Часть 1. Разрешимость в радикалах

Пусть $p(x) \in K[x]$ — неприводимый многочлен над полем K, $\operatorname{char} K = 0$.

Определение 1.1. Будем говорить, что уравнение $p(x) = 0$ разрешимо в радикалах над полем K, если поле разложения L многочлена $p(x)$ является разрешимым расширением поля K, то есть существует башня полей $K = K_0 \subset \cdots \subset K_m$, каждый этаж которой является полем разложения многочлена вида $x^{r_s} - a_s$, и $L \subset K_m$.

Определение 1.2. Цепочка подгрупп $G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1$, называется башней подгрупп. Башня подгрупп называется нормальной, если $\forall 1 \leqslant s \leqslant m-1$ группа G_s нормальна в G_{s-1}; абелевой, если она нормальна и $\forall s$ группа G_{s-1}/G_s абелева; циклической, если она нормальна и $\forall s$ группа G_{s-1}/G_s циклическая. Конечная группа G называется разрешимой, если она обладает абелевой башней.

Теорема 1.3. *Уравнение $p(x) = 0$ разрешимо в радикалах $\iff$ группа Галуа многочлена $p(x)$ разрешима.*

Теорема будет доказана в конце лекции, пока же займемся подготовкой.

Часть 2. Разрешимые группы

Примеры 2.1.
1. Всякая абелева группа разрешима.
2. Группы $\mathfrak{S}_3$ и $\mathfrak{S}_4$ разрешимы.
3. Группы A_n и $\mathfrak{S}_n$ при $n \geqslant 5$ неразрешимы.
4. Группа верхнетреугольных матриц разрешима.

Лемма 2.2. *Всякая подгруппа и всякая факторгруппа разрешимой группы разрешима.*

Доказательство: пусть $G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = 1$ — абелева башня. Если $H \subset G$ — произвольная подгруппа, то $H = H \cap G_0 \supset H \cap G_1 \supset \cdots \supset H \cap G_{m-1} \supset H \cap G_m = 1$ — абелева башня. Действительно, группа $H \cap G_s$ является ядром гомоморфизма $H \cap G_{s-1} \to G_{s-1} \to G_{s-1}/G_s$, следовательно нормальна, а факторгруппа $H \cap G_{s-1}/H \cap G_s$ изоморфна образу этого гомоморфизма, следовательно изоморфна подгруппе абелевой группы G_s/G_{s-1} и, значит, сама абелева. Аналогично, если H — факторгруппа группы G и $f : G \to H$ — естественный эпиморфизм, то $H = f(G_0) \supset f(G_1) \supset \cdots \supset f(G_{m-1}) \supset f(G_m) = 1$ — абелева башня. Действительно, если $g_s \in G_s$, $g_{s-1} \in G_{s-1}$, то $f(g_s)f(g_{s-1})f(g_s)^{-1} = f(g_s g_{s-1} g_s^{-1}) \in f(G_{s-1})$, поэтому $f(G_{s-1})$ нормальна в $f(G_s)$. Кроме того, гомоморфизм $G_s \to f(G_s) \to f(G_s)/f(G_{s-1})$ сюръективен и индуцирует сюръективный гомоморфизм $G_s/G_{s-1} \to f(G_s)/f(G_{s-1})$, следовательно группа $f(G_s)/f(G_{s-1})$ изоморфна факторгруппе абелевой группы G_s/G_{s-1}, и, значит, сама абелева. □

Лемма 2.3. *Группа G разрешима $\iff$ G обладает нормальной башней, в которой все G_{s-1}/G_s разрешимы.*

Доказательство: пусть $G = G_0 \supset \cdots \supset G_m = 1$ — нормальная башня, в которой все группы $H^s := G_{s-1}/G_s$ разрешимы. Выберем абелевы башни $H^s = H^s_0 \supset \cdots \supset H^s_{l_s} = 1$. Обозначим через G^s_t прообраз H^s_t относительно гомоморфизма $G_{s-1} \to G_{s-1}/G_s$. Тогда $G = G^1_0 \supset \cdots \supset G^1_{l_1} = G^2_0 \supset \cdots \supset G^{m-1}_{l_{m-1}} = G^m_0 \supset \cdots \supset G^m_{l_m} = 1$ — абелева башня. □

Лемма 2.4. *Конечная группа G разрешима $\iff$ G обладает циклической башней.*

Доказательство: достаточно заметить, что любая конечная абелева группа обладает циклической башней (докажите!), и применив конструкцию из предыдущего доказательства, собрать циклические башни факторов G_{s-1}/G_s в циклическую башню всей группы. □

Часть 3. Циклические расширения

Определение 3.1. Характером группы G со значениями в абелевой группе A называется гомоморфизм групп $G \to A$.

Теорема 3.2 (Артин)**.** *Любое множество несовпадающих характеров группы G со значениями в K^* (мультипликативной группе поля) линейно независимо в векторном пространстве всех отображений из G в K.*

Доказательство: пусть $\chi_1, \dots, \chi_n$ — минимальный линейно зависимый набор характеров. Ясно, что $n > 1$, так как, подставляя $g = 1$ в соотношение $a_1\chi_1(g) = 0$, получаем $a_1 = 0$. Пусть $a_1\chi_1(g) + \dots + a_n\chi_n(g) = 0$ — линейная зависимость. Тогда $a_i \neq 0$ в силу минимальности. Так как $\chi_1 \neq \chi_2$, то найдется $g_1 \in G$, такое что $\chi_1(g_1) \neq \chi_2(g_1)$. Подставляя в линейную зависимость $g_1 g$, получим $a_1\chi_1(g_1)\chi_1(g) + a_2\chi_2(g_1)\chi_2(g) + \dots = 0$. Вычитая исходную зависимость, умноженную на $\chi_1(g_1)$, получаем $a_2(\chi_2(g_1) - \chi_1(g_1))\chi_2(g) + \dots = 0$. Ясно, что $a_2(\chi_2(g_1) - \chi_1(g_1)) \neq 0$ по построению, поэтому мы получили нетривиальную линейную зависимость между характетрами $\chi_2, \dots, \chi_n$, что противоречит минимальности исходного набора. $\square$

Теорема 3.3 (Гильберта-90)**.** *Пусть L/K расширение Галуа с $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$, σ — образующая группы $\mathrm{Gal}(L/K)$, и $\beta \in L^*$. Тогда $\mathrm{N}_{L/K}(\beta) := \prod_{k=0}^{n-1} \sigma^k(\beta) = 1 \iff$ найдется $\alpha \in L^*$, т.ч. $\beta = \alpha/\sigma(\alpha)$.*

Доказательство: $\Longleftarrow$) очевидно, докажем $\Longrightarrow$). Автоморфизмы σ^k поля L можно рассматривать как характры группы L^* со значениями в группе L^*. В силу их линейной независимости найдется $a \in L^*$, такое что $\alpha = \sum_{k=0}^{n-1} b_k \sigma^k(a) \neq 0$, где $b_k = \beta\sigma(\beta)\dots\sigma^{k-1}(\beta)$. Ясно, что $b_{k+1} = \beta\sigma(b_k)$ при $0 \leqslant k \leqslant n-2$. Кроме того, из условия $\mathrm{N}_{L/K}(\beta) = 1$ следует, что $b_0 = \beta\sigma(b_{n-1})$. Поэтому $\alpha = \beta\sigma(\alpha)$ и остается разделить на $\sigma(\alpha)$. $\square$

Следствие 3.4. *Если L/K — расширение Галуа с $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$, и K содержит все корни степени n из 1, то L — поле разложения многочлена $x^n - a$, $a \in K$.*

Доказательство: пусть β — образующая группы $\mu_n(K) \cong \mathbb{Z}/n\mathbb{Z}$, а σ — образующая группы $\mathrm{Gal}(L/K)$. Тогда $\sigma^k(\beta) = \beta$, значит $\mathrm{N}_{L/K}(\beta) = \beta^n = 1$, следовательно, по теореме Гильберта-90 найдется $\alpha \in L^*$, такое что $\alpha = \beta\sigma(\alpha)$. Тогда $\sigma^k(\alpha) = \beta^{-k}\alpha$. Значит $1, \sigma, \dots, \sigma^{n-1}$ — попарно различные автоморфизмы поля $K(\alpha)$ над K, следовательно $[K(\alpha) : K] \geqslant [K(\alpha) : K]_s \geqslant n = [L : K]$, значит $K(\alpha) = L$. С другой стороны, $\sigma^k(\alpha^n) = \beta^{-kn}\alpha^n = \alpha^n$, значит $\alpha^n \in L^{\mathrm{Gal}(L/K)} = K$, то есть $\alpha^n - a = 0$, $a \in K$. $\square$

Часть 4. Доказательство основной теоремы

Лемма 4.1. *Группа Галуа многочлена $x^r - 1$ абелева.*

Доказательство: заметим, что группа $\mu_r(\overline{K})$ — циклическая группа, а ее порядок равен r, следовательно $\mu_r(\overline{K}) \cong \mathbb{Z}/r\mathbb{Z}$. Пусть ζ — образующая группы $\mu_r(\overline{K})$. Тогда поле разложения многочлена $x^r - 1$ равно полю $K(\zeta)$. Если $\sigma \in \mathrm{Gal}(K(\zeta)/K)$, то $\sigma(\zeta) = \zeta^{k_\sigma}$, $k_\sigma \in \mathbb{Z}/r\mathbb{Z}$. Далее, легко видеть, что $k_{\tau\sigma} = k_\tau \cdot k_\sigma$ в кольце $\mathbb{Z}/r\mathbb{Z}$. Следовательно, $\sigma \mapsto k_\sigma$ — гомоморфизм группы $\mathrm{Gal}(K(\zeta)/K)$ в $(\mathbb{Z}/r\mathbb{Z})^*$, причем очевидно инъективный. Остается заметить, что группа $(\mathbb{Z}/r\mathbb{Z})^*$ абелева. $\square$

Лемма 4.2. *Если поле Kсодержит все корни степени r из 1, то группа Галуа многочлена $x^r - a$ изоморфна $\mu_r(K) \cong \mathbb{Z}/r\mathbb{Z}$.*

Доказательство: если α — корень $x^r - a$, то всякий другой корень имеет вид $\alpha\zeta$, $\zeta \in \mu_r(K)$. Значит поле разложения многочлена $x^r - a$ равно полю $K(\alpha)$. Если $\sigma \in \mathrm{Gal}(K(\alpha)/K)$, то $\sigma(\alpha) = \alpha\zeta_\sigma$, $\zeta_\sigma \in \mu_r(K)$. Далее, легко видеть, что $\zeta_{\tau\sigma} = \zeta_\tau \cdot \zeta_\sigma$ в группе $\mu_r(K)$. Следовательно, $\sigma \mapsto \zeta_\sigma$ — гомоморфизм группы $\mathrm{Gal}(K(\alpha)/K)$ в $\mu_r(K)$. Более того, легко видеть, что это изоморфизм. $\square$

Следствие 4.3. *Группа Галуа многочлена $x^r - a$ разрешима.*

Доказательство: пусть L — поле разложения многочлена $x^r - a$, а L' — поле разложения многочлена $x^r - 1$. Ясно, что $K \subset L' \subset L$, значит по теореме Галуа $\mathrm{Gal}(L/K) \supset \mathrm{Gal}(L/L')$ и $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/L') \cong \mathrm{Gal}(L'/K)$. Остается заметить, что группа $\mathrm{Gal}(L'/K)$ абелева по лемме 4.1, а группа $\mathrm{Gal}(L/L')$ абелева по лемме 4.2. $\square$

Следствие 4.4. *Если уравнение разрешимо в радикалах, то его группа Галуа разрешима.*

Доказательство: пусть $K = K_0 \subset \cdots \subset K_m$ — башня полей из определения 1.1. Пусть $G_s = \mathrm{Gal}(K_m/K_s)$. По теореме Галуа башня $G_0 \supset \cdots \supset G_m$ нормальна, а $G_{s-1}/G_s \cong \mathrm{Gal}(K_s/K_{s-1})$, то есть разрешима по следствию 4.3. Значит группа G_0 разрешима по лемме 2.3. Наконец, по теореме Галуа группа $\mathrm{Gal}(L/K)$ является факторгруппой группы G_0, и в силу леммы 2.2 тоже разрешима. $\square$

Тем самым одно из утверждений теоремы доказано.

Лемма 4.5. *Пусть K_1/K расширение полей и $p(x) \in K[x]$. Если L — поле разложения многочлена $p(x)$ над полем K, а L_1 — поле разложения многочлена $p(x)$ над полем K_1, то группа $\mathrm{Gal}(L_1/K_1)$ изоморфна подгруппе группы $\mathrm{Gal}(L/K)$.*

Доказательство: если $\sigma \in \mathrm{Gal}(L_1/K_1)$, то $\sigma(L) \subset L$, так как L/K нормально, следовательно $\sigma_{|L} \in \mathrm{Gal}(L/K)$. Отображение $\sigma \mapsto \sigma_{|L}$ является гоморфизмом групп $\mathrm{Gal}(L_1/K_1) \to \mathrm{Gal}(L/K)$, ядро которого есть группа всех автоморфизмов поля L_1, неподвижных на L и K_1 одновременно. Если $\alpha_1, \ldots, \alpha_n$ — корни $p(x)$, то $L = K(\alpha_1, \ldots, \alpha_n)$ и $L_1 = K_1(\alpha_1, \ldots, \alpha_n)$, поэтому автоморфизм неподвижный на K_1 и L равен Id_{L_1}. $\square$

Теперь можно завершить доказательство теоремы 1.3. Пусть $p(x) \in K[x]$ многочлен с разрешимой группой Галуа G и L — его поле разложения над K, $[L : K] = n$. Обозначим через K_1 поле, полученное присоединением к полю K всех корней степени n из 1. Расширение $K = K_0 \subset K_1$ будет первым этажом нашей башни. Пусть далее L_1 — поле разложения многочлена $p(x)$ над K_1. По лемме 4.5 группа $\mathrm{Gal}(L_1/K_1)$ изоморфна подгруппе группы G, следовательно по лемме 2.2 разрешима. Выберем ее циклическую башню: $\mathrm{Gal}(L_1/K_1) = G_1 \supset \cdots \supset G_m = 1$. Пусть $K_s = L_1^{G_s}$ — неподвижное поле. Получаем башню $K_1 \subset \cdots \subset K_m = L_1$. По теореме Галуа каждый этаж этой башни является расширением Галуа, причем $\mathrm{Gal}(K_s/K_{s-1}) \cong \mathbb{Z}/r_s\mathbb{Z}$, а $r_s | (G_1 : 1) | (G : 1) = n$, следовательно поле K_{s-1} содержит все корни степени r_s из 1. Значит, согласно следствию 3.4 поле K_s является полем разложения многочлена $x^{r_s} - a_s$ над полем K_{s-1}. Если вспомнить, что поле K_1 является полем разложения многочлена $x^n - 1$ над полем K_0, и $L \subset L_1 = K_m$, то построенная башня полей доказывает разрешимость в радикалах уравнения $p(x) = 0$. $\square$

Часть 5. Случай положительной характеристики

Теорема 1.3 выполняется также и для полей положительной характеристики, если немного изменить определение поля, разрешимого в радикалах. А именно, если $\mathrm{char}\, K = p$, то в башне полей, устанавливающей разрешимость в радикалах поля L, следует также разрешить этажи, в которых K_s является полем разложения многочлена $x^p - x - a_s$, $a_s \in K_{s-1}$ (расширение Артина-Шрайера).

В этом случае, полезной оказывается также аддитивная версия Теоремы Гильберта-90, а именно

Теорема 5.1 (Гильберта-90)**.** *Пусть L/K расширение Галуа с $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$, σ — образующая группы $\mathrm{Gal}(L/K)$, и $\beta \in L^*$. Тогда $\mathrm{Tr}_{L/K}(\beta) := \sum_{k=0}^{n-1} \sigma^k(\beta) = 0 \iff$ найдется $\alpha \in L^*$, т.ч. $\beta = \alpha - \sigma(\alpha)$.*

Доказательство: $\Longleftarrow$) очевидно, докажем $\Longrightarrow$). Автоморфизмы σ^k поля L можно рассматривать как характеры группы L^* со значениями в группе L^*. В силу их линейной независимости найдется $a \in L^*$, такое что $\mathrm{Tr}_{L/K}(a) = \sum_{k=0}^{n-1} \sigma^k(a) \neq 0$. Положим $\alpha = \left(\sum_{k=0}^{n-1} b_k \sigma^k(a)\right) / \mathrm{Tr}_{L/K}(a)$, где $b_k = \beta + \sigma(\beta) + \cdots + \sigma^{k-1}(\beta)$. Ясно, что $b_{k+1} = \beta + \sigma(b_k)$ при $0 \leqslant k \leqslant n-2$. Кроме того, из условия на $\mathrm{Tr}_{L/K}(\beta) = 0$ следует, что $b_0 = \beta + \sigma(b_{n-1})$. Поэтому $\alpha = \beta + \sigma(\alpha)$, и остается вычесть $\sigma(\alpha)$. $\square$

Следствие 5.2. *Если $\mathrm{char}\, K = p$ и L/K — расширение Галуа с $\mathrm{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$, то L — поле разложения многочлена $x^p - x - a$, $a \in K$.*

Доказательство: пусть $\beta = -1$, а σ — образующая группы $\mathrm{Gal}(L/K)$. Тогда $\sigma^k(\beta) = \beta$, следовательно $\mathrm{Tr}_{L/K}(\beta) = \sum_{k=0}^{p-1} \sigma^k(\beta) = p\beta = 0$, следовательно, по теореме Гильберта-90 найдется $\alpha \in L^*$, такое что $\alpha = \sigma(\alpha) - 1$. Тогда $\sigma^k(\alpha) = \alpha + k$. Значит $1, \sigma, \ldots, \sigma^{n-1}$ — попарно различные автоморфизмы поля $K(\alpha)$ над K, следовательно $[K(\alpha) : K] \geqslant [K(\alpha) : K]_s \geqslant p = [L : K]$, значит $K(\alpha) = L$. С другой стороны, $\sigma^k(\alpha^p - \alpha) = (\alpha + k)^p - (\alpha + k) = \alpha^p - \alpha$, значит $\alpha^p - \alpha \in L^{\mathrm{Gal}(L/K)} = K$, то есть $\alpha^p - \alpha - a = 0$, $a \in K$. $\square$