zeta)$ разрешимо, и осталось проверить только разрешимость группы $\mathrm{Gal}\,(\mathbf{Q}(\zeta)/\mathbf{Q})$. Эта группа даже коммутативна, что мы установим чуть позже. Обратная импликация доказывается схожим образом.

Поскольку группа $\mathbf{S}_n$ при $n \geq 5$ неразрешима, то можно было бы считать, что вопрос закрыт, но необходимо ещё предъявить уравнение с группой Галуа, скажем, $\mathbf{S}_5$. Как это сделать, и вообще, как сосчитать группу Галуа конкретного уравнения - отдельная проблема, способов решения которой мы коснемся позже. Стоит отметить,

что вопрос о том, существует ли конечное расширение Галуа поля $\mathbf{Q}$ с данной группой Галуа, решён на настоящий момент не для всех групп, а только для отдельных их классов. Сравнительно несложно построить расширение $\mathbf{Q}$ с группой Галуа $\mathbf{S}_n$, однако, несмотря на то, что действие сдвигами на множестве собственных элементов определяет вложение произвольной конечной группы в $\mathbf{S}_n$, это не приносит пользы, поскольку в башне расширений $\mathbf{Q} \subset M \subset K$ подгруппа $\mathrm{Gal}\,(K/M) \subset \mathrm{Gal}\,(K/k)$ есть группа Галуа правого, а не левого этажа. Даже построение расширения $\mathbf{Q}$ с циклической группой Галуа, отличной от $\mathbf{Z}/(2)$, требует некоторых усилий, а тот факт, что это можно сделать для любой разрешимой группы, - весьма трудная теорема.

Последовательная процедура решения уравнения в радикалах оставляет чувство неудовлетворенности даже тогда, когда она доступна (в случае разрешимой группы Галуа). Возникает естественный вопрос: нельзя ли, ограничившись каким-то подклассом разрешимых групп, эту процедуру распараллелить. Например, заменим поле $\mathbf{Q}$ на поле $k = \mathbf{Q}(\zeta_n)$. Слегка обобщив предыдущую теорему, можно установить, что конечные расширения Галуа K/k с коммутативной группой Галуа периода n (последнее означает, что в разложении $G = \oplus\mathbf{Z}/(p_i^{k_i})$ все $p_i^{k_i}$ делят n) находятся во взаимнооднозначном соответствии с конечными подгруппами группы $k^*/(k^*)^n$. Немного рискуя остаться непонятым, я всё же укажу, что на самом деле это соответствие порождено граничным гомоморфизмом в последовательности когомологий для точной последовательности Куммера $1 \to \mu_n \to \overline{k}^* \overset{x \mapsto x^n}{\to} \overline{k}^* \to 1$. Сказанное же чуть выше означает, что расширение с группой Галуа такого вида может быть получено путем одновременного извлечения корней разных степеней, делящих n, из элементов поля k.

Вдохновившись этим примером, спросим, а нельзя ли что-то подобное сделать для всех конечных абелевых расширений, не ограничивая размер группы Галуа? Понятно, что основная проблема - что делать с корнями из единицы, которых пришлось бы добавлять всё больше и больше? Например, для основного поля $\mathbf{Q}$ всё это работает только в случае квадратичных расширений. Примерно через десять лет после работы Куммера Леопольд Кронекер высказал гипотезу, что для получения всех абелевых расширений поля $\mathbf{Q}$ достаточно добавить **сами корни из единицы**, но прошло более сорока лет, прежде, чем в 1896 году Давид Гильберт, наконец, ликвидировал все пробелы в доказательстве.

Корни из единицы.

Мы уже видели, что корни полинома $T^n - 1$ в $\mathbf{C}$ образуют циклическую группу порядка n. Пусть G - группа Галуа поля разложения этого полинома (разумеется, при $n > 1$ он приводим). Исследуем действие группы G на корнях. Пусть ζ - первообразный корень, а $g \in G$. Тогда $g(\zeta)$ - также первообразный корень (при $d < n$ равенство $(g(\zeta))^d = 1$ не может выполняться, потому что оно выполнялось бы и для $\zeta = g^{-1}(g(\zeta)))$. Зададим $l(g)$ формулой $g(\zeta) = \zeta^{l(g)}$, тогда $l(g)$ корректно определено как вычет по модулю n (ибо $\zeta^n = 1$), и этот вычет взаимно прост с n по предыдущему замечанию. Далее, $l(gh) = l(g)l(h)$. поэтому $g \mapsto l(g)$ задает гомоморфизм $G \to \mathbf{Z}/(n)^*$ в мультипликативную группу обратимых элементов кольца $\mathbf{Z}/(n)$. Если $g(\zeta) = \zeta$, то $g = \mathrm{Id}$, так как ζ порождает поле разложения, следовательно, этот гомоморфизм - вложение. Первая в ряду идейно важных теорем (пока что довольно простая), доказательства которых я буду вынужден опустить за недостатком времени, утверждает, что на самом деле это не просто вложение, но изоморфизм. Но, по крайней мере, в том, что группа G коммутативна, мы убедились, и это завершает тему решения уравнений в радикалах.

Теорему, которую мы не стали доказывать, можно сформулировать по-иному. Разложим исходный полином в произведение $T^n - 1 = \prod\limits_{d|n} f_d(T)$, где $f_d(T) = \prod\limits_{\omega \in \Omega_d} (T - \omega)$, и последнее произведение берется по всем корням из 1 порядка ровно d. Каждый полином f_d инвариантен относительно действия группы G (как мы уже видели, действие автоморфизма не может изменить порядок корня из 1), поэтому $f_d \in \mathbf{Q}[T]$. На самом деле, по элементарной лемме Гаусса, $f_d \in \mathbf{Z}[T]$. Полиномы f_d называются круговыми, степень каждого их них равна порядку группы $\mathbf{Z}/(d)^*$. Например, $f_1 = T - 1, f_2 = T + 1, f_4 = T^2 + 1, f_p = 1 + T + \ldots T^{p-1}$ при простом p. Задача на дом: проверить, что пропущенная нами теорема утверждает, что все f_d неприводимы. Иными словами, $\mathbf{Q}_{T^{n-1},\,\mathrm{split}} \simeq \mathbf{Q}_{f_n}$.

Стоит подчеркнуть разницу между между корнями из единицы степени n и корнями полиномов $T^n - b$ над полем, в котором эти корни из единицы уже содержатся. В последнем случае группа Галуа вкладывается в группу корней из единицы, изоморфную $\mathbf{Z}/(n)$, а первом - в группу $\mathbf{Z}/(n)^*$, тоже коммутативную, но имеющую совсем другую структуру.

Рассмотрим два примера.

В первом из них построим нормальное (и, следовательно, циклическое) расширение третьей степени поля $\mathbf{Q}$. Первая из групп $\mathbf{Z}/(n)^*$, порядок которой делится на 3, это группа $\mathbf{Z}/(7)^*$. Пусть $\zeta \in \mathbf{C}$ - какой-нибудь первообразный корень. Поскольку 7 - простое число, годится любой, кроме 1, например, $\zeta = \exp(\frac{2\pi i}{7})$. Рассмотрим промежуточное подполе $M = \mathbf{Q}(\tau) = \mathbf{Q}(\zeta + \zeta^{-1}) \subset K = \mathbf{Q}(\zeta)$. Пусть автоморфизм g переводит $\zeta \mapsto \zeta^3$, легко проверить, что g - образующая циклической группы $\mathrm{Gal}\,(K/\mathbf{Q}) = \mathbf{Z}/(7)^* \simeq \mathbf{Z}/(6)$ (в общем случае группа $\mathbf{Z}/(n)^*$ вовсе не обязана быть циклической, но при простом n это так, ибо $\mathbf{Z}/(n)$ - конечное поле). Легко видеть, что на τ уже g^3 действует тождественно, поэтому $\deg M/\mathbf{Q} = 3$. Минимальный полином $P \stackrel{\mathrm{def}}{=} P_{\tau,\,\mathbf{Q}} = (T-\tau)(T-g(\tau))(T-g^2(\tau)) = T^3+T^2-2T-1$ имеет дискриминант $16 \cdot 49$, являющийся полным квадратом, как и ожидалось, поскольку мы уже знаем, что группа Галуа поля $k_{P,\,\mathrm{split}} = k_{\mathfrak{p}}$ изоморфна $\mathbf{Z}/(3)$.

Второй пример сложнее, но универсальнее. Пусть p - нечетное простое число. Для каждого $a \in \mathbf{Z}/(p)$ положим $\chi(a) \stackrel{\mathrm{def}}{=} a^{\frac{p-1}{2}} \mod p$ - это так называемый символ Лежандра. Легко проверить (задача!), что для ненулевых a $\chi(a)$ принимает ровно два значения: 1, если a является квадратом $\mod p$, и -1 в противном случае. Выражение $\tau = \sum\limits_{a \mod p} \chi(a) \exp \frac{2\pi i a}{p}$ называется гауссовой суммой. Различные варианты гауссовых сумм встречаются в теории чисел очень часто. Рутинное вычисление показывает, что $\tau^2 = \chi(-1)p$. Это доказывает теорему Кронекера-Вебера для расширений с группой Галуа $\mathbf{Z}/(2)$.

Для дальнейшего нам понадобится ещё небольшой кусочек теории. Необходим язык, который позволит вести речь о бесконечных расширениях, не прибегая постоянно к оговоркам. Пусть K/k - расширение Галуа, не обязательно конечное. Рассмотрим множество всех его конечных подрасширений Галуа $\{k \subset M \subset K,\ M/k \text{ конечно}\}$, пронумеруем их каким-нибудь множеством индексов I. Подрасширения M_i/k частично упорядочены по включению, и группы $G_i \stackrel{\mathrm{def}}{=} \mathrm{Gal}\,(M_i/k)$ образуют так называемую проективную систему. Это означает, что для любой башни $k \subset M_i \subset M_j \subset K$ определен канонический гомоморфизм групп Галуа $\phi_{ji} : G_j \mapsto G_i$(это стандартная проекция группы на её факторгруппу), и эти гомоморфизмы естественным образом согласованы, когда $M_i \subset M_j \subset M_l$. Определим проективный предел $\varprojlim G_i$ как подмножество $\widehat{G} \subset \prod G_i$ состоящее из таких наборов $\{g_i \in G_i, i \in I\}$, что $\phi_{ji}(g_j) = g_i$

каждый раз, когда $M_i \subset M_j$. Структура группы очевидным образом переносится с групп G_i на группу $\widehat{G}$, и нетрудно видеть, что естественный гомоморфизм $\mathrm{Gal}\,(K/k) \to \widehat{G}$ является изоморфизмом. Действительно, он инъективен, поскольку любой элемент K содержится в каком-то конечном нормальном расширении, и сюръективен, поскольку действие прообраза набора $\{g_i\} \in \widehat{G}$ на элементе $x \in K$ можно задать, используя g_i, отвечающий какому-нибудь M_i, в котором x содержится; от выбора M_i определение не зависит, ибо $g_i(x)$ и $g_j(x)$ оба совпадают с $g_l(x)$, где $M_l = M_i \cap M_j$, по условию согласованности, определяющему проективный предел. Далее эти совпадающие группы мы будем обозначать просто G.

Естественный вопрос: зачем тогда нужна эта конструкция. Ответ таков: проективные пределы семейств конечных групп имеют много хороших свойств, которых нет у абстрактных бесконечных групп. На G можно определить топологию (она называется топологией Крулля), в которой базой окрестностей единицы будут нормальные подгруппы конечного индекса (то есть ядра канонических проекций $G \mapsto G_i$), а остальные открытые множества будут получаться, как объединения их сдвигов. Легко доказать (мы этого делать не будем), что группа G в этой топологии компактна и вполне несвязна (это означает, что для любого $g \in G$ существует открытая компактная окрестность единицы, не содержащая g) . Теперь можно сформулировать основную теорему теории Галуа. Она, как и в случае конечных расширений, устанавливает взаимнооднозначное соответствие между промежуточными подполями $k \subset M \subset K$ (на этот раз расширение M/k не обязано быть конечным) и подгруппами $H \subset G$, но не всеми, а только **замкнутыми**. Ничего странного в этом нет - довольно естественно, что если элементы подгруппы H оставляют какой-то $x \in K$ на месте, то так же ведут себя и близкие к H элементы её замыкания, и они как раз и есть те "лишние" элементы $\mathrm{Gal}\,(K/K^H)$, отсутствие которых нам удалось доказать в случае конечных расширений. Доказательство "бесконечной" версии теоремы - средней сложности домашняя задача.

Тут самое время напомнить определение p - адических чисел. $\mathbf{Z}_p \stackrel{\mathrm{def}}{=} \varprojlim \mathbf{Z}/(p^i)$. Это множество обладает очевидной структурой кольца, и элементарно проверяется, что оно, в отличие от всех, кроме первого, своих конечных этажей, целостно, и что его характеристика равна 0. Любой идеал в $\mathbf{Z}_p$ главный и порождается какой-то неотрицательной степенью числа p (точнее, его образа при вложении $i : \mathbf{Z} \to \mathbf{Z}_p$); эта степень называется p - показателем идеала или любой его образующей и обозначается $\mathrm{v}_p(I)$ (соответственно, $\mathrm{v}_p(a)$). Обратимость элемента a в кольце $\mathbf{Z}_p$ равносильна условию $\mathrm{v}_p(a) = 0$. Поле частных $\mathbf{Z}_p$ (строящееся с помощью дробей

так же, как $\mathbf{Q}$ строится по $\mathbf{Z}$) обозначается $\mathbf{Q}_p$, оно содержит $\mathbf{Q}$. Расширение $\mathbf{Q}_p/\mathbf{Q}$ трансцендентно (ибо уже в $\mathbf{Z}_p$ несчётное множество элементов). На поле $\mathbf{Q}_p$ можно определить абсолютную величину по формуле $||x|| \stackrel{\text{def}}{=} s^{-\mathrm{v}_p(x)}$, где $s > 1$ - фиксированное действительное число, а показатель $\mathrm{v}_p(x)$ определяется как разность показателей числителя и знаменателя. Метрическая топология, определяемая абсолютной величиной, на подкольце $\mathbf{Z}_p$ совпадает с топологией проективного предела

Перейдём к вычислениям. Для начала сосчитаем группу Галуа $\mathrm{Gal}\,(\overline{k}/k)$ для случая, когда $k = \mathbf{F}_p$. Прежде всего, нужно проверить, что k совершенно. Мы можем использовать полученное ранее описание конечных полей, поскольку оно базировалось только на k_P - конструкции, а она применима к любым полям. Согласно этому описанию, любой неприводимый полином над $\mathbf{F}_p$ делит какой-то из полиномов вида $T^{p^r} - T$, а последний не имеет кратных корней в $\overline{\mathbf{F}_p}$ (его производная равна -1), поэтому исходный полином также взаимно прост с производной, что завершает проверку. Любое конечное подполе $\mathbf{F}_q \subset \overline{k}$ есть, как мы знаем, неподвижное поле автоморфизма Fr^r поля $\overline{k}$, где $q = p^r$. Будучи полем разложения полинома $T^q - T$, расширение $\mathbf{F}_q/\mathbf{F}_p$ нормально, и мы уже видели, что оно имеет степень r. Никакая степень автоморфизма Фробениуса, меньшая r, очевидно, не может действовать на $\mathbf{F}_q$ тождественно, поэтому $\{\mathrm{Id}, Fr, \ldots, Fr^{r-1}\}$ - полный список элементов группы Галуа (их должно быть ровно r штук), и $\mathrm{Gal}\,(\mathbf{F}_q/\mathbf{F}_p) \simeq \mathbf{Z}/(r)$, а Fr - её образующая. Тем самым, полная группа Галуа $\mathrm{Gal}\,(\overline{k}/k)$ есть так называемое проконечное пополнение группы $\mathbf{Z}$, а именно, $G = \widehat{\mathbf{Z}} \stackrel{\text{def}}{=} \varprojlim \mathbf{Z}/(r)$. Несложно проверить, что $\widehat{\mathbf{Z}} = \prod_p \mathbf{Z}_p^+$, где $\mathbf{Z}_p^+$ - аддитивная группа кольца $\mathbf{Z}_p$.

Теперь займемся более насущной задачей. Пусть $K/\mathbf{Q}$ - общее поле разложения всех полиномов вида $T^n - 1$. Вычислим группу $\mathrm{Gal}\,(K/k)$. В отличие от предыдущего случая, K содержит нормальные конечные подрасширения, не совпадающие ни с каким из $M_n \stackrel{\text{def}}{=} \mathbf{Q}_{T^n-1,\,\mathrm{split}}$, но любое такое подрасширение в каком-то из полей этого списка содержится, и любые два поля из списка содержатся в каком-то третьем. Простые соображения, на которых мы не будем останавливаться, показывают, что всего этого достаточно для того, чтобы имело место равенство $G = \varprojlim \mathrm{Gal}\,(M_n/\mathbf{Q}) = \varprojlim \mathbf{Z}/(n)^*$. Последняя группа изоморфна $\prod_p \mathbf{Z}_p^*$, где $\mathbf{Z}_p^*$ - мультипликативная группа обратимых элементов кольца $\mathbf{Z}_p$.

Эта группа имеет ещё одну чрезвычайно важную интерпретацию: это факторгруппа по связной компоненте единицы группы классов иделей поля $\mathbf{Q}$. Сперва надо определить, что такое идели. Для начала домножим нашу группу на $\mathbf{R}^*$. Далее увеличим её ещё следующим образом. Разрешим компонентам элемента в произведении принимать значения не только в $\mathbf{Z}_p^*$, но во всей группе $\mathbf{Q}_p^*$, но при этом условимся, что такое будет случаться не более, чем конечное число раз. Получится группа иделей $J_{\mathbf{Q}}$. Группа $\mathbf{Q}^*$ вкладывается в $J_{\mathbf{Q}}$ (отметим, что никакого естественного вложения $\mathbf{Q}^* \to \prod\limits_p \mathbf{Z}_p^*$ указать нельзя), а соответствующая факторгруппа называется группой классов иделей $C_{\mathbf{Q}}$. Понятно, что всегда можно подобрать такое рациональное число, что умножение на него превратит все p - адические компоненты иделя в элементы $\mathbf{Z}_p^*$ (если α - идель, то для этого достаточно выбрать $a \in \mathbf{Q}$ так, чтобы $\forall p \quad \mathrm{v}_p(a) = -\mathrm{v}_p(\alpha_p)$. Знак a можно выбирать произвольно; воспользовавшись этим, можно сделать $\mathbf{R}$ - компоненту иделя α положительной. Мы доказали, что $J_{\mathbf{Q}}/\mathbf{Q}^* = (\mathbf{R}^*)_+ \prod\limits_p \mathbf{Z}_p^*$. Ясно, что связная компонента единицы в этой группе есть $(\mathbf{R}^*)_+ \prod\limits_p \{(1)\}$, и факторизуя по ней, мы получим нашу группу Галуа.

Полезно в явной форме описать действие группы $\prod\limits_p \mathbf{Z}_p^*$ на корнях из единицы. Мы знаем, что при любом n элемент $a \in \mathbf{Z}/(n)^*$ действует на корне из единицы ζ степени n по формуле $\zeta \mapsto \zeta^a$. Не вдаваясь в подробности, отметим, что на самом деле это означает, что элемент $u \in \prod\limits_p \mathbf{Z}_p^*$ (точнее, его образ в $\mathrm{Gal}\left(\mathbf{Q}_{T^n-1,\,\mathrm{split}}\right)$ действует так: компонента u_p на корнях из единицы степеней, не делящихся на p, действует тождественно, а на корнях из единицы степени p^i - по формуле $\zeta \mapsto \zeta_p^u$. Это выражение имеет смысл, поскольку $\zeta^{p^i} = 1$, следовательно, ответ зависит только от вычета $u_p \mod p^i$.

Пусть теперь $K/\mathbf{Q}$ - произвольное конечное расширение. Представим расширение $K/\mathbf{Q}$ в виде $\mathbf{Q}_P/\mathbf{Q}$, где P - неприводимый полином (в качестве P можно взять минимальный полином любого примитивного элемента). Поле $\mathbf{Q}$ канонически вкладывается в $\mathbf{Q}_l$, причём над полем $\mathbf{Q}_l$ полином P не обязан оставаться неприводимым и в общем случае распадается в произведение некоторого числа неприводимых полиномов $P = \prod P_i$. По китайской теореме об остатках (в кольце полиномов над полем она имеет точно такой же вид, как и в $\mathbf{Z}$) кольцо $\mathbf{Q}_l[T]/(P)$ распадется в прямую сумму $\oplus \mathbf{Q}_l[T]/(P_i) = \oplus K_i$. Разумеется, поля K_i - это конечные расширения $\mathbf{Q}_l$, причем можно проверить, что набор классов изоморфизма этих расширений не зависит от выбора полинома P. Рассмотрим подмножество таких элементов в K, что их мимнимальный полином

имеет **целые** коэффициенты. Простое рассуждение показывает, что это подкольцо $\mathcal{O}_K \subset K$, оно называется кольцом целых элементов. Кольцо $\mathcal{O}$ похоже на кольцо $\mathbf{Z}$, в частности, все простые идеалы в нём максимальны (интуитивно это означает, что кольцо "одномерно"), но оно может, в отличие от $\mathbf{Z}$, не быть кольцом главных идеалов. Любой ненулевой идеал в таком кольце распадается в конечное произведение простых идеалов. В частности, главный идеал $l\mathcal{O}_K = \prod \Lambda_i^{e_i}$, где Λ_i - простые идеалы в $\mathcal{O}_K$. Не слишком трудная теорема показывает, что расширения $K_i/\mathbf{Q}_l$, рассмотренные выше, взаимнооднозначно соотетствуют простым идеалам Λ_i. У этого соответствия имеется и третья компонента - это множество различных продолжений l - адической абсолютной величины с поля $\mathbf{Q}$ на поле K.

Если $K/\mathbf{Q}$ - расширение Галуа, картина упрощается. В этом случае все $K_i/\mathbf{Q}_l$ изоморфны, и тоже являются расширениями Галуа, а все показатели e_i (они именуются индексами ветвления) совпадают. Подгруппа в $\mathrm{Gal}\,(K/\mathbf{Q})$, оставляющая на месте идеал Λ_i, называется его подгруппой разложения, и можно проверить, что она изоморфна $\mathrm{Gal}\,(K_i/\mathbf{Q}_l)$. Подгруппы разложения, отвечающие разным идеалам Λ_i, сопряжены.

В случае, если G коммутативна (нас интересует именно он) картина ещё упрощается. Все подгруппы разложения совпадают, и мы получаем однозначно определенную подгруппу $G_l \subset G$, изоморфную группе Галуа расширения $K_0/\mathbf{Q}_l$, определенного с точностью до изоморфизма.

Как устроены расширения поля $\mathbf{Q}_l$? Это сильно зависит от того, равен ли единице индекс ветвления e. Несложно проверить, что для данного конечного расширения Галуа $K/\mathbf{Q}$ он может отличаться от единицы не более, чем для конечного числа простых чисел l (из классической леммы Минковского следует, что хотя бы одно такое l обязательно найдётся). В оставшихся случаях расширение $K_0/\mathbf{Q}_l$ называется неразветвленным, и его группа Галуа устроена особенно просто. Любой элемент кольца $\mathbf{Z}_l$ обладает вычетом по модулю l, который лежит в кольце $\mathbf{Z}_l/(l) \simeq \mathbf{F}_l$. Подкольцо целых чисел в поле $\mathcal{O}_{K_0} \subset K_0$, состоит из элементов, чей минимальный полином имеет коэффициенты, лежащие уже не в $\mathbf{Z}$, а в $\mathbf{Z}_l$. В неразветвленном случае и только в нем $\mathcal{O}_{K_0}/(l)$ также является полем. Это конечное расширение поля F_l, и знаменитая лемма Гензеля о подъёме корней полиномов из $\mathbf{F}_l$ в $\mathbf{Z}_l$ приводит к теореме: $\mathrm{Gal}\,(K_0/\mathbf{Q}_l) \simeq \mathrm{Gal}\,(\mathcal{O}_{K_0}/(l)/\mathbf{F}_l)$. Это означает, что в группе Галуа **л**юбого конечного абелева расширения для каждого простого числа l, над которым $K/\mathbf{Q}$ неразветвлено, содержится так называемый элемент Фробениуса f_l, соответствующий гомоморфизму Фробениуса в расширении полей вычетов.

Например, круговое расширение $\mathbf{Q}_{T^{p^i}-1,\,\mathrm{split}}$ разветвлено только над простым числом p, все остальные f_l действуют на порождающих его корнях из единицы (но не на прочих элементах) возведением в l-ю степень.

Выше мы вычислили действие на корнях из единицы группы Галуа, которая, как мы уже знаем, изоморфна факторгруппе группы классов иделей по связной компоненте единицы $C_{\mathbf{Q}}/D_{\mathbf{Q}} \simeq \prod\limits_l \mathbf{Z}_l^*$. Иделю α с компонентами $\alpha_l \in \mathbf{Q}_l^*$ и $\alpha_\infty \in \mathbf{R}^*$ при отображении $J_{\mathbf{Q}} \to \prod\limits_l \mathbf{Z}_l^*$ соответствует набор $u(\alpha) \stackrel{\mathrm{def}}{=} \{u_l(\alpha) = \frac{\alpha_l}{\mathrm{sgn}(\alpha_\infty)\prod\limits_m m^{\mathrm{v}_m(\alpha_m)}}\}$ (очевидно, что если α - главный идель, то есть элемент образа вложения $\mathbf{Q}^* \to J_{\mathbf{Q}}$, что означает, что все его компоненты совпадают с рациональным числом a, которое каждый раз рассматривается, как элемент соответствующего поля, то все $u_l(\alpha) = 1$). На корнях из единицы степени p^i идель α действует по формуле $\alpha(\zeta) = \zeta^{u_p(\alpha)}$.

Отметим, что идель, все компоненты которого, кроме l - й, равны 1, а пропущенная компонента равна $l^{-1} \in \mathbf{Q}_l$, на корнях из единицы, чья степень не делится на l, действует так же, как элемент Фробениуса f_l.

Теория полей классов, полное изложение которой потребовало бы десятка лекций, утверждает, в частности, что для произвольного конечного абелева расширения $K/\mathbf{Q}$ с группой Галуа G существует единственный гомоморфизм $\psi : J_{\mathbf{Q}} \to G$ (гомоморфизм Артина) такой, что он тривиален на главных иделях, задается формулой $\psi(\alpha) = \prod\limits_l f_l^{\mathrm{v}_l(\alpha_l)}$, если одновременно $\alpha_\infty = 1$ и $\alpha_p = 1$ для всех p, над которыми расширение $K/\mathbf{Q}$ разветвлено, и непрерывен в естественной топологии $J_{\mathbf{Q}}$, базу которой составляют произведения конечного числа произвольных открытых множеств в координатных группах $\mathbf{Q}_l^*$ или $\mathbf{R}^*$ и подмножеств $\mathbf{Z}_l^* \subset \mathbf{Q}_l^*$ в оставшихся координатных группах. В разобранном выше примере $\psi(\alpha) = (u(\alpha))^{-1}$.

Гомоморфизм Артина, как ясно из определения, пропускается через $C_{\mathbf{Q}} = J_{\mathbf{Q}}/\mathbf{Q}^*$, и его конструкции для $K/\mathbf{Q} \subset L/\mathbf{Q}$ согласованы. Можно посчитать ядро гомоморфизма Артина - оказывается, что это произведение $(D_{\mathbf{Q}} = \mathbf{R}_+^*)\mathbf{Q}^* N_{K/\mathbf{Q}}(J_K)$, где $N_{K/\mathbf{Q}}(J_K)$ так называемая норменная подгруппа. Это подгруппа всех элементов $J_{\mathbf{Q}}$, являющихся нормами элементов из группы иделей поля K (отображение нормы определяется той же формулой, что и для самих полей). Переход к пределу устанавливает непрерывный изоморфизм между $C_{\mathbf{Q}}/D_{\mathbf{Q}}$ и группой Галуа $\mathrm{Gal}\,(\mathbf{Q}^{ab}/\mathbf{Q})$ максимального абелева

расширения поля $\mathbf{Q}$ - наименьшего подполя $\overline{\mathbf{Q}}$, содержащего все конечные абелевы расширения. Поскольку все поля, порожденные корнями из единицы, содержатся в $\mathbf{Q}^{ab}$, а группы Галуа совпадают, отсюда следует, что корни из единицы порождают $\mathbf{Q}^{ab}$.

Теория полей классов справедлива и в более широком контексте: изоморфизм Артина $C_K/D_K \simeq \mathrm{Gal}\,(K^{ab}/K)$ имеет место для любых конечных расширений $\mathbf{Q}$. Возникает естественный вопрос: нельзя ли дать прямую конструкцию абелевых расширений и других полей ?

Попытки такого рода математики начали предпринимать ещё в середине XIX века, задолго до того, как появилась теория полей классов. Довольно быстро обнаружилось, что хорошую перспективу имеют мнимоквадратичные поля. Пусть K - такое поле, $\mathcal{O}_K$ - его кольцо целых элементов. Поле K вкладывается в $\mathbf{C}$, легко проверить, что $\mathcal{O}_K$ становится решеткой в $\mathbf{C}$. Факторгруппа аддитивной группы $\mathbf{C}$ по этой решетке представляет собой компактную риманову поверхность (тор), и не слишком сложная теорема показывает, что эту поверхность E (её принято называть эллиптической кривой) можно вложить в двумерное проективное пространство над $\mathbf{C}$, где она будет задаваться уравнениями с коэффициентами, лежащими в K или в его легко контролируемом конечном расширении. Это расширение H/K называется гильбертовым полем классов поля K, оно является максимальным абелевым нигде не разветвленным расширением K, и совпадает с K в точности тогда, когда $\mathcal{O}_K$ является кольцом главных идеалов. В последнем случае кривой можно ограничиться, иначе приходится рассматривать набор кривых $\{E_i = \mathbf{C}/\Lambda_i\}$, соответствующих решеткам, представляющим различные классы идеалов кольца $\mathcal{O}_K$; количество этих классов равно $\deg H/K$.

Кривые E_i наследуют групповую структуру с $\mathbf{C}$, несложная проверка показывает, что групповые операции после задания кривой уравнениями становятся алгебраическими отображениями. Благодаря тому, что умножения на различные элементы $\mathcal{O}_K$ переводит любую решетку Λ_i внутрь себя, имеется много алгебраических отображений $E_i \to E_i$, сохраняющих групповую структуру. Это весьма специальный класс кривых: они называются кривыми с комплексным умножением.

Теория, начавшая развиваться почти одновременно с теорией корней из единицы, и завершенная только в XX веке, много позже того, как Гильберт сформулировал свою проблему, показала, что абелевы расширения поля K проконтролировать можно следующим образом. Прежде всего, множество эллиптических кривых, коэффициенты уравнений которых лежат в данном поле, одномерно: кривая характеризуется так

называемым j - инвариантом, рационально выражающимся через коэффициенты уравнений. К полю K сначала надо добавить все инварианты $j(E_i)$ (получится поле H), а затем добавить координаты точек всех конечных порядков на кривых E_i. Для каждого целого числа n на эллиптической кривой имеется n^2 точек порядка n, поскольку тор - это произведение двух окружностей (стоит вспомнить, что корней из единицы было n, и они лежали на одной окружности) и конструкция сильно напоминает предыдущую. Максимальное абелево расширение мнимоквадратичного поля K порождено добавленными выше элементами.

С тех пор была развита похожая теория ещё для одного класса полей, связанных с многомерными аналогами эллиптических крмвых с комплексным умножением, но в основном проблема явного построения максимального абелева расширения для числовых полей (примерно так формулировал проблему Давид Гильберт) остается нерешённой. Непреодолимые трудности возникают уже в случае вещественноквадратичных полей. Существуют определенные основания полагать, что решение следует искать на фронтах некоммутативной алгебраической геометрии.

Я благодарен И.А. Панину и В.В.Успенскому за ценные замечания по ходу рассказа, а всем слушателям за доброжелательное внимание и подсказки.