Лекция 2. Приложения теории Галуа.

Теорема 2.1. Пусть K поле, $\mathrm{char}K = 0$, $f(x) \in K[x]$ — некоторый неприводимый многочлен. Тогда уравнение $f(x) = 0$ разрешимо в радикалах тогда и только тогда, когда разрешима группа Галуа многочлена f, то есть группа Галуа его поля разложения.

Определение. Уравнение $f(x) = 0$ *разрешимо в радикалах*, если существует поле F, содержащее K и некоторый корень α данного уравнения и являющееся композицией расширений $K = K_0 \subset K_1 \subset \ldots \subset K_m = F$ вида $K_{i+1} = K_i(\sqrt[n_i]{a_i})$, где $a_i \in K_i$.

Определение. *Коммутантом* группы G называется подгруппа G', порожденная элементами вида $[g,h] = ghg^{-1}h^{-1}$, где $g, h \in G$. Группа G *разрешима*, если ряд $G \supset G' \supset G'' \supset \ldots \supset G^{(m)} \supset \ldots$ конечен, то есть существует такое n, что $G^{(n)} = \{e\}$.

Утверждение 2.2. Конечная группа G разрешима тогда и только тогда, когда ее можно представить в виде $\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$, где $G_i \triangleleft G_{i+1}$ и все G_{i+1}/G_i являются циклическими группами.

Применим это для группы Галуа G поля разложения L нашего многочлена f. По основной теореме теории Галуа, представлению G в виде композиции таких расширений групп соответствует соответствует представление поля L как последовательности расширений $K = K_0 \subset \ldots \subset K_n = L$, где K_{i+1}/K_i является расширением Галуа с циклической группой Галуа. Такие расширения полей называются *циклическими*.

Для их изучения рассмотрим сначала круговые расширения.

Определение. Поле разложения L многочлена $x^n - 1$ над полем K называется *круговым* или *циклотомическим* расширением поля K.

Утверждение 2.3. Пусть $(\mathrm{char}K, n) = 1$. Тогда соответствующее круговое расширение является *абелевым* расширением, то есть расширением Галуа с абелевой группой Галуа.

Доказательство. Из условия на характеристику следует, что многочлен $x^n - 1$ сепарабельный, а значит, L/K является расширением Галуа. Рассмотрим в поле L корни n-ой степени из единицы, то есть все корни многочлена $x^n - 1$. Это конечная подгруппа U_n в поле L. Из упражнения 1.7(б) следует, что она циклическая. Пусть $U_n =< \zeta >_n$. Порождающий элемент ζ называется *примитивным* корнем n-ой степени из 1. Обычно он обозначается просто $\sqrt[n]{1}$. Заметим, что $L = K(\zeta)$. Кроме того, группа Галуа $\mathrm{Gal}(L/K)$ действует на U_n, как на группе (то есть каждому элементу g группы

Галуа соответствует некоторый автоморфизм группы U_n), и мы имеем вложение $\mathrm{Gal}(K(\zeta)/K) \hookrightarrow \mathrm{Aut}(U_m) \cong (\mathbb{Z}/n\mathbb{Z})^*$. Значит, $\mathrm{Gal}(K(\zeta)/K)$ абелева.

Сформулируем теперь центральное для нас

Утверждение 2.4.(Теория Куммера.) Пусть $(\mathrm{char} K, n) = 1$, и пусть поле K содержит все корни n-ой степени из 1. Тогда расширение L/K является циклическим степени d, делящей n, тогда и только тогда, когда оно имеет вид $L = K(\sqrt[n]{a})$ для некоторого $a \in K$.

Доказательство. Пусть $L = K(\alpha)$, где $\alpha = \sqrt[n]{a}$. Заметим, что $g(\alpha)/\alpha$ является корнем n-ой степени из 1 (не обязательно примитивным) и лежит в поле K. Это ключевое соображение, ибо таким образом мы получаем гомоморфизм группы Галуа в U_n:

$$g \in \mathrm{Gal}(L/K) \mapsto g(\alpha)/\alpha.$$

Ясно, что это вложение. Значит, $\mathrm{Gal}(L/K)$ является циклической группой некоторого порядка d, который делит n.

Для доказательства утверждения в обратную сторону, то есть для построения a, нам нужна некоторая теорема о "существовании". Введем для начала следующее понятие.

Определение. Пусть L/K расширение Галуа с группой Галуа G. Тогда *нормой Галуа* $N_{L/K}(\alpha)$ элемента $\alpha \in L$ называется следующий элемент поля K:

$$N_{L/K}(\alpha) = \prod_{g \in G} g(\alpha) \in K.$$

Утверждение 2.5.(Теорема Гильберта 90.) Пусть L/K циклическое расширение с группой Галуа $G =< g >_n$. Тогда для любого элемента $\beta \in L$ его норма Галуа равна 1 тогда и только тогда, когда существует элемент $\alpha \in K$ такой, что $\beta = \alpha/g(\alpha)$.

Доказательство. Так как G-орбиты элементов α и $g(\alpha)$ совпадают, то $N_{L/K}(\alpha) = N_{L/K}(g(\alpha))$, и $N_{L/K}(\alpha/g(\alpha)) = 1$. Докажем утверждение в другую сторону. Рассмотрим следующее отображение из поля L в себя:

$$\varphi = \beta g.$$

Наша цель найти ненулевой элемент $\alpha \in L$, неподвижный относительно φ, то есть такой, что $\varphi(\alpha) = \alpha$. Заметим, что, так как $N_{L/K}(\beta) = 1$, то $\varphi^n = \beta g(\beta g(\beta) g^2(\beta) \cdot \ldots \cdot g^{n-2}(\beta) g^{n-1}) = \mathrm{Id}$. Тогда для любого $\gamma \in L$ элемент $\alpha = \psi(\gamma)$ неподвижен относительно φ, где

$$\psi = \mathrm{Id} + \varphi + \ldots + \varphi^{n-1}.$$

Так как g^i являются гомоморфизмами $L^* \to L^*$, а

$$\psi = \mathrm{Id} + \beta g + \beta g(\beta) g^2 + \ldots + \beta g(\beta) g^2(\beta) \cdot \ldots \cdot g^{n-2}(\beta) g^{n-1},$$

то из теоремы Артина о линейной независимости характеров следует существование такого $\gamma \in L$, что $\alpha \neq 0$.

В данном доказательстве мы использовали следующее простое и удивительно общее

Утверждение 2.6.(Теорема Артина о характерах.) Пусть H произвольная группа, K — поле, а $\chi_1, \ldots, \chi_n : H \to K^*$ различные гомоморфизмы групп (*характеры*). Тогда они линейно независимы над K.

Теперь мы достаточно технически подготовлены для того, чтобы завершить доказательство утверждения 2.4.

Окончание доказательства утверждения 2.4. Пусть L/K циклическое расширение степени d, делящей n. Применим теорему Гильберта 90 к $\zeta = \sqrt[d]{1}$: поскольку $\zeta \in K$, и $g(\zeta) = \zeta$, то $N_{L/K}(\zeta^{-1}) = (\zeta^{-1})^d = 1$. Значит, существует такой $\alpha \in L$, что $g(\alpha) = \zeta\alpha$. Действие на него группы Галуа устроено очень просто: $g^i(\alpha) = \zeta^i\alpha$. Значит, у α имеется ровно n различных сопряженных, и, стало быть, $L = K(\alpha)$. Причем $g(\alpha^n) = (g(\alpha))^n = (\zeta\alpha)^n = \alpha^n$, и $a = \alpha^n \in K$.

Вернемся к полю разложения L исходного многочлена f. Теперь ясно, что если бы в поле K были все корни из единицы, то теорема уже была бы доказана из утверждения 2.4. Не стесняясь, добавим его к полю K. Чтобы обосновать данный переход, введем еще одно понятие.

Определение. Пусть $K \subset L_1$ и $K \subset L_2$ два расширения данного поля, причем и L_1, и L_2 содержатся в одном поле F. Тогда их *композитом* называется минимальное поле $L = L_1 \cdot L_2 \subset F$, содержащее и L_1, и L_2.

Утверждение 2.7. Пусть L_1/K и L_2/K два расширения Галуа, $L_1, L_2 \subset F$. Тогда их композит $L = L_1 \cdot L_2$ тоже является расширением Галуа поля K, и $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.
Доказательство Конструтивно, поле L является множеством всевозможных рациональных функций от нескольких элементов полей L_1 и L_2. Поэтому его нормальность и сепарабельность следует из того, что сепарабельные и нормальные (введите это понятие самостоятельно) элементы образуют поле. Мы можем рассматривать ограничение действия группы Галуа $\mathrm{Gal}(L/K)$ на L_1 и L_2. Из вышесказанного также следует, что если у некоторого элемента группы Галуа $\mathrm{Gal}(L/K)$ эти ограничения тривиальны, то он сам тривиален.

Зафиксируем теперь какие-нибудь вложения в $\overline{K}$ поля разложения L многочлена f и кругового расширения $K(\sqrt[n]{1})$ и построим их композит F, где $n = [L : K]$. Тогда из последнего утверждения и из утверждения 2.3 следует, что группа $\mathrm{Gal}(L/K)$ разрешима тогда и только тогда, когда разрешима группа $\mathrm{Gal}(F/K(\sqrt[n]{1}))$. При этом ясно, что уравнение $f(x) = 0$ разрешимо в радикалах над полем K тогда и только тогда, когда оно разрешимо в радикалах над полем $K(\sqrt[n]{1})$ (так как $\sqrt[n]{1}$ — это радикал!). Значит, теорема полностью сведена к полю $K(\sqrt[n]{1})$, а для него она, как уже было сказано, следует из теории Куммера.

Зададимся теперь вопросом: разрешимо ли в радикалах над произвольным полем K произвольное уравнение степени n в том смысле, что для решения уранения существует универсальная формула от его коэффициентов, в которую входят операции сложения, вычитания, умножения, деления и извлечения корня некоторой степени? Существование такой универсальной формулы от коэффициентов означало бы разрешимость в радикалах уравнения $x^n + a_1x^{n-1} + \ldots + a_n$ над полем $K(a_1, \ldots, a_n)$, где $a_1, \ldots, a_n$ алгебраически независимы над K. Как мы выяснили в упражнении 1.9 (г), его группа Галуа изоморфна S_n. Из теории групп известно, что она неразрешима при $n \geq 5$. Значит, уравнения степени большей или равной 5 неразрешимы в общем случае.

У теории Галуа есть применение к построениям циркулем и линейкой. Введем на вещественной плоскости структуру поля комплексных чисел (то есть отметим начало координат, единичный отрезок и проведем вещественную и мнимую оси). Заметим, что тогда циркулем и линейкой можно выполнить любую полевую операцию с двумя данными комплексными числами. Многие задачи на построение могут быть сформулированы в виде: на плоскости комплексных чисел отмечены 1 и несколько (комплексных) чисел $z_1, \ldots, z_n$; требуется построить (комплексное) число z. Анализируя построения точек циркулем и линейкой, то есть как пересечений окружностей и прямых, проходящих через уже построенные точки, можно прийти к выводу, что каждая новая точка w лежит в квадратичном расширении поля $\mathbb{Q}(w_1, \ldots, w_N)$, где $w_1, \ldots, w_N$ — уже построенные точки. Причем циркулем и линейкой мы можем построить любое квадратичное расширение $\mathbb{Q}(w_1, \ldots, w_N)$. Значит, точку z можно построить циркулем и линейкой тогда и только тогда, когда группа Галуа минимального многочлена для z над полем $K = \mathbb{Q}(z_1 \ldots, z_n)$ является 2-группой.

Пример. Рассмотрим задачу построения правильного n-угольника. Она равносильна построению точки $\zeta_n = \sqrt[n]{1}$ когда дана лишь точка 1. Данная задача разрешима тогда и только тогда, когда $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ является 2-группой. Как следует из упражнения 2.1, это в свою очередь равносильно тому, что $\varphi(n)$ является степенью двойки. Например, правильный 16- и 17-угольник можно построить, а 18-угольник нельзя!