РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ
УНИВЕРСИТЕТ имени А. И. ГЕРЦЕНА

Издательство «Образование»

# МЕТОДИЧЕСКАЯ РАЗРАБОТКА ПО ТЕМЕ „ЭЛЕМЕНТЫ ТЕОРИИ ГАЛУА"

САНКТ-ПЕТЕРБУРГ
1992

Печатается по решению кафедры алгебры и РИСа РГПУ им. А.И. Герцена

В разработке изложены элементы теории Галуа для студентов III-V курсов педагогического университета. Может быть использована для спецкурсов и спецсеминаров при подготовке магистров наук и аспирантов.

Составители: Е.Я. Карачинский, Д.Г.Бенуа, Д.Д. Ломадзе, А.А.Петров, С.А. Севостьянова, А.Г. Тутыгин, Л.В. Лободина, Е.Ю.Яшина

Научный редактор канд. физ-мат. наук, проф. М.М.Лесохин

Рецензенты: д-р физ.-мат. наук, проф. В.С.Виденский



---

Алгебраические уравнения – это уравнения вида $P(x_1,\dots,x_n)=0$, где $P$ – многочлен от переменных $x_1,\dots,x_n$.

Алгебраические уравнения первой степени с одним неизвестным $ax=b$ решали уже в Древнем Египте и Древнем Вавилоне во II тысячелении до н.э. Вавилонские писцы умели решать и квадратные уравнения вида $ax^2+bx+c=0$. С помощью особых таблиц они решали даже некоторые уравнения третьей степени, например, $x^3+x=a$.

Математики средневекового Востока, пользуясь геометрическими методами, исследовали решения кубических уравнений. Однако им не удалось вывести формулу для их решения. Итальянский математик С. дель-Ферро (I465-I526) решил уравнение $x^3+px=q$ и сообщил решение своему ученику А.-М. Фиоре, который вызвал на математический турнир замечательного математика-самоучку Н.Тарталью (I499-I557). За несколько дней до турнира Тарталья нашел общий метод решения кубических уравнений и победил. Однако найденная Тартальей формула для решения уравнения $x^3+px+q=0$

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

была опубликована не им, а итальянским ученым Д.Кардано (I50I-I576), который узнал ее от Тартальи. В это же время Феррари (I522-I565), ученик Кардано нашел решение уравнения четвертой степени. Одной из самых важных задач теории алгебраических уравнений в XVIII-XVIII веках было отыскание формулы для решения уравнения пятой степени. После бесплодных поисков многих поколений алгебраистов усилиями французского ученого Ж. Лагранжа (I736-I8I3), итальянского ученого П. Руффини (I765-I822) и норвежского математика Н. Абеля (I802-I829) в конце XVIII – начале XIX века было доказано, что не существует формулы, с помощью которой можно выразить корни любого уравнения пятой степени через его коэффициенты в радикалах, т.е. используя лишь арифметические операции и извлечение корней.

Эти исследования были завершены работами Э.Галуа (I8II-I832), теория которого позволяет для любого уравнения определить, выражаются ли его корни в радикалах.

# I. РАЗРЕШИМЫЕ ГРУППЫ. ГРУППЫ ПРЕОБРАЗОВАНИЙ

## I. Группы

Определение I. Множество $G$ называется группой, если в нем определено алгебраическое действие "$\circ$", которое ассоциативно; $(\exists e \in G)(\forall a \in G)\, a \circ e = e \circ a = a$ и $(\forall a \in G)(\exists a^{-1} \in G)\, a \circ a^{-1} = a^{-1} \circ a = e$. Если действие коммутативно, то группа называется абелевой. Очевидно, что $(\forall a, b, x \in G)\ (ab)^{-1} = b^{-1}a^{-1}$; $(a^{-1})^{-1} = a$; если $ax = bx$, то $a = b$ (проверьте эти свойства).

Определение 2. Пусть $G$ –группа, $H \subset G$. $H$ называется подгруппой группы $G$, если $(\forall a, b \in H)\ a \circ b \in H$ и $(\forall a \in H)\ a^{-1} \in H$.

Определение 3. Пусть $G$ –группа, $M \subset G$. Подгруппой, порожденной множеством $M$, называется множество $[M] = \{a_1 \circ a_2 \circ \ldots \circ a_i \circ \ldots \circ a_n\}$, где $a_i \in M$ или $a_i^{-1} \in M$, $i \in \{1, \ldots, n\}$. Докажите самостоятельно, что $[M]$ – подгруппа (используя определение 2).

Определение 4. Пусть $G$ –группа, $a \in G$. Множество $[a] = \{a^0 = e, a, a^2, \ldots, a^i, \ldots, a^{-1}, a^{-2}, \ldots, a^{-i}, \ldots\}$ называется циклической подгруппой, порожденной элементом $a$.

Пусть $H$ –подгруппа группы $G$. Рассмотрим бинарное отношение $\sigma_H^{(\lambda)}$ на множестве $G$ такое, что $(a, b) \in \sigma_H^{(\lambda)} \Leftrightarrow ab^{-1} \in H$. Можно доказать, что $\sigma_H^{(\lambda)}$ –эквивалентность (сделайте это самостоятельно). Обозначим через $\bar{a}_{\sigma_H^{(\lambda)}}$ класс по эквивалентности $\sigma_H^{(\lambda)}$, т.е. множество таких элементов, с которыми $a$ находится в отношении $\sigma_H^{(\lambda)}$.

Предложение I. $\bar{a} = Ha = \{x \mid x = ha, h \in H\}$.

Доказательство: $\bar{x} \in \bar{a} \Leftrightarrow (x, a) \in \sigma_H^{(\lambda)} \Leftrightarrow xa^{-1} \in H \Leftrightarrow xa^{-1} = h \Leftrightarrow$ $\Leftrightarrow x = ha \in Ha$.

Множество $Ha$ называется левым классом смежности группы $G$ по подгруппе $H$. (Множество $aH$ называется правым классом смежности).

Ясно, что среди классов смежности есть сама подгруппа $H$ $(H = eH = He)$.

Лемма. Пусть $\bar{a}, \bar{b}$ – два произвольных класса по эквивалентности $\sigma_H^{(\lambda)}$. Тогда существует биекция $\varphi\ \bar{a}$ на $\bar{b}$.

Доказательство: Отношение $\varphi$ зададим следующим образом:

$(x, y) \in \varphi \Leftrightarrow (\exists h \in H):\ x = ha,\ y = hb$



Докажем, что $\varphi$ –функция.

Пусть $\begin{matrix}(a_1, b_1) \in \varphi \\ (a_1, c_1) \in \varphi\end{matrix} \Rightarrow a_1 = h_1 a,\ b_1 = h_1 b,\ c_1 = h_1 b \Rightarrow b_1 = c_1$.

Будет ли $\varphi$ отображением?

Пусть $x \in Ha \Rightarrow x = ha$. Положим $y = hb \in Hb$. По определению $\varphi$. $(x, y) \in \varphi$, значит, $\varphi$ –отображение.

Возьмем $x_1 \neq x_2$. Допустим, что $\varphi(x_1) = \varphi(x_2)$.

$x_1 = h_1 a$, $\varphi(x_1) = h_1 b$

$x_2 = h_2 a$, $\varphi(x_2) = h_2 b$  $\varphi(x_1) = \varphi(x_2) \Rightarrow h_1 = h_2 \Rightarrow$

$\Rightarrow x_1 = x_2$, что противоречит выбору $x_1$ и $x_2$. Получили, что $\varphi$ –инъекция. Осталось показать, что $\varphi$ является сюръекцией.

Пусть $y \in Hb \Rightarrow y = hb$. Рассмотрим $x = ha \in Ha$. По определению $\varphi$ $(x, y) \in \varphi$, что и означает сюръективность $\varphi$. Таким образом, доказано, что $\varphi$ –биекция. Следовательно, любые два класса смежности равномощны (т.е. имеют одинаковое количество элементов).

ТЕОРЕМА I. (ЛАГРАНЖА). Пусть $G$ –группа, содержащая $n$ элементов, $H$ –подгруппа, содержащая $m$ элементов. Тогда $n \vdots m$.

Доказательство: Рассмотрим отношение $\sigma_H^{(\lambda)}$. Это эквивалентность, значит, можно говорить о классах по этой эквивалентности. Среди этих классов есть сама подгруппа $H$ (смотри выше). По лемме все классы содержат одинаковое количество элементов, значит, количество элементов в группе $G$ есть число, кратное количеству элементов в подгруппе $H$, т.е. $n \vdots m$ (классы не пересекаются и в объединении дают всю группу $G$). Теорема доказана.

Следствие. Если $G$ –группа, содержащая $p$ элементов ($p$ – простое число), то $G$ – циклическая группа. В самом деле, $G \neq \{e\}$ (I – не простое число!). Пусть $a \in G$, $a \neq e$. Рассмотрим подгруппу $[a]$, содержащую $k$ элементов, $k \neq 1$ и $p \vdots k$ (по теореме Лагранжа), следовательно, по свойству простых чисел $k = p \Rightarrow$ $G = [a]$, т.е. $G$ – циклическая группа.

Определение 5. Пусть $N$ – подгруппа группы $G$. $N$ называется нормальным делителем $G$, если $(\forall x \in G)\ xN = Nx$.

ТЕОРЕМА 2. Пусть $G$ – группа, $N$ – ее подгруппа. $N$ является нормальным делителем $G$ тогда и только тогда, когда

$$(\forall x\in G)(\forall n\in N)\ xnx^{-1}\in N.$$

Доказательство: Пусть $N$ – нормальный делитель $G$ . Возьмем произвольное $x\in G$ . Известно, что $xN=Nx$.

$$(\forall n\in N)\ xnx^{-1}=\bar{n}xx^{-1}=\bar{n}\in N.$$

Обратное утверждение докажите самостоятельно. Теорема доказана.

Предложение 2. Пусть $G$ – группа, $N$ – ее подгруппа. $N$ является нормальным делителем $G$ тогда и только тогда, когда левое и правое разбиение $G$ на классы смежности по $N$ совпадают.

Доказательство очевидно следует из определения 5.

Определение 6. Пусть $G$ – группа, $N$ – нормальный делитель группы $G$ . Фактор-группой группы $G$ по нормальному делителю $N$ называется множество $G/N$ всевозможных классов по эквивалентности $\sigma_N$ .

Действие в множестве $G/N$ зададим так: $\bar{a}_{\sigma_N}\cdot\bar{b}_{\sigma_N}=\overline{a\cdot b}_{\sigma_N}$

Докажем, что фактор-множество относительно введенного в ней алгебраического действия является группой. Для этого сначала покажем, что введенное действие не зависит от выбора представителей классов: пусть $\bar{a}_1=\bar{a}_2,\ \bar{b}_1=\bar{b}_2\ \Rightarrow (a_1,a_2)\in\sigma_N,\ (b_1,b_2)\in\sigma_N$

Это значит, что $a_1a_2^{-1}\in N,\ b_1b_2^{-1}\in N$.

$$a_1b_1b_2^{-1}a_2^{-1}=a_1\underbrace{b_1b_2^{-1}}_{n_N}a_1^{-1}\underbrace{a_1a_2^{-1}}_{n_N}\in N,$$ а тогда

$$(a_1b_1,\ a_2b_2)\in\sigma_N\Rightarrow\overline{a_1b_1}=\overline{a_2b_2}\Rightarrow\bar{a}_1\cdot\bar{b}_1=\bar{a}_2\cdot\bar{b}_2$$

Теперь докажем, что действие ассоциативно: возьмем произвольные элементы $\bar{a},\bar{b},\bar{c}$ из $G/N$: $\bar{a}(\bar{b}\bar{c})=\bar{a}\cdot\overline{bc}=\overline{a(bc)}=\overline{(ab)c}=\overline{ab}\cdot\bar{c}=(\bar{a}\cdot\bar{b})\bar{c}$ (мы воспользовались ассоциативностью в $G$ и определением действия в $G/N$).

Найдем единицу в $G/N$ . В $G$ есть $e$ . Рассмотрим элемент $\bar{e}\in G/N$ . Имеем : $(\forall\bar{a}\in G)\ \bar{a}\cdot\bar{e}=\overline{ae}=\bar{a}$ . Покажем, что $\bar{a}^{-1}=\overline{a^{-1}}$ . Действительно, $\bar{a}\,\overline{a^{-1}}=\overline{aa^{-1}}=\bar{e}$ .

Следовательно, фактор-множество является группой относительно введенного выше действия. Элементами фактор-группы являются классы по эквивалентности $\sigma_N$ (которые в силу леммы состоят из одинакового количества элементов).

Определение 7. Пусть $G$ – группа с алгебраическим действием $\cdot$,



$\bar{G}$ – группа с алгебраическим действием $*$ . Отображение $\varphi$ : $G\to\bar{G}$ называется гомоморфизмом, если $(\forall a,b\in G)$

$$\varphi(a\cdot b)=\varphi(a)*\varphi(b).$$

Если $\varphi$ – биекция, то это отображение называется изоморфизмом $G$ на $\bar{G}$ (сами группы тогда называют изоморфными и обозначают $G\approx\bar{G}$ ).

Свойства гомоморфизма.

1 $\varphi(e)=\bar{e}$

2 $\varphi(a^{-1})=\varphi(a)^{-1}\ (\forall a\in G)$

Докажите эти свойства самостоятельно.

Предложение 3. Пусть $\varphi$ – гомоморфизм группы $G$ в группу $\bar{G}$.

Тогда ядро $\varphi$ . $Ker\,\varphi=\{x\in G\mid\varphi(x)=\bar{e}\}$ – нормальный делитель $G$ , а образ $\varphi$ $Im\,\varphi=\{y\in\bar{G}\mid(\exists x\in G)\,\varphi(x)=y\}$ подгруппа $\bar{G}$.

Доказательство:

1) Покажем, что $Ker\,\varphi$ – подгруппа.

Пусть $x_1,x_2\in Ker\,\varphi\Rightarrow\varphi(x_1)=\varphi(x_2)=\bar{e}\Rightarrow$

$\varphi(x_1\cdot x_2)=\varphi(x_1)\cdot\varphi(x_2)=\bar{e}\cdot\bar{e}=\bar{e}\Rightarrow x_1x_2\in Ker\,\varphi$.

Пусть $x\in Ker\,\varphi\Rightarrow\varphi(x)=\bar{e}\Rightarrow\varphi(x^{-1})=\varphi(x)^{-1}=\bar{e}^{-1}=\bar{e}\Rightarrow$ $\Rightarrow x^{-1}\in Ker\,\varphi$ (мы использовали определение ядра и гомоморфизма, а также 2 свойство).

Возьмем теперь $x\in G$ и $t\in Ker\,\varphi$.

$\varphi(x^{-1}tx)=\varphi(x^{-1})\varphi(t)\varphi(x)=\varphi(x)^{-1}\cdot\bar{e}\,\varphi(x)=\varphi(x)^{-1}\varphi(x)=\bar{e}\Rightarrow$ $\Rightarrow x^{-1}tx\in Ker\,\varphi$ , что по теореме 2 означает, что $Ker\,\varphi$ – нормальный делитель $G$.

2) Покажем, что $Im\,\varphi$ – подгруппа.

Пусть $y_1\in Im\,\varphi,\ y_2\in Im\,\varphi\Rightarrow(\exists x_1,x_2\in G)\ \varphi(x_1)=y_1,\ \varphi(x_2)=y_2$, $\varphi(x_1\cdot x_2)=\varphi(x_1)\varphi(x_2)=y_1\cdot y_2$ , т.е. для $y_1y_2$ есть прообраз. $\varphi(x^{-1})=\varphi(x)^{-1}=y^{-1}$.

Пусть $y\in Im\,\varphi$ , т.е. для $y^{-1}$ есть прообраз.

Получили, что $y_1\cdot y_2,\ y^{-1}\in Im\,\varphi$ , что и требовалось.

ТЕОРЕМА 3. Пусть $\varphi$ – гомоморфизм $G$ в $\bar{G}$ . Тогда существует изоморфизм $\psi$ $G/Ker\,\varphi$ на $Im\,\varphi$

Доказательство: Установим соответствие $\psi$ между множествами $G/Ker\,\varphi$ и $Im\,\varphi$

Положим $\Psi(\bar{a}_{\sigma_{\ker\varphi}}) = \varphi(a)$ , где $\bar{a}_{\sigma_{\ker\varphi}}$ – класс группы $G$ , по ядру гоморфизма $\varphi$ , т.е. $\bar{a}_{\sigma_{\ker\varphi}} \in G/\ker\varphi$ , а $\varphi(a) \in \Im m\,\varphi$.

Покажем, что найденное соответствие является биекцией.

а) Будет ли $\Psi$ функцией?

Пусть $\bar{a}_\sigma = \bar{b}_\sigma$ (для простоты будем писать $\sigma$ вместо $\sigma_{\ker\varphi}$). Тогда по определению функции нужно показать, что $\Psi(\bar{a}_\sigma) = \Psi(\bar{b}_\sigma)$. Так как $\bar{a}_\sigma = \bar{b}_\sigma$ , то $(a,b) \in \sigma$ и по определению $\sigma$ имеем: $ab^{-1} \in \ker\varphi$ , т.е. $\varphi(ab^{-1}) = e$, $\varphi(a)\varphi(b^{-1}) = \bar{e}$. Умножим последнее равенство на $\varphi(b)$. Получим: $\varphi(a)\varphi(b^{-1})\varphi(b) = \bar{e}\,\varphi(b)$, $\varphi(a) = \varphi(b)$. По определению $\Psi$ $\varphi(a) = \Psi(\bar{a}_\sigma)$, $\varphi(b) = \Psi(\bar{b}_\sigma)$. Следовательно, $\Psi(\bar{a}_\sigma) = \Psi(\bar{b}_\sigma)$ , а это значит, что $\Psi$ – функция.

б) Будет ли $\Psi$ отображением? Нужно показать, что $\Psi$ определено для всякого элемента из фактор-группы $G/\ker\varphi$. Пусть $\bar{a}_\sigma \in G/\ker\varphi$. Тогда $\bar{a}_\sigma$ состоит из тех и только тех элементов группы $G$ , которые находятся с $a$ в отношении $\sigma$ . Но $\sigma$ – эквивалентность, следовательно, $\sigma$ рефлексивно, значит, $a \in \bar{a}_\sigma$ . Так как $\varphi$ – гомоморфизм, значит, $\varphi$ всюду определен на $G$ , значит $\varphi(a)$ определено и принадлежит $\Im m\,\varphi$ . Отсюда получаем, что $\Psi$ – отображение.

в) Покажем, что $\Psi$ – инъекция.

Пусть $\bar{a}_\sigma \neq \bar{b}_\sigma$ , но $\Psi(\bar{a}_\sigma) = \Psi(\bar{b}_\sigma)$.

Отсюда $\varphi(a) = \varphi(b)$, $\varphi(ab^{-1}) = \bar{e} \Rightarrow ab^{-1} \in \ker\varphi \Rightarrow (a,b) \in \sigma$, т.е. $\bar{a}_\sigma = \bar{b}_\sigma$ , но это невозможно, значит, $\Psi$ – инъекция.

г) Докажем, что $\Psi$ – сюръекция.

Пусть $y \in \Im m\,\varphi$. Найдем для него $\bar{x}_\sigma \in G/\ker\varphi$. Так как $y \in \Im m\,\varphi$, то $(\exists x \in G)$ $\varphi(x) = y$ . Рассмотрим $\Psi(\bar{x}_\sigma)$. Видим, что $\Psi(\bar{x}_\sigma) = \varphi(x) = y$ , следовательно, $\Psi$ – сюръекция, значит, биекция. Осталось показать, что $\Psi(\bar{a}_\sigma \cdot \bar{b}_\sigma) = \Psi(\bar{a}_\sigma) \cdot \Psi(\bar{b}_\sigma)$ . Имеем: $\Psi(\bar{a}_\sigma \bar{b}_\sigma) = \Psi(\overline{ab}_\sigma) = \varphi(ab) = \varphi(a)\varphi(b) = \Psi(\bar{a}_\sigma)\Psi(\bar{b}_\sigma)$ (мы воспользовались определением умножения в фактор-группе и тем, что $\varphi$ – гомоморфизм).

Итак, доказано, что $G/\ker\varphi \approx \Im m\,\varphi$ . Теорема доказана.

Определение 8. Группой преобразований множества $M$ называется некоторое множество биективных преобразований $S(M)$ , обладающее свойствами:



I) $(\forall f,g \in S(M))$ $f \circ g \in S(M)$

2) $(\forall f \in S(M))$ $f^{-1} \in S(M)$.

Очевидно, что относительно композиции преобразований $S(M)$, образует группу.

## 2. Коммутаторы и коммутант

Определение I. Пусть $G$ – группа; $x, y \in G$. $K_{x,y} = x^{-1}y^{-1}xy$ называется коммутатором элементов $x$ и $y$.

ПРИМЕР. В группе всех квадратных неособенных матриц второго порядка для элементов $x = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $y = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}$

$K_{x,y} = x^{-1}y^{-1}xy = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \times$ коммутатор

$\times \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -3 & -4 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -3 & -10 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix} =$

$= \begin{pmatrix} 7 & 4 \\ -2 & -1 \end{pmatrix}$

(вспомнить, как ищется обратная матрица, а также правило умножения матриц).

Свойства коммутаторов.

$I^0$. В абелевой группе все коммутаторы равны $e$ ( $e$ – единица группы). И обратно: если все коммутаторы равны $e$ , то группа абелева.

Доказательство: Пусть $G$ – абелева группа, тогда

$$K_{x,y} = x^{-1}y^{-1}xy = x^{-1}xy^{-1}y = ee = e. \quad (\forall x,y \in G)$$

обратно: если $x^{-1}y^{-1}xy = e$ , то $xx^{-1}y^{-1}xy = xe$ ,

$$y^{-1}xy = x,$$

$$yy^{-1}xy = yx,$$

$(\forall x,y \in G)$ $xy = yx$ , т.е. $G$ – абелева группа.

$2^0$. $xy = yx \cdot K_{x,y}$

Действительно, $yx \cdot K_{x,y} = yxx^{-1}y^{-1}xy = yey^{-1}xy = xy$.

$3^0$. Обратный к коммутатору – коммутатор:

$K^{-1}_{x,y} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = K_{y,x}$.

$4^0$. Если $z = K_{x,y}$ , то $(\forall a \in G)(\exists u,v \in G)$ $aza^{-1} = K_{u,v}$.

Доказательство: Нужно доказать, что $(\forall a \in G)(\exists u,v \in G)$ $ax^{-1}y^{-1}xya^{-1} = u^{-1}v^{-1}uv$.

$$ax^{-1}y^{-1}xya^{-1} = ax^{-1}ey^{-1}e\,xeya^{-1} = axa^{-1}aya^{-1}a^{-1}axa^{-1}aya^{-1} =$$
$$= u^{-1}v^{-1}uv, \text{ где } u = axa^{-1},\ v = aya^{-1}$$
$$(u^{-1} = (axa^{-1})^{-1} = ax^{-1}a^{-1},$$
$$v^{-1} = (aya^{-1})^{-1} = ay^{-1}a^{-1}).$$

Определение 2. Пусть $G$ – группа, $M$ – множество всех коммутаторов элементов $x, y \in G$.

Множество $K = [M]$ называется коммутантом группы $G$.

ПРИМЕР. В группе всех квадратных неособенных матриц второго порядка коммутант – это подгруппа матриц с определителем +I, так как для коммутатора $K_{x,y}$

$K_{x,y} = x^{-1}y^{-1}xy$ $\quad (x, y$ – матрицы)

$\mathcal{D}(K_{x,y}) = \mathcal{D}(x^{-1}y^{-1}xy) = \mathcal{D}(x^{-1})\mathcal{D}(y^{-1})\mathcal{D}(x)\mathcal{D}(y) = \mathcal{D}(x^{-1}x)\mathcal{D}(y^{-1}y) =$

$= \mathcal{D}(e)\mathcal{D}(e) = 1 \cdot 1 = 1$ (вспомнить об определителе произведения матриц), и поэтому порождающее множество состоит только из матриц с определителем I.

Свойство коммутанта. Пусть $G$ – группа, $K$ – ее коммутант.

$K = e \iff G$ – абелева.

Доказательство очевидно следует из свойства I° коммутаторов и определения коммутанта.

ТЕОРЕМА (О КОММУТАНТЕ). Пусть $G$ – группа, $K$ – ее коммутант. Тогда

I) $K$ – нормальный делитель $G$,

2) $G/K$ – абелева группа,

3) если $N$ – нормальный делитель $G$, $G/N$ – абелева, то $K \subset N$.

Доказательство:

I) возьмем $k \in K$; $k = K_{x_1,y_1} \cdot K_{x_2,y_2} \cdot \ldots \cdot K_{x_t,y_t}$ (использовано свойство 3° коммутаторов). $(\forall a \in G)\ aka^{-1} = a K_{x_1,y_1} a a^{-1} K_{x_2,y_2} a a^{-1} \ldots a K_{x_t,y_t} a^{-1}$. Используя свойство 4° коммутаторов, получим, что $aka^{-1} = K_{u_1,v_1} \cdot K_{u_2,v_2} \cdot \ldots \cdot K_{u_t,v_t} \in K$, $u_i, v_i \in G$, $i \in \{1, \ldots, t\}$, а тогда



$K$ – нормальный делитель $G$ (смотри соответствующую теорему 2 в §I).

2) Пусть $\bar{x}, \bar{y} \in G/K$. Нужно доказать, что $\bar{x}\bar{y} = \bar{y}\bar{x}$.
$\bar{x}\bar{y} = xKyK = xyK$; $\bar{y}\bar{x} = yKxK = yxK$.

Покажем, что $xyK = yxK$.

$z \in xyK \iff z = xyk,\ k \in K \iff z = xyK_{u_1,v_1} \cdot \ldots \cdot K_{u_t,v_t} \iff$
$\iff z = yx\,K_{x,y} \cdot K_{u_1,v_1} \cdot \ldots \cdot K_{u_t,v_t}$

(по свойству 2° коммутаторов), а это означает, что $z \in yxK$.

3) Пусть $N$ – нормальный делитель $G$. Докажем, что любой коммутатор элементов $x, y \in G$ принадлежит $N$.

Если рассмотреть разбиение $G$ на классы по $N$, то

$K_{x,y} = x^{-1}y^{-1}xy \in x^{-1}y^{-1}xyN = x^{-1}Ny^{-1}NxNyN =$
$= x^{-1}NxNy^{-1}NyN = x^{-1}xNy^{-1}yN = N \cdot N = N.$

(мы использовали правило умножения классов в фактор-группе и то, что $G/N$ – абелева).

Поскольку $N$ – подгруппа и $K_{x,y} \in N$ для всех $x, y \in G$ то и произведение коммутаторов будет принадлежать $N$, т.е. $K \subset N$. Теорема доказана.

## 3. Разрешимые группы

Определение. Группа $G$ называется разрешимой, если ряд последовательных коммутантов

$G = K_0 \supset K_1 \supset \ldots \supset K_i \supset K_{i+1} \supset \ldots \supset K_n = e$

($K_{i+1}$ – коммутант $K_i$) обрывается на единичной подгруппе.

ПРИМЕР I. Всякая абелева группа $G$ разрешима. В самом деле, по свойству коммутанта, у абелевой группы $K = e$ и имеем:
$G = K_0 \supset K = e$, что и означает разрешимость группы $G$.

ПРИМЕР 2. Всякая циклическая группа разрешима. Действительно, циклическая группа является абелевой (это очевидно), а всякая абелева группа разрешима (пример I).

ТЕОРЕМА. Следующие 3 условия равносильны:

I. $G$ – разрешимая группа.

2. $G$ обладает конечной последовательностью подгрупп

$G = G_0 \supset G_1 \supset \ldots \supset G_n = e$, где $G_{i+1}$ – нормальный де-

Следствие 2. Если $G$ – разрешимая группа, $N$ – ее нормальный делитель, то $G/N$ – разрешимая группа. Это становится очевидным, если в качестве гомоморфизма рассмотреть гомоморфизм $\varphi: G \to G/N$ по правилу $(\forall a \in G)\ \varphi(a) = \bar{a}$ (проверьте, что заданное отображение является гомоморфизмом).

ТЕОРЕМА 3. Пусть даны группа $G$ и ее нормальный делитель $N$. Известно, что $N$ разрешим и $G/N$ разрешима. Тогда $G$ – разрешимая группа.

Доказательство: Зададим гомоморфизм $\varphi: G \to G/N$ по правилу: $(\forall a \in G)\quad \varphi(a) = \bar{a}$ (естественный гомоморфизм). Так как $G/N$ разрешима, то по теореме из §3 ( 2 ) существует конечная последовательность подгрупп $G/N = \bar{G}_0 \supset \bar{G}_1 \supset \bar{G}_2 \supset \ldots \supset \bar{G}_n = \bar{e}$, где $\bar{G}_{i+1}$ – нормальный делитель $\bar{G}_i$ и $K_{\bar{x},\bar{y}} \in \bar{G}_{i+1}$ $(\forall \bar{x}, \bar{y} \in \bar{G}_i)$ $i \in \{0, \ldots, n-1\}$.

Пусть $G_1 = \varphi^{-1}(\bar{G}_1)$

$G_2 = \varphi^{-1}(\bar{G}_2)$

$\ldots\ldots$

$G_n = \varphi^{-1}(\bar{G}_n) = \varphi^{-1}(\bar{e}) = N$

По условию имеем ряд, показывающий разрешимость $N$:

$N = H_0 \supset H_1 \supset \ldots \supset H_m = e$ ( $H_{i+1}$ – нормальный делитель $H_i$ ), $K_{x,y} \in H_{i+1}$ $(\forall x, y \in H_i)$.

Тогда уже для группы $G$ получится ряд

$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = N = H_0 \supset H_1 \supset H_1 \supset \ldots \supset H_m = e, \quad G_i = \varphi^{-1}(\bar{G}_i),\ i \in \{1, \ldots, n\}$.

Остается показать, что:

I) $G_{i+1}$ – нормальный делитель $G_i$,

2) $K_{x,y} \in G_{i+1}$ $(\forall x, y \in G_i)$

I) $(\forall x \in G_{i+1})\ x \in \varphi^{-1}(\bar{G}_{i+1}) \Rightarrow \varphi(x) \in \bar{G}_{i+1} \subset \bar{G}_i \Rightarrow$
$\Rightarrow x \in \varphi^{-1}(\bar{G}_i) = G_i$, так что действительно $G_{i+1} \subset G_i$.

Теперь покажем, что $G_{i+1}$ – подгруппа $G_i$.

$(\forall x, y \in G_{i+1})\ \varphi(x), \varphi(y) \in \bar{G}_{i+1} \Rightarrow \varphi(x) \cdot \varphi(y)^{-1} \in \bar{G}_{i+1}$

(так как $\bar{G}_{i+1}$ – подгруппа), а тогда $\varphi(xy^{-1}) \in \bar{G}_{i+1} \Rightarrow$



$\Rightarrow xy^{-1} \in \varphi^{-1}(\bar{G}_{i+1}) = G_{i+1}$.

Осталось установить, что $(\forall x \in G_{i+1})(\forall a \in G_i)\ a^{-1}xa \in G_{i+1}$,

$\underbrace{\varphi(a)^{-1}}_{\in \bar{G}_i} \underbrace{\varphi(x)}_{\in \bar{G}_{i+1}} \underbrace{\varphi(a)}_{\in \bar{G}_i} = \varphi(a^{-1}xa) \in \bar{G}_{i+1}$, так как $\bar{G}_{i+1}$ – нормальный делитель $\bar{G}_i$ (смотри теорему 2 в I ), а тогда $a^{-1}xa \in G_{i+1}$.

Доказано, что $G_{i+1}$ – нормальный делитель $G_i$.

2) $K_{\varphi(x),\varphi(y)} = \varphi(x)^{-1}\varphi(y)^{-1}\varphi(x)\varphi(y) \in \bar{G}_{i+1}$; тогда $\varphi(x^{-1}y^{-1}xy) \in \bar{G}_{i+1}$, следовательно, $x^{-1}y^{-1}xy \in G_{i+1}$ т.е. $K_{x,y} \in G_{i+1}$ $(\forall x, y \in G_i)$.

Применяя теорему из 3 получаем, что $G$ – разрешимая группа. Теорема доказана.

## 5. Группы подстановок и их разрешимость

Определение I. Пусть $M = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ – конечное множество, состоящее из $n$ элементов. Подстановкой множества $M$ называется биективное отображение множества $M$ на себя (или геометрическое преобразование $M$ ). Будем рассматривать $M = \{1, 2, 3, \ldots, n\}$. Тогда обозначение подстановки: $f = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$. Группу всех подстановок множества $M$ обозначают $S_n$.

ПРИМЕР I. Если $M = \{1, 2\}$, то $S_2 = \left\{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right\}$

Определение 2. Подстановка называется циклом, если $(\exists \alpha, \beta, \ldots, \delta \in M)$ $\alpha \to \beta \to \ldots \to \delta \to \alpha$, а остальные элементы множества $M$ переходят в себя. Обозначение цкла: $(\alpha, \beta \ldots \delta)$.

ПРИМЕР 2. Пусть $M = \{1, 2, 3, 4, 5\}$

$(2\,3\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}$. Умножение циклов производится так: $(2\,3\,4) \cdot (1\,3) = (1\,4\,2\,3)$.

Лемма. Если $G$ – группа, $N$ – ее нормальный делитель, то $|G| = |G/N| \cdot |N|$, где $|M|$ – количество элементов в множестве $M$.

Доказательство непосредственно следует из теоремы Лагранжа (I), если учесть, что все классы в фактор-группе $G/N$ содержат одинаковое число элементов – столько же, сколько их содержит $N$.

ТЕОРЕМА. $S_1, S_2, S_3, S_4$ – разрешимые группы, а $S_n$ $(n \geq 5)$ неразрешимы.

Доказательство:

I. Покажем разрешимость $S_n$ $(1 \leq n \leq 4,\ n \in \mathbb{Z})$.

а) $S_1$ абелева, а потому разрешима (пример I в 3),

б) $S_2 = \left[\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\right]$ – циклическая, а потому тоже разрешима (пример 2 в 3),

в) $S_3 = \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$.

Рассмотрим $H = \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$.

Легко проверить, что $H$ – нормальный делитель $S_3$ (проделать самостоятельно). Следовательно, можно говорить о фактор-группе $S_3/H$, которая по лемме состоит из двух элементов. Так как 2 – простое число, то по следствию из теоремы Лагранжа (I) $S_3/H$ – циклическая, а значит, разрешима. По той же причине $H$ – разрешимая группа (состоит из трех (простое число!) элементов). Применяя теорему 3 (4), получаем, что $S_3$ разрешима.

г) в $S_4$ всего 24 подстановки (мы их все выписывать не будем). Рассмотрим $H = \left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\right\}$.

Можно проверить (например, используя предложение 2 в I), что $H$ – нормальный делитель $S_4$ (проделать самостоятельно). Поэтому можно говорить о фактор-группе $S_4/H$, которая по лемме состоит из шести элементов, а именно: $S_4 = H \cup a_1 H \cup a_2 H \cup a_3 H \cup a_4 H \cup a_5 H$, где $a_1 = (12)$, $a_2 = (132)$, $a_3 = (13)$, $a_4 = (23)$, $a_5 = (123)$, $a_i \in S_4$.



Здесь $a_i \in S_4$.

Установим соответствие $\varphi: S_4/H \to S_3$ по правилу $\varphi(a_i H) = \underset{\in S_3}{a_i}$; $\varphi(H) = e_3 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$.

$\varphi$ взаимно однозначно (и в $S_4/H$ и в $S_3$ по шесть элементов, причем все они различны), значит, $\varphi$ – биекция. Докажем, что $\varphi$ – гомоморфизм:

$\varphi(a_2 H a_4 H) = \varphi(a_2 a_4 H) = \varphi(a_3 H) = a_3$

$\varphi(a_2 H)\varphi(a_4 H) = a_2 \cdot a_4 = a_3$, т.е. $\varphi(\bar{a}_2 \cdot \bar{a}_4) = \varphi(\bar{a}_2)\varphi(\bar{a}_4)$.

Получим, что $\varphi$ – изоморфизм $S_4/H$ на $S_3$, а значит, по следствию I из теоремы 2 (4) $S_4/H$ разрешима.

Теперь осталось доказать, что $H$ разрешима, ибо тогда, пользуясь теоремой 3 из 4, получим, что $S_4$ разрешима.

Пусть $A = \left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\right\}$.

$A$ – нормальный делитель $H$ (почему?); $|A| = 2$ и $|H/A| = 2 \Rightarrow A$, $H/A$ циклические, а значит, разрешимы (смотри доказательство разрешимости $S_3$), следовательно, по теореме 3 из 4 $H$ разрешима, что нам и требовалось показать.

II. Докажем, что $S_n$ $(n \geq 5)$ неразрешимы. Для этого нам понадобится доказать, что любой коммутант в ряду $S_n = K_0 \supset K_1 \supset K_2 \supset \ldots$ содержит все тройные циклы (количество элементов $\alpha, \beta, \ldots, \delta$ в определении цикла задает его кратность). Рассмотрим цикл $(\alpha\beta\gamma) \in S_n$, $(\alpha, \beta, \gamma \in M)$. Пусть $\mu, \nu \in M$ и отличны от $\alpha, \beta, \gamma$ $(\mu, \nu$ существуют, так как $|M| = n \geq 5)$.

Теперь рассмотрим циклы $x = (\mu\gamma\beta) \in S_n$ и $y = (\alpha\beta\nu) \in S_n$, $K_{x,y} = (\alpha\beta\gamma)$ (проверьте!), (умножение циклов производим справа налево), а тогда $K_{x,y}$ принадлежит коммутанту $S_n$. И т. д. Таким образом, в "ряду" $S_n = K_0 \supset K_1 \supset K_2 \supset \ldots \supset K_i \supset \ldots$ каждый коммутант $K_i$ содержит тройные циклы, т.е. "ряд" коммутантов никогда не оборвется на $e$ (единичная группа тройные циклы не содержит). Следовательно, $S_n, (n \geqslant 5)$ неразрешимы. Теорема доказана.

## 6. Транзитивные группы преобразований

Определение. Группа преобразований $S(\Omega)$ конечного множества $\Omega$ называются транзитивной, если

$$(\forall \alpha, \beta \in \Omega)(\exists f \in S(\Omega)) \quad f(\alpha) = \beta.$$

ПРИМЕР I. Группа всех подстановок $S_n$ множества $\Omega$ $(|\Omega| = n)$ транзитивна. В самом деле, $(\forall \alpha, \beta \in \Omega)(\exists f = (\alpha\beta) \in S_n)$, переводящее $\alpha$ в $\beta$ (по определению цикла).

ПРИМЕР 2. Пусть дана группа, порожденная двумя подстановками:

$$\left[(1234)(56);\ (123)\right], \quad \Omega = \{1,2,3,4,5,6\}.$$

Эта группа не является транзитивной, так как, например, для элементов I и 6 не существует преобразования этой группы, переводящего I в 6.

Предложение. Пусть $S(\Omega)$ – транзитивная группа преобразований (здесь это несущественно!).

$$G_\alpha = \{f \in S(\Omega) \mid f(\alpha) = \alpha, \alpha \in \Omega\}.$$

Тогда $G_\alpha$ – подгруппа $S(\Omega)$, т.е. $(\forall a, b \in G_\alpha)\ ab^{-1} \in G_\alpha$.

Доказательство: Возьмем произвольные $a, b \in G_\alpha$. Так как $a, b \in G_\alpha$, то по определению $G_\alpha$ $a(\alpha) = \alpha; b(\alpha) = \alpha$. $\alpha = b^{-1}(b(\alpha)) = b^{-1}(\alpha)$, т.е. $b^{-1}(\alpha) = \alpha$.

А тогда $ab^{-1}(\alpha) = a(b^{-1}(\alpha)) = a(\alpha) = \alpha$, что означает, что $ab^{-1} \in G_\alpha$.

## 7. Понятие об импримитивных группах преобразований. Свойства ряда импримитивности

Определение I. Пусть $\Omega$ – конечное множество, $G$ – транзитивная группа преобразований этого множества. $G$ импримитивна, если существует разбиение множества $\Omega$ (ряд импримитивности) на классы $M_i$ $(i \in \mathcal{J})$:

1) $|\mathcal{J}| \neq 1$,
2) $(\exists j \in \mathcal{J})\ |M_j| \neq 1$,
3) $(\forall u \in G)(\forall M_i)(\exists M_j)\ u(M_i) = M_j \quad (i, j \in \mathcal{J})$.

Определение 2. Если $G$ – транзитивная группа и указанного разбиения не существует, то $G$ называют примитивной группой.

ПРИМЕР I. Группа $[(\alpha,\beta,\gamma,\delta);\ (\alpha\gamma)]$ импримитивна. Действительно, данная группа транзитивна (по определению). Искомое разбиение множества $\Omega = \{\alpha, \beta, \gamma, \delta\}$ выглядит так:

$$M_1 = \{\alpha, \gamma\}, \quad M_2 = \{\beta, \delta\}.$$



Очевидно, что первые 2 условия из определения I выполняются. Третье условие проверим на примерах:

для $u = (\alpha\gamma)$ и $M_2 = \{\beta, \delta\}$; $(\exists M_2)$ $u(M_2) = M_2$

для $u = (\alpha\beta\gamma\delta)$ и $M_1 = \{\alpha, \gamma\}$; $(\exists M_1)$ $u(M_1) = M_2$.

и так далее.

ПРИМЕР 2. Группа всех подстановок $S_n$ множества $\Omega$ $|\Omega| = n > 2, n \in N$ примитивна. Докажем это. $S_n$ транзитивна (пример I в 6). Допустим, что $S_n$ импримитивна. По условию $(\exists \alpha, \beta, \gamma \in \Omega)$ $\alpha \neq \beta \neq \gamma$. По нашему предположению $(\exists M_1): \delta, \varepsilon \in M_1$ (по 2) условию из определения I) и $(\exists M_2) \neq M_1 : \mu \in M_2$ (по I) условию из определения I). По третьему условию из определения I для $u = (\delta\varepsilon\mu) \in S_n$ и для класса $M_1$ должен найтись класс $M_j$ : $u(M_1) = M_j$. Попытаемся найти $M_j$. $j = 1$ не годится (ибо $u(\varepsilon) = \mu, \varepsilon \in M_1, \mu \in M_2$, а должно быть $u(M_1) = M_1$);

$j \neq 1$ тоже не годится (в этом случае $u(\delta) = \varepsilon, \delta \in M_1, \varepsilon \in M_1$, а должно быть $u(M_1) = M_j$, где $j \neq 1$). Так что 3) условие из определения I не выполняется, а значит, $S_n$ примитивна (по определению 2).

Свойства ряда импримитивности. Пусть $G$ – импримитивная группа преобразований (в смысле определения I).

I. если $\alpha \in M_i$ $(i \in \mathcal{J})$, $u \in G$, $u(\alpha) \in M_j$ $(j \in \mathcal{J})$, то $u(M_i) = M_j$.

Доказательство: По 3) условию определения I для $u \in G$, $M_i (i \in \mathcal{J}) (\exists M_k)$ $u(M_i) = M_k$, но $u(\alpha) \in M_j \Rightarrow M_k = M_j$ $(\alpha \in M_i)$ ($M_i$ образуют разбиение множества $\Omega$, следовательно, классы разбиения не пересекаются!).

2. $(\forall u \in G)(\forall M_j)(j \in \mathcal{J})(\exists M_i)(i \in \mathcal{J})$ $u(M_i) = M_j$.

Доказательство: Так как $G$ – группа, то $(\exists u^{-1} \in G)$. По 3) условию определения I для $u^{-1} \in G$, $M_j (j \in \mathcal{J}) (\exists M_k)(k \in \mathcal{J})$: $u^{-1}(M_j) = M_k \Rightarrow uu^{-1}(M_j) = u(M_k) \Rightarrow M_j = u(M_k)$, полагая $k = i$, получаем требуемое. Таким образом, каждое преобразование на классах $M_i$ $(i \in \mathcal{J})$ является сюръекцией.

3. Если $M_i \neq M_j$, то $(\forall u \in G)\ u(M_i) \neq u(M_j)\ (i,j \in J)$

В самом деле, допустим, что $u(M_i) = u(M_j)$. Тогда $u^{-1}u(M_i) = u^{-1}u(M_j) \Rightarrow M_i = M_j$, что противоречит условию. Таким образом, каждое преобразование на классах $M_i\ (i \in J)$ является инъекцией.

4. $(\forall M_i, M_j)\ |M_i| = |M_j|,\ (i,j \in J)$.

Доказательство: Возьмем произвольные $\alpha \in M_i,\ \beta \in M_j$. Тогда по транзитивности $G\ (\exists u \in G)\ u(\alpha) = \beta$, по I свойству это означает, что $u(M_i) = M_j$. По 2 и 3 свойству $u$ – биекция на классах $M_i\ (i \in J)$, а значит, $|M_i| = |M_j|$.

<u>Следствие</u>. Если $G$ – транзитивная группа преобразований $\Omega$ и $|\Omega| = p$, где $p$ – простое число, то $G$ примитивна. В самом деле, если бы $G$ была импримитивной, то все классы в ряду импримтивности были бы равномощны, причем по 2) условию определения I количество элементов в каждом из них было бы не равно единице, а тогда $|\Omega|$ не могла бы быть простым числом.

## 8. <u>Важнейшие теоремы об импримитивных группах преобразований</u>

ТЕОРЕМА I. (критерий импримитивности).

Пусть $G$ – транзитивная группа преобразований $\Omega$.

$G$ импримитивна $\Leftrightarrow (\exists \alpha \in \Omega)\ (\exists H$ - подгруппа $G)$:

$$G_\alpha \subsetneqq H \subsetneqq G;\ \text{где } G_\alpha = \{f \in G \mid f(\alpha) = \alpha,\ \alpha \in \Omega\}$$

Доказательство:

I. <u>Необходимость</u>. Пусть $G$ импримитивна. Возьмем $\alpha \in \Omega : \alpha \in M_1$.

Пусть $H = \{g \in G \mid g(M_1) = M_1\}$,

$H \neq G$. В самом деле, по определению I из 7 существует класс $M_2 \neq M_1$, а значит, $(\exists \beta \in M_2)$. По транзитивности $G\ (\exists u \in G)$, $u(\alpha) = \beta$, что по I свойству ряда импримитивности означает, что $u(M_1) = M_2$, т.е. $u \notin H$.

$H$ – подгруппа $G$:

$(\forall g_1, g_2 \in H)\ \ g_1 \circ g_2(M_1) = g_1(g_2(M_1)) = g_1(M_1) = M_1$, т.е. $g_1 \circ g_2 \in H$.

$(\forall g \in H)\ \ g(M_1) = M_1 \Rightarrow g^{-1} \circ g(M_1) = g^{-1}(M_1) \Rightarrow M_1 = g^{-1}(M_1)$, т.е. $g^{-1} \in H$.

Далее, пусть $f \in G_\alpha$. Следовательно, $f(\alpha) = \alpha$. По I свойству ряда импримитивности это означает, что $f(M_1) = M_1$, т.е. $f \in H$, а тогда $G_\alpha \subset H$.

Осталось показать, что $H \neq G_\alpha$.

$|M_1| \geq 2$ (из определения I из 7 и 4 свойства ряда импримитивности), вытекает, что $(\exists \beta \in M_1)\ \beta \neq \alpha$, тогда по транзитивности $G\ (\exists u \in G)\ u(\alpha) = \beta$ и опять же по I свойству ряда импримитивности $u(M_1) = M_1$, т.е. $u \in H$, но $u \notin G_\alpha$ (ибо $u(\alpha) = \beta,\ \alpha \neq \beta$), что и означает, что $H \neq G_\alpha$.



II. <u>Достаточность</u>. Пусть теперь $(\exists \alpha \in \Omega)$ и $(\exists H$ – полугруппа $G)$: $G_\alpha \subsetneqq H \subsetneqq G$. Докажем, что $G$ импримитивна. Рассмотрим множество классов группы $G$ по эквивалентности $\sigma_H^{(\lambda)}$. Обозначим его $G/H$.

Пусть $H = \{u_1, \ldots, u_k\}$, $|G/H| = m$ $(m \neq 1$, иначе $G = H$, что противоречит условию).

$G/H = \{v_1 H, v_2 H, \ldots, v_m H\}$, где $v_1, v_2, \ldots, v_m \in G$. (по предложению I из I).

Пусть $M_i = \{v_i u_1(\alpha), v_i u_2(\alpha), \ldots, v_i u_k(\alpha)\}$
$u_1, \ldots, u_k \in H,\ v_i \in G,\ i \in J = \{1, \ldots, m\}$

Докажем, что множества $M_i$ образуют разбиение $\Omega$.

а) $(\forall \beta \in \Omega)(\exists t \in G)\ \ t(\alpha) = \beta$ (по транзитивности $G$), но $\bigcup\limits_i v_i H = G$, поэтому $t \in v_j H$, т.е. $t = v_j u_e$.

Итак, $\beta = t(\alpha) = (v_j u_e)(\alpha) \in M_j$ по построению $M_i$ (см. выше). Значит, $\Omega \subset \bigcup\limits_i M_i$. Обратное включение очевидно (проверьте!). Таким образом, $\bigcup\limits_i M_i = \Omega$.

б) Допустим, что $M_i \bigcap\limits_{i \neq j} M_j \neq \emptyset \Rightarrow (\exists \delta)\ \delta \in M_i, \delta \in M_j \Rightarrow$
$\Rightarrow \delta = v_i u_e(\alpha)$ и $\delta = v_j u_h(\alpha) \Rightarrow v_i u_e(\alpha) =$
$= v_j u_h(\alpha)$

Значит, $\alpha = u_e^{-1} v_i^{-1} v_j u_h(\alpha)$, тогда $u_e^{-1} v_i^{-1} v_j u_h \in G_\alpha$, причём, $G_\alpha \subset H$, т.е. $\alpha = u_p(\alpha)$, где $u_p \in H$. Получаем, что $v_i^{-1} v_j \in H$ (так как $v_i^{-1} v_j = u_e u_p u_h^{-1}) \Rightarrow v_j \in v_i H$, а это означает, что $v_j H = v_i H$ (по свойствам эквивалентности), т.е. $i = j$ (так как в $G/H$ нет одинаковых классов). Однако $i \neq j$, а значит, $M_i \cap M_j = \emptyset$.

Таким образом, доказано, что множества $M_i$ образуют разбиение $\Omega$. Покажем теперь, что это разбиение обладает тремя свойствами, присущими ряду импримитивности (см. определение I из 7).

1) $\|\mathcal{J}\| \neq 1$, так как $|G/H| \neq 1$

2) $|H| \neq 1$, так как $G_\alpha \subsetneq H$ (если бы $|H| = 1$, то и $|G_\alpha| = 1$, что означало бы, что $G_\alpha = H$). Значит,

$(\exists u_1, u_2 \in H)$ $u_1 \neq u_2$. Возьмем $u_1 \in H, u_1 \notin G_\alpha$, $u_2 = e$.

$u_1(\alpha) \neq u_2(\alpha) \Rightarrow \underset{(v_1 \in G)}{v_1(u_1(\alpha)) \neq v_1(u_2(\alpha))}$ так как $v_1$ – инъекция,

$v_1(u_1(\alpha))$ и $v_1(u_2(\alpha))$ принадлежат $M_1$ по построению $M_i$, следовательно, $(\exists i \in J)$ $|M_i| \neq 1$ (здесь $i = 1$), т.е. выполнено 2) условие определения I из 7.

3) Пусть $\omega \in G$. Для произвольного класса $M_i$ найдем класс $M_j$: $\omega(M_i) = M_j$. Возьмем $\delta \in M_i$; $\omega(\delta) \in M_j$, где $M_j$ – некоторый класс. Докажем, что он искомый.

а) Пусть $\varepsilon \in M_i \Rightarrow \varepsilon = v_i u_e(\alpha)$, $\delta = v_i u_s(\alpha)$, $\omega(\delta) = \omega(v_i u_s(\alpha))$, но $\omega(\delta) \in M_j$, следовательно, $\omega(\delta) = v_j u_t(\alpha)$, и тогда $\omega v_i = v_j u_r$ $(*)$. Получаем, что $\omega(\varepsilon) = \omega v_i u_e(\alpha) = v_j u_r u_e(\alpha) = v_j u_n(\alpha) \in M_j$.

б) Обратно: берем $\mu \in M_j$ и ищем $\nu \in M_i$: $\omega(\nu) = \mu$, $\mu = v_j u_k(\alpha)$. Положим $\nu = \omega^{-1}(\mu)$. Тогда $\nu = \omega^{-1} v_j u_k(\alpha) \overset{(*)}{=} v_i u_r^{-1} u_k(\alpha) = v_i u_m(\alpha) \in M_i$, т.е. найдено $\nu \in M_i$.

Группа $G$ удовлетворяет определению I из 7, т.е. является импримитивной.

Теорема доказана.

Лемма. Пусть $G$ – группа преобразований множества $\Omega$. Известно, что $(i1); (i2); \ldots (in) \in G$, $i \in \Omega \setminus \{1, 2, \ldots, n\}$. Тогда $G = S_n$.

а) $G \subset S_n$, так как $S_n$ – группа всех преобразований $\Omega$.

б) $S_n \subset G$. Докажем это.

Во-первых, всякий двойной цикл раскладывается в произведение двойных циклов нужного нам вида. В самом деле,

$$(ts) = (it)(is)(it) \in G.$$

Теперь рассмотрим любую подстановку из $S_n$: $\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$. Покажем, что она представляется в виде произведения двойных



циклов, а тогда по сказанному выше это будет означать требуемое.

Заметим, что любая подстановка может быть единственным образом разложена в произведение попарно независимых циклов (т.е. циклов без общих действительно перемещаемых символов). Разложение осуществляется следующим образом: начинаем с любого из действительно перемещаемых символов и выписываем за ним те символы, в которые он входит при повторении подстановки, пока не вернемся к исходному символу. После этого "закрытия" цикла начинаем с одного из оставшихся действительно перемещаемых символов, получаем второй цикл и т.д.

Итак, $\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix} = (i_1 i_2 \ldots i_k)(j_1 j_2 \ldots j_e) \ldots (s_1 s_2 \ldots s_t)$.

Далее – любой цикл длины $m$ можно представить в виде произведения $m-1$ двойного цикла (двойной цикл еще называют транспозицией):

$$(t_1 t_2 \ldots t_m) = (t_1 t_m)(t_1 t_{m-1}) \ldots (t_1 t_2),$$

что и требовалось доказать. Таким образом, $G = S_n$.

ТЕОРЕМА II. Пусть $G$ – транзитивная группа преобразований $\Omega$ ($|\Omega| = n$), $G \neq S_n$, существует транспозиция $(\alpha\, \beta) \in G$. Тогда $G$ импримитивна.

Доказательство (по критерию импримитивности): Рассмотрим $\alpha$ из транспозиции.

$H = [G_\alpha, (\alpha\beta), (\alpha\gamma_1), \ldots, (\alpha\gamma_k)]$, $\gamma_1, \ldots, \gamma_k \in \Omega$, $(\alpha\gamma_i) \in G$, $G_\alpha \subset H$, $G_\alpha \neq H$, $H \subset G$ по построению $H$. Остается доказать, что $H \neq G$.

Пусть $T = \{\alpha, \beta, \gamma_1, \ldots, \gamma_k\}$ $T \neq \Omega$ так как иначе по лемме $H = S_n \Rightarrow G = S_n$, но $G \neq S_n$ по условию, следовательно, $(\exists \delta \in \Omega)$ $\delta \notin T$.

Проверим, что $(\forall u \in G_\alpha)(\forall \xi \in T)$ $u(\xi) \neq \delta$ $(*)$.

Предположим, что $(\exists \xi_0 \in T)(\exists u_0 \in G_\alpha)$ $u_0(\xi_0) = \delta$. Тогда $u_0^{-1}(\delta) = \xi_0$, $\omega = u_0(\alpha\, \xi_0) u_0^{-1} \in H$ (так как $u_0 \in G_\alpha \subset H$, $(\alpha\, \xi_0) \in H$, т.к. $\xi_0 \in T$, $u_0^{-1} \in G_\alpha \subset H$); $\omega(\delta) = \alpha$, $\omega(\alpha) = \delta$ (проверьте!), следует что $\omega = (\alpha\delta)$ (других циклов в $H$ нет). $\delta \notin T$, что противоречит тому, что $H$ содержит только циклы вида $(\alpha\mu)$, где $\mu \in T$. Значит, наше предположение было неверным, и можно сказать, что $(\forall u' \in G_\alpha)(\forall \varepsilon \in T)$ $u'(\delta) \neq \varepsilon$ $(**)$ – получается из $(*)$ действием $u' = u^{-1} \in G_\alpha$ ($u'$ – инъекция).

Возьмем теперь $\omega \in H \Rightarrow \omega = \upsilon_1 \circ \upsilon_2 \circ \ldots \circ \upsilon_s$; $\omega(\delta) = \upsilon_1 \circ \upsilon_2 \circ \ldots \circ \upsilon_i(\delta)$.

Если $\upsilon_i$ – двойной цикл, то $\upsilon_i(\delta) = \delta \notin T$, так как $\delta$ в цикл не входит, если $\upsilon_i \in G_2$, то по доказанному выше $\upsilon_i(\delta) \neq \varepsilon \in T$, т.е. $\omega(\delta) \notin T$. $G$ – транзитивна, значит, $(\exists\, \upsilon \in G)$ $\upsilon(\delta) = \alpha$ $(\alpha, \delta \in \Omega)$, $\upsilon \notin H$ (так как иначе $\upsilon(\delta) \notin T$, а $\alpha \in T$). Отсюда следует, что $H \neq G$, а тогда $G$ импримитивна по теореме I. Теорема доказана.

## II. РАСШИРЕНИЯ ПОЛЕЙ. ГРУППЫ АВТОМОРФИЗМОВ

### 9. Различные типы расширения полей и связь между ними

Напомним, что числовым полем называется множество, содержащее не менее двух элементов, замкнутое относительно действий +, –, , : (деление должно производиться на ненулевой элемент).

Будем предполагать, что все рассматриваемые поля содержатся в множестве комплексных чисел .

Определение I. Пусть $P$ – числовое поле, $\alpha \in \mathbb{C}$. Множество $P[\alpha] = \left\{ \frac{f(\alpha)}{g(\alpha)} \right\}$, где $f(x), g(x)$ – полиномы над $P$ и $g(\alpha) \neq 0$, называется простым расширением поля $P$ с помощью примитивного элемента $\alpha$.

Предложение I. I) $P[\alpha]$ – поле; $\alpha \in P[\alpha]$, $P \subset P[\alpha]$

2) если некоторое поле $\bar{P} \supset P, \alpha \in \bar{P}$, то $\bar{P} \supset P[\alpha]$ (т.е. $P[\alpha]$ – наименьшее из всех полей, содержащих $P$ и $\alpha$).

Докажите самостоятельно.

Замечание I. Если $\alpha \in P$, то $P[\alpha] = P$.

Определение 2. Число $\alpha \in \mathbb{C}$ называется алгебраическим относительно поля $P$, если существует полином $f(x) \neq 0$ над этим полем, имеющий $\alpha$ своим корнем.

Определение 3. Расширение $P[\alpha]$ называется простым алгебраическим расширением поля $P$, если $\alpha$ алгебраично относительно поля $P$.

Предложение 2. Множество алгебраических относительно $P$ чисел образует поле. Доказательство этого предложения будет дано ниже.

ТЕОРЕМА I. Пусть $\alpha$ алгебраично относительно поля $P$. Тогда существует полином $p(x)$ над $P$, обладающий двумя свойствами:

I) $\alpha$ – корень $p(x)$,

2) $p(x)$ неприводим над $P$.



При этом если полином $f(x)$ над полем $P$ имеет $\alpha$ своим корнем, то $f(x) \,\vdots\, p(x)$.

Примечание. Этот полином $p(x)$ называется минимальным полиномом для $\alpha$ относительно поля $P$.

Доказательство: Так как $\alpha$ алгебраично, то существует некоторый полином $\tilde{f}(x)$, имеющий $\alpha$ своим корнем. Разложим $\tilde{f}(x)$ на неприводимые полиномы над полем $P$:

$\tilde{f}(x) = p_1(x) \ldots p_i(x) \ldots p_m(x)$ при $x = \alpha$ $0 = p_1(\alpha) \ldots p_i(\alpha) \ldots p_m(\alpha)$.

Пусть $p_i(\alpha) = 0$. Рассмотрим полином $p_i(x)$. Он удовлетворяет условиям теоремы, т.е. $p(x)$ найден. Покажем теперь, что любой полином $f(x)$, имеющий $\alpha$ своим корнем, делится на $p(x)$. Пусть $f(x)$ – полином над $P$ и $f(\alpha) = 0$. $f(x) = q_1(x) \ldots q_j(x) \ldots q_e(x)$, где $q_1(x), \ldots, q_e(x)$ – неприводимые полиномы над $P$. При $x = \alpha$ $0 = q_1(\alpha) \ldots q_j(\alpha) \ldots q_e(\alpha)$. Пусть $q_j(\alpha) = 0$. Рассмотрим полином $q_j(x)$. По свойству неприводимых полиномов $p(x)$ и $q_j(x)$ либо взаимно просты, либо отличаются постоянным множителем. Допустим, что они взаимно просты. Тогда $1 = F_1(x)p(x) + F_2(x)q_j(x)$. При $x = \alpha$ получим $1 = 0$, что невозможно.

Итак, $q_j(x)$ с точностью до постоянной равняется $p(x)$. Этого достаточно для доказательства теоремы, так как $f(x) \,\vdots\, q_j(x)$. Теорема доказана.

ТЕОРЕМА 2. (об освобождении от иррациональности в знаменателе). Пусть $\alpha$ алгебраично относительно поля $P$, $p(x)$ – минимальный полином для $\alpha$ относительно $P$. Пусть степень $p(x)$ равна $n$. Тогда любое $\gamma \in P[\alpha]$ представимо и, притом, единственным образом, в виде

$$\gamma = a_0 \alpha^{n-1} + \ldots + a_{n-1}, \quad a_i \in P$$

(т.е. $P[\alpha]$ состоит из значений полиномов от $\alpha$ над полем $P$ степени, меньшей $n$).

Доказательство:

I. Возможность

Пусть $\gamma \in P[\alpha] \Rightarrow \gamma = \dfrac{f(\alpha)}{g(\alpha)}$, где $g(\alpha) \neq 0$, а $f(x), g(x)$ – полиномы над $P$. Рассмотрим полиномы $g(x)$ и $p(x)$. По свойствам неприводимых полиномов ($p(x)$ – неприводим!) $g(x) \,\vdots\, p(x)$ или $g(x)$ и $p(x)$ взаимно просты. Первый вариант невозможен, так как иначе было бы $g(\alpha) = 0$. Значит, $g(x)$ и $p(x)$ взаимно просты, а тогда

$1 = F_1(x)g(x) + F_2(x)p(x)$. При $x=\alpha$
$1 = F_1(\alpha)g(\alpha)$ (так как $p(\alpha)=0$).

$$\gamma = \frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha)\cdot 1}{g(\alpha)} = \frac{f(\alpha)\cdot F_1(\alpha)\, g(\alpha)}{g(\alpha)} = f(\alpha)\cdot F_1(\alpha).$$

Поделим $f(x)\cdot F_1(x)$ на $p(x)$ с остатком:
$f(x)\cdot F_1(x) = p(x)S(x) + \tau(x)$, степень $\tau(x)$ > степени $p(x) \Rightarrow$
$\tau(x) = a_0x^{n-1} + \ldots + a_{n-1}$. При $x=\alpha$ $\gamma = f(\alpha)\cdot F_1(\alpha) = a_0\alpha^{n-1} + \ldots + a_{n-1}$

II. Единственность.

Пусть $\gamma = a_0\alpha^{n-1} + \ldots + a_{n-1}$ $(a_i \in P)$ и $\gamma = b_0\alpha^{n-1} + \ldots + b_{n-1}$ $(b_j \in P)$

Тогда $a_0\alpha^{n-1} + \ldots + a_{n-1} = b_0\alpha^{n-1} + \ldots + b_{n-1}$ или $(a_0 - b_0)\alpha^{n-1} + \ldots + a_{n-1} - b_{n-1} = 0$. Обозначим $a_0 - b_0 = d_0, \ldots, a_{n-1} - b_{n-1} = d_{n-1}$. Получим: $d_0\alpha^{n-1} + \ldots + d_{n-1} = 0$. Тогда $\alpha$ – корень полинома над $P$, имеющего степень, меньшую $n$. Это значит, что $d_0 = \ldots = d_{n-1} = 0$, т.е. $a_0 = b_0, \ldots, a_{n-1} = b_{n-1}$, что и означает единственность представления числа $\gamma$. Теорема доказана.

Замечание 2. Простое алгебраическое расширение можно теперь рассмаривать как конечномерное линейное пространство над полем $P$ с базисом $1, \alpha, \ldots, \alpha^{n-1}$. Такие расширения принято называть конечными. Из теоремы 2 следует, что размерность простого алгебраического расширения $P[\alpha]$ совпадает со степенью минимального полинома $p(x)$ над полем $P$ для числа $\alpha$.

Определение 4. Число $\alpha$ называется трансцендентным относительно поля $P$, если оно не является алгебраическим.

Предложение 3. Пусть $P$ – поле, $\alpha$ – трансцендентно относительно $P$ и $\gamma \in P[\alpha]$. Тогда $\gamma$ представимо и, притом единственным образом в виде $\gamma = \frac{f(\alpha)}{g(\alpha)}$, где $f(x)$, $g(x)$ – полиномы над полем $P$, $g(x)$ имеет старший коэффициент, равный единице и $f(x)$, $g(x)$ взаимно просты.

Доказательство:

I. Возможность. $\gamma \in P[\alpha] \Rightarrow \gamma = \frac{\bar{f}(\alpha)}{\bar{g}(\alpha)}$, где $\bar{f}(\alpha), \bar{g}(\alpha)$ – полиномы над $P$ и $\bar{g}(\alpha) \neq 0$. Рассмотрим $d(x) = НОД(\bar{f}(x), \bar{g}(x))$. Тогда $\bar{f}(x) = d(x)\bar{\bar{f}}(x)$, $\bar{g}(x) = d(x)\bar{\bar{g}}(x)$, причем $\bar{\bar{g}}(x)$ и $\bar{\bar{f}}(x)$ взаимно просты. Вытекает что

$$\gamma = \frac{\bar{\bar{f}}(\alpha)d(\alpha)}{\bar{\bar{g}}(\alpha)d(\alpha)} \Rightarrow \gamma = \frac{\bar{\bar{f}}(\alpha)}{\bar{\bar{g}}(\alpha)},$$



где $\bar{\bar{f}}'(x)$ и $\bar{\bar{g}}(x)$ – полиномы над $P$, взаимно простые. Поделим числитель и значенатель на старший коэффициент $\bar{\bar{g}}(x)$. Получим требуемое.

II. Единственность. Допустим, что $\gamma = \frac{f(\alpha)}{g(\alpha)} = \frac{t(\alpha)}{s(\alpha)}$, где $f(x), g(x), t(x)$ и $s(x)$ удовлетворяют условию. Рассмотрим полином $f(x)s(x) - g(x)t(x) \equiv F(x)$. $F(\alpha) = 0$.
Так как $\alpha$ трансцедентно, то $F(x) \equiv 0$. Тогда
$$f(x)s(x) = g(x)t(x) \tag{I}$$
$f(x)s(x) \,\vdots\, t(x)$, но $t(x)$ и $s(x)$ взаимно просты, значит, $f(x) \,\vdots\, t(x)$, $g(x)t(x) \,\vdots\, f(x)$, но $f(x)$ и $g(x)$ взаимно просты, значит $t(x) \,\vdots\, f(x)$. По свойству делимости
$$f(x) = c\,t(x) \tag{2}$$

Представим (2) в (I): $c\,s(x) = g(x)$. Но у $s(x)$ и $g(x)$ старшие коэффициенты равны единице, значит, $c = 1$ по единственности нормальной формы, т.е. $s(x) = g(x)$. А тогда из (I) $\Rightarrow f(x) = t(x)$. И это означает единственность представления $\gamma$.

ТЕОРЕМА 3.

I. Любой элемент простого алгебраического расширения $P[\alpha]$ алгебраичен.

2. Любой элемент простого транцедентного расширения $P[\alpha]$, не принадлежащий $P$, тарнсцедентен.

Доказательство:

I. часть теоремы доказывается ниже (в процессе доказательства теоремы 5).

2. часть: пусть $\gamma \in P[\alpha]$ следовательно, по предложению 3 $\gamma = \frac{f(\alpha)}{g(\alpha)}$, где $f(x)$ и $g(x)$ удовлетворяют условиям этого предложения. $\gamma \notin P \Rightarrow f(x) \neq c$ или $g(x) \neq c$.
Действительно, если бы $f(x) = const$ и $g(x) = const$, то они принадлежали бы $P$ и $\gamma$, как их частное, тоже лежало бы в $P$. Допустим противное: $\gamma$ алгебраично относительно $P$. Значит, существует полином $F(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m$ | $F(x) \neq c$ и $F(\gamma) = 0$.

Имеем: $b_0(f(\alpha))^m + b_1(f(\alpha))^{m-1} g(\alpha) + \ldots + b_{m-1}f(\alpha)g^{m-1}(\alpha) = -(g(\alpha))^m b_m$.

Пусть $f(x) \neq c$. $\alpha$ – корень $G(x) = b_0(f(x))^m + \ldots + b_m(g(x))^m$, но $\alpha$ трансцедентно, значит $G(x)\equiv 0$. Получим: $b_0(f(x))^m + b_1(f(x))^{m-1}g(x)+\dots+b_{m-1}f(x)g^{m-1}(x) = -b_m(g(x))^m$

Так как $f(x)\neq c$, то у $f(x)$ есть неприводимый множитель $p(x)$. Левая часть последнего равенства делится на $p(x)$, значит, и правая часть делится на $p(x)$. Это означает, что $g(x)\,\vdots\,p(x)$ (почему?)

$f(x)\,\vdots\,p(x)$, $g(x)\,\vdots\,p(x) \Rightarrow НОД(f(x),g(x))\,\vdots\,p(x)$, но $f(x)$ и $g(x)$ взаимно просты по построению $\Rightarrow$ $\Rightarrow 1\,\vdots\,p(x)$ $(1 = НОД(f(x),g(x)))$. Получили противоречие. Значит, $\gamma$ трансцедентно относительно $P$. Теорема доказана.

ТЕОРЕМА 4. (О примитивном элементе).

Пусть $P$ – поле; $\alpha,\beta$ – алгебраичны относительно $P$. Тогда существует алгебраическое относительно $P$ число $\gamma$, такое, что $P[\gamma] = (P[\alpha])[\beta]$.

Доказательство: I) Сначала найдем $\gamma$. Так, $\alpha,\beta$ алгебраичны относительно $P$, то по теореме I существуют неприводимые над полем $P$ полиномы $p(x)$ и $q(x)$, которые имеют $\alpha$ и $\beta$ своими корнями.

Рассмотрим полином $p(x)$. Пусть $\alpha_1,\alpha_2,\dots,\alpha_i,\dots,\alpha_n$ – все корни этого полинома. Пусть $\beta_1,\beta_2,\dots,\beta_j,\dots,\beta_m$ – все корни полинома $q(x)$. Множество

$$A = \left\{ \pm\frac{\alpha-\alpha_i}{\beta_j-\beta},\ \beta_j\neq\beta \right\}$$ – конечное множество.

$Q\cap A$ – конечное (или пустое) множество. $T = Q\setminus(Q\cap A)\neq\emptyset$ (если бы $T=\emptyset$, то $Q = Q\cap A$, но $Q$ – бесконечно, а $Q\cap A$ конечно). Значит, $(\exists c\in T\subset Q)$. Положим $\gamma = \alpha + c\beta$.

2) Докажем, что $P[\gamma]\subset(P[\alpha])[\beta]$. По предложению I для этого достаточно показать, что $\gamma\in(P[\alpha])[\beta]$ и $P\subset(P[\alpha])[\beta]$,

$$P\subset P[\alpha]\subset(P[\alpha])[\beta],$$

$\gamma = \alpha + c\beta$, но $\alpha\in P[\alpha]\subset(P[\alpha])[\beta]$; Следовательно, $c\in Q\subset P\subset(P[\alpha])[\beta]$; $\gamma\in(P[\alpha])[\beta]$;



$\beta\in(P[\alpha])[\beta]$ (так как $(P[\alpha])[\beta]$ – поле).

3) Докажем теперь, что $(P[\alpha])[\beta]\subset P[\gamma]$. По предложению I достаточно показать, что $\alpha\in P[\gamma]$, $\beta\in P[\gamma]$, $P\subset P[\gamma]$. Очевидно, что $P\subset P[\gamma]$. Рассмотрим полином $p(\gamma - cx)$. Это полином над полем $P[\gamma]$. Полином $q(x)$ также на полем $P[\gamma]$. Найдем их НОД: $d(x) = НОД(p(\gamma-cx), q(x))$, $d(x)$ – полином над $P[\gamma]$. $\beta$ – корень $q(x)$ по построению; $p(\gamma - c\beta) = p(\alpha) = 0$, так как $\alpha$ – корень $p(x)$ по построению. Итак, $\beta$ – общий корень $q(x)$ и $p(\gamma - cx)$, значит, $q(x)\,\vdots\,(x-\beta)$, $p(\gamma - cx)\,\vdots\,(x-\beta)$. А тогда $d(x)\,\vdots\,(x-\beta)$, а значит, $\beta$ – корень $d(x)$.

Покажем, что никаких других корней $d(x)$ не имеет. Пусть $\delta\neq\beta$ – корень $d(x)$. Тогда $p(\gamma - c\delta) = 0$, $q(\delta) = 0$; $\gamma - c\delta$ – корень $p(x) \Rightarrow \gamma - c\delta = \alpha_i \neq \alpha$ (иначе, $\gamma - c\delta = \alpha \Rightarrow$ $\Rightarrow \delta = \beta$, а это не так). $\delta$ – корень $q(x) \Rightarrow \delta = \beta_j \neq \beta$. Итак, $\gamma - c\beta_j = \alpha_i$; $\alpha + c\beta - c\beta_j = \alpha_i$; $c = \frac{\alpha_i - \alpha}{\beta - \beta_j}\in A$, но $c\notin A$. Значит, у полинома $d(x)$ только один корень $\beta$. Тогда $d(x) = (x-\beta)^k$, $k\in N$. Второй коэффициент в нормальной форме $d(x)$ – $k\beta$, все коэффициенты лежат в $P[\gamma]$ ($d(x)$ – полином над $P[\gamma]$), значит, $-k\beta\in P[\gamma]$.

$k\in N\subset Q\subset P\subset P[\gamma] \Rightarrow \beta = \frac{-k\beta}{-k}\in P[\gamma]$ ($P[\gamma]$ – поле!)

Мы показали, что $\beta\in P[\gamma]$. Кроме того, известно, что $\gamma\in P[\gamma]$. $c\in Q\subset P\subset P[\gamma]$. Следовательно, $\alpha = \gamma - c\beta\in P[\gamma]$.

4) Осталось доказать, что $\gamma$ алгебраично относительно поля $P$. Если бы $\gamma$ было трансцедентным относительно $P$, то по теореме 3 все элементы $P[\gamma]$, не лежащие в $P$, тоже были бы трансцедентными. Однако числа $\alpha$ и $\beta$ принадлежат $P[\gamma]$ и являются алгебраическими относительно $P$, значит, $\gamma$ тоже алгебраично относительно $P$. (Если $\alpha\in P$ и $\beta\in P$, то $\gamma = \alpha + c\beta\in P$ и, следовательно, алгебраично относительно $P$). Теорема доказана.

Теперь можно доказать предложение 2, сформулированное в начале этого параграфа.

Пусть $\alpha,\beta$ алгебраичны относительно $P$. По теореме о примитивном элементе $(P[\alpha])[\beta] = P[\gamma]$, где $\gamma$ алгебраично относительно $P$. По теореме 3 все элементы $P[\gamma]$ алгебраичны относительно $P$, поэтому, поскольку

$$\alpha \pm \beta \in P[\gamma],\ \alpha\cdot\beta \in P[\gamma],\ \frac{\alpha}{\beta} \in P[\gamma],\ \beta\neq 0)$$

( $P[\gamma]$ – поле, $\alpha\in P[\gamma], \beta\in P[\gamma]$ ), то числа $\alpha\pm\beta, \alpha\cdot\beta, \frac{\alpha}{\beta}$ алгебраичны относительно $P$, т.е. множество всех алгебраических числе образует поле.

Определение 5. Пусть $P$ – числовое поле, $\alpha_1,\dots,\alpha_n \in \mathbb{C}$. Множество $P[\alpha_1,\dots,\alpha_n] = \left\{\frac{f(\alpha_1,\dots,\alpha_n)}{g(\alpha_1,\dots,\alpha_n)}\right\}$, где $f(x_1,\dots,x_n)$, $g(x_1,\dots,x_n)$ – полиномы над $P$ и $g(\alpha_1,\dots,\alpha_n)\neq 0$, называется расширением поля $P$, порожденным элементами $\alpha_1,\dots,\alpha_n$.

Определение 6. Расширение $P[\alpha_1,\dots,\alpha_n]$ называется алгебраически порожденным, если $\alpha_1,\dots,\alpha_n$ алгебраичны относительно поля $P$.

Для расширений, порожденных элементами $\alpha_1,\dots,\alpha_n$, выполняется предложение, аналогичные предложению I для простых расширений (сформулируйте самостоятельно).

Лемма. $P[\alpha_1,\dots,\alpha_n] = (P[\alpha_1,\dots,\alpha_{n-1}])[\alpha_n]$, т.е. расширение $P[\alpha_1,\dots,\alpha_n]$ можно получить из $P$ при помощи ряда последовательных расширений. Доказательство проведите самостоятельно (покажите, что $P[\alpha_1,\dots,\alpha_n] \subset (P[\alpha_1,\dots,\alpha_{n-1}])[\alpha_n]$ и наоборот: $((P[\alpha_1,\dots,\alpha_{n-1}])[\alpha_n] \subset P[\alpha_1,\dots,\alpha_n]$, используя определение 5). С помощью этой леммы методом математической индукции, доказывается, что

I) $P[\alpha_1,\dots,\alpha_n]$ состоит из всевозможных значений полиномов над $P$ от $\alpha_1,\dots,\alpha_n$ (теорема, аналогичная теореме об освобождении от иррациональности в знаменателе при $n=1$ ).

2) если $P$ – поле, $\alpha_1,\dots,\alpha_n$ являются алгебраическими относительно $P$, то существует алгебраическое относительно $P$ число $\delta$ такое, что $P[\alpha_1,\dots,\alpha_n] = P[\delta]$.

(теорема, аналогичная теореме о примитивном элементе при $n=2$ ).

ТЕОРЕМА 5. Любое конечное расширение $K$ является алгебраически порожденным.

Доказательство: Пусть $K$ – конечное расширение поля $P$ и пусть размерность $K$ относительно $P$ равна $n$. Возьмем произвольный элемент $\beta\in K$. Тогда $1,\beta,\dots,\beta^n$ линейно зависимы над $P$, т.е. $(\exists c_0, c_1,\dots,c_n)$ такие, что $(\exists i)(0\le i\le n)$



$c_i \neq 0$ и $c_0 + c_1\beta + \dots + c_n\beta^n = 0$. Это означает, что $\beta$ – корень полинома $c_0 + c_1\beta + \dots + c_n\beta^n$ и, следовательно, является алгебраическим числом относительно $P$. (точно так же доказывается I часть теоремы 3). Пусть теперь $\alpha_1,\dots,\alpha_n$ – базис $K$ над $P$. По доказанному все числа $\alpha_1,\dots,\alpha_n$ алгебраические относительно $P$, значит, если мы докажем, что $K = P[\alpha_1,\dots,\alpha_n]$, то тем самым докажем теорему. С одной стороны, $\alpha_1,\dots,\alpha_n \in P[\alpha_1,\dots,\alpha_n]$, тогда $b_1\alpha_1 + \dots + b_n\alpha_n$ ( $b_i \in P$ ) тоже принадлежат $P[\alpha_1,\dots,\alpha_n]$ т.е. $K \subset P[\alpha_1,\dots,\alpha_n]$

С другой стороны, $P[\alpha_1,\dots,\alpha_n] \subset K$ в силу того, что $P[\alpha_1,\dots,\alpha_n]$ – минимальное из всех полей, содержащих $P$ и $\alpha_1,\dots,\alpha_n$. Теорема доказана.

Замечание 3. Всякое алгебраическое порожденное расширение является простым (смотри пункт 2) перед теоремой 5). А тогда с учетом теорем 5 и 2 можно сделать вывод о том, что конечные расширения исчерпываются простыми алгебраическими расширениями.

## 10. Нормальные расширения полей

Определение I. Простое алгебраическое расширение $P[\delta]$ поля $P$ называется нормальным, если существует полином $f(x)$ над полем $P$, такой что

$P[\delta] = P[\beta_1,\dots,\beta_n]$, где $\{\beta_1,\dots,\beta_n\}$ – множество всех корней $f(x)$

Определение 2. Корни минимального полинома для числа $\delta$ относительно поля $P$ называются числами, сопряженными с $\delta$ относительно $P$.

ПРИМЕР. Пусть $P = Q$, $\delta = \sqrt{2}$. Расширение $Q[\sqrt{2}]$ – нормальное, так как существует полином $f(x) = x^2 - 2$ над $Q$ ( $\beta_1 = \sqrt{2}$, $\beta_2 = -\sqrt{2}$ / его корни), такой что $Q[\sqrt{2}] = Q[\sqrt{2}, -\sqrt{2}]$ – это равенство очевидно следует из предложения I из 9.

$-\sqrt{2}$ – число, сопряженное с $\sqrt{2}$ относительно $Q$; степень расширения $Q[\sqrt{2}]$ равна двум.

Лемма. Пусть $\delta_1$ – сопряженное с $\delta$ относительно $P$. Тогда если некоторый полином $f(x)$ над полем $P$ имеет $\delta$ своим корнем, то он имеет и $\delta_1$ своим корнем.

Доказательство: Пусть $p(x)$ – минимальный полином для $\delta$ относительно поля $P$.

Тогда $f(x) \vdots p(x) \Longleftrightarrow f(x) = p(x)q(x)$

$$f(\delta_i) = p(\delta_i)q(\delta_i) = 0$$

ибо $\delta_i$ – сопряженное с $\delta$ относительно $P$, и потому $p(\delta_i) = 0$.

ТЕОРЕМА (Критерий нормальности).

Простое алгебраическое расширение $P[\delta]$ поля $P$ является нормальным тогда и только тогда, когда все числа, сопряженные с $\delta$ относительно поля $P$, принадлежат $P[\delta]$.

Доказательство:

I. Необходимость. Пусть $P[\delta]$ – нормальное расширение. По определению I существует полином $f(x)$ с корнями $\beta_1, \dots, \beta_n$ такой, что

$$P[\delta] = P[\beta_1, \dots, \beta_n] \qquad (1)$$

$\beta_i \in P[\delta]$, $i = 1, \dots, n$, следовательно, по теореме об освобождении от иррациональности в знаменателе

$$\beta_i = H_i(\delta) \qquad (2)$$

( $H_i$ – полиномы над $P$ )

$f(H_i(\delta)) = f(\beta_i) = 0$ – таким образом, $\delta$ – корень полиномов $f(H_i(x))$, тогда по лемме любое $\delta_j$, сопряженное с $\delta$ относительно $P$, – корень $f(H_i(x))$, $f(H_i(\delta_j)) = 0$ значит, $H_i(\delta_j) = \beta_k$ (3), так как других корней у $f(x)$ кроме $\beta_1, \dots, \beta_n$, нет. $\delta = \Phi(\beta_1, \dots, \beta_n)$ по "обобщенной" теореме об освобождении от иррациональности в знаменателе, следовательно, учитывая (2), получаем, что $\delta = \Phi(H_1(\delta), \dots, H_n(\delta))$.

Рассмотрим полином над $P$, $x - \Phi(H_1(x), \dots, H_n(x))$. Любое $\delta_j$ будет его корнем по лемме (ведь $\delta$ – его корень!), откуда каждое

$$\delta_j = \Phi(H_1(\delta_j), \dots, H_n(\delta_j)) \underset{(3)}{=} \Phi(\beta_1, \beta_2, \dots, \beta_n) \underset{(1)}{\in} P[\delta]$$

II. Достаточность. Пусть теперь все числа, сопряженные с $\delta$ относительно поля $P$, принадлежат $P[\delta]$. Докажем, что $P[\delta]$ – нормальное расширение. Здесь доказательство очень простое: возьмем в качестве полинома $f(x)$ из определения нормальности полином $p(x)$, минимальный для $\delta$ относительно $P$. Так как все его корни лежат в $P[\delta]$, то ясно, что $P[\delta] = P[\delta, \delta_2, \dots, \delta_n]$.



Теорема доказана полностью.

## II. Автоморфизмы простых расширений

Вообще автоморфизмом множества $M$ называется биективное отображение $M$ на себя (геометрическое преобразование $M$), "сохраняющее" действия.

Определение. Пусть $P[\alpha]$ – простое расширение поля $P$. Биективное отображение $f: P[\alpha] \to P[\alpha]$ называется автоморфизмом $P[\alpha]$, если

$$\forall a, b \in P[\alpha] \quad \begin{cases} f(a+b) = f(a) + f(b) \\ f(ab) = f(a) \cdot f(b) \end{cases}$$

$$\forall \beta \in P \qquad f(\beta) = \beta$$

Предложение I. Совокупность всех автоморфизмов $P[\alpha]$ (обозначаем $G_{P[\alpha]}$ ) образует группу преобразований $P[\alpha]$.

Доказательство: Все автоморфизмы – биективные преобразования (по определению). Пусть $f, g$ – автоморфизмы; $f \circ g$ – биекция (композиция биекций – биекция!) и, кроме того, $\forall a, b \in P[\alpha]$

$$(f \circ g)(ab) = f(g(ab)) = f(g(a)g(b)) =$$
$$= f(g(a)) \cdot f(g(b)) = (f \circ g)(a) \cdot (f \circ g)(b)$$

Аналогично для другого действия.

Очевидно, что $\forall \beta \in P \quad (f \circ g)(\beta) = \beta$.

Итак, по определению $f \circ g$ – автоморфизм. Пусть $h$ – автоморфизм, $h^{-1}$ – существует и является биекцией $\forall a, b \in P[\alpha]$

$$h(h^{-1}(a+b)) = a+b$$
$$h(h^{-1}(a) + h^{-1}(b)) = h(h^{-1}(a)) + h(h^{-1}(b)) = a+b$$

Так как образы при биекции равны, то равны и прообразы и $h^{-1}(a+b) = h^{-1}(a) + h^{-1}(b)$.

Аналогично для другого действия. $h(h^{-1}(\beta)) = \beta = h(\beta), \forall \beta \in P$ следовательно, $h^{-1}(\beta) = \beta$, т.е. $h^{-1}$ – автоморфизм. А тогда $G_{P[\alpha]}$ – группа преобразований $P[\alpha]$ по определению 9 из I.

Аналогично вводится понятие автоматизма расширения $P[\alpha_1, \dots, \alpha_n]$, порожденного элементами $\alpha_1, \dots, \alpha_n$ и показывается, что $G_{P[\alpha_1, \dots, \alpha_n]}$ – группа.

Предложение 2. Любой автоморфизм из $G_{P[\alpha]}$ переводит каждый корень $\varepsilon \in P[\alpha]$ некоторого полинома над полем $P$ снова в корень этого же полинома.

Доказательство: Пусть $\varepsilon$ – корень некоторого полинома $g(x)$ над полем $P$. Тогда $g(\varepsilon)=0$. Докажем, что $f(\varepsilon)$ – корень полинома $g(x)$, т.е. $g(f(\varepsilon))=0$, $(f \in G_{P[\alpha]})$.

$$g(f(\varepsilon)) = a_0(f(\varepsilon))^n + a_1(f(\varepsilon))^{n-1} + \ldots + a_n = \underset{(a_i \in P)}{}$$
$$= f(a_0\varepsilon^n + a_1\varepsilon^{n-1} + \ldots + a_n) = f(g(\varepsilon)) = f(0) = 0.$$

(мы использовали то, что $f$ – автоморфизм, а также то, что $0 \in P$).

Лемма. У минимального полинома $p(x)$ для числа $\alpha$ относительно поля $P$ нет кратных корней.

Доказательство: Допустим противное:

$p(x) = (x-\alpha_1)\cdot\ldots\cdot(x-\beta)(x-\beta)\cdot\ldots\cdot(x-\alpha_e)$, т.е. $\beta$ – кратный корень $p(x)$. Пусть $d(x) = НОД(p(x), p'(x))$, $p(x) = d(x)\bar{p}(x)$; $\bar{p}(x)$ – полином над $P$ и $\bar{p}(\alpha)=0$ по известной из курса алгебры теореме о том, что $\bar{p}(x)$ имеет те же корни, что и $p(x)$, но только первой кратности. $d(x) \neq const$, так как $\beta$ – корень и $p(x)$ и $p'(x)$, следовательно, $\alpha$ – корень полинома над $P$ степени меньшей, чем степени $p(x)$, что противоречит минимальности $p(x)$.

ТЕОРЕМА I. Пусть $P[\alpha]$ – нормальное расширение размерности $n$, тогда $|G_{P[\alpha]}| = n$.

Доказательство: Нужно установить биекцию между $G_{P[\alpha]}$ и множеством, состоящим из $n$ элементов. По лемме минимальный полином $p(x)$ для $\alpha$ относительно $P$ имеет $n$ различных корней, поэтому соответствие установим между $G_{P[\alpha]}$ и $T=\{\beta_1,\ldots,\beta_n\}$ где $\beta_{i\,(i=\overline{1,n})}$ – корни полинома $p(x)$, по правилу $\forall f \in G_{P[\alpha]}$

$\varphi(f) = f(\alpha)$ Заметим, что $f(\alpha) \in T$ по предложению 2. Покажем, что установленное соответствие $\varphi$ является биекцией. $\varphi$ – функция и отображение, так как $f$ – функция и отображение. Докажем, что $\varphi$ – инъекция. Допустим, что $f_1 \neq f_2$, а $\varphi(f_1) = \varphi(f_2)$, это значит, что $f_1(\alpha) = f_2(\alpha)$ (I). Тогда $\forall \delta \in P[\alpha]$ по теореме об освобождении от иррацио-



нальности в знаменателе $\delta = H(\alpha)$ ($H$ – полином над $P$), т.е. $\delta = b_0\alpha^{n-1} + \ldots + b_{n-1}$ $(b_i \in P)$;

$$f_1(\delta) = b_0(f_1(\alpha))^{n-1} + \ldots + b_{n-1} = b_0(f_2(\alpha))^{n-1} + \ldots + b_{n-1} = f_2(\delta)$$

(мы использовали то, что $f_1$ и $f_2$ – автоморфизмы, а также равенство (I)). Получили, что $f_1 = f_2$, что противоречит данному. Значит, $\varphi(f_1) \neq \varphi(f_2)$, и инъекция доказана. Осталось доказать, что $\varphi$ – сюръекция. Пусть есть некоторый корень полинома $p(x)$. Обозначим его $\beta$. Преобразование $f: P[\alpha] \to P[\alpha]$ зададим так:

$$\forall \delta = a_0\alpha^{n-1} + \ldots + a_{n-1} \in P[\alpha]$$
$$f(\delta) = a_0\beta^{n-1} + \ldots + a_{n-1}, \quad (a_i \in P).$$

Покажем, что $f$ – необходимый нам автоморфизм. $f(\alpha)=\beta$ по заданию $f$. Остается проверить, что $f$ – автоморфизм $P[\alpha]$. $f(\delta) \in P[\alpha]$, так как $\beta \in P[\alpha]$ по критерию нормальности, $a_i \in P \subset P[\alpha]$, а $P[\alpha]$ – поле; $f$ – функция: если $f(\delta) = \alpha_1$ и $f(\delta) = \alpha_2$, то $\alpha_1 = \alpha_2$ по единственности освобождения от иррациональности в знаменателе. $f$ – отображения, так как $\forall \delta \in P[\alpha]$, $\delta = H(\alpha)$ ($H$ – полином над $P$), значит, $f(\delta)$ определено.

Пусть теперь $\delta_1, \delta_2 \in P[\alpha]$ : $\delta_1 \neq \delta_2$, $\delta_1 = H(\alpha)$, $\delta_2 = G(\alpha)$, причем степени полиномов $H$, $G$ меньше $n$, $F(x) \equiv H(x) - G(x) \neq 0$ (так как $H(\alpha) \neq G(\alpha)$), степень $F(x)$ также меньше $n$.

Предположим, что $f(H(\alpha)) = f(G(\alpha))$. Тогда поскольку $f$ – автоморфизм, это будет означать, что $H(f(\alpha)) = G(f(\alpha))$ следовательно $H(f(\alpha)) - G(f(\alpha)) = 0 \Rightarrow F(f(\alpha)) = 0 \Rightarrow F(\beta) = 0$. Получили, что $\beta$ – корень полинома степени меньшей, чем $n$, значит, с одной стороны, по теореме I из 9 $F(x) \vdots p(x)$, а с другой стороны, степень $F(x)$ < степени $p(x)$ (противоречие). Поэтому $f(H(\alpha)) \neq f(G(\alpha))$, т.е. $f$ – инъекция. $f$ – также и сюръекция:

$$\forall \mu = a_0\beta^{n-1} + \ldots + a_{n-1} \in P[\alpha], \ \exists\, \delta = a_0\alpha^{n-1} + \ldots + a_{n-1} \in P[\alpha]$$
$$f(\delta) = \mu$$

Итак, преобразование $f$ биективно.

$$f(\delta_1+\delta_2) = f(a_0\alpha^{n-1}+\ldots+a_{n-1}+b_0\alpha^{n-1}+\ldots+b_{n-1}) =$$

$$= f(\alpha^{n-1}(a_0+b_0)+\ldots+a_{n-1}+b_{n-1}) \underset{f(\alpha)=\beta}{=}$$

$$= (a_0+b_0)\beta^{n-1}+\ldots+a_{n-1}+b_{n-1} =$$

$$= f(\delta_1)+f(\delta_2)$$

Пусть $\mu = \sum_{i=0}^{n-1} a_i\cdot\alpha^i$ ; $\nu = \sum_{j=0}^{n-1} b_j\cdot\alpha^j$

$$f(\mu\nu) = f\left(\sum_{i,j=0}^{n-1} a_i\cdot b_j\cdot\alpha^{i+j}\right) =$$

$$= \sum_{i,j=0}^{n-1} a_i\cdot b_j\cdot\beta^{i+j} = \sum_{i=0}^{n-1} a_i\cdot\beta^i\cdot\sum_{j=0}^{n-1} b_j\cdot\beta^j =$$

$$= f(\mu)f(\nu).$$

Наконец, $f(\beta)=\beta$ , $\forall\beta\in P$ по правилу задания $f$ .
Вывод: $f$ - автоморфизм. Доказана сюръективность соответствия $\varphi$ . Таким образом, $\varphi: G_{P[\alpha]} \to T=\{\beta_1,\ldots,\beta_n\}$ - биекция, а тогда $G_{P[\alpha]}$ содержит ровно $n$ элементов. Теорема доказана.

Замечание I. В процессе доказательства инъективности $\varphi$ было доказано, что из равенства автоморфизмов $P[\alpha]$ на элементе $\alpha$ следует их равенство на всем $P[\alpha]$.

ПРИМЕР. Как уже было показано, $Q[\sqrt{2}]$ - нормальное алгебраическое расширение размерности 2. Найдем группу автоморфизмов этого расширения.

$$\forall f\in G_{Q[\sqrt{2}]} \qquad 2 = f(2) = f((\sqrt{2})^2) = f(\sqrt{2})\cdot f(\sqrt{2}) = (f(\sqrt{2}))^2$$

следовательно, $\left[\begin{array}{l} f(\sqrt{2}) = \sqrt{2} \\ f(\sqrt{2}) = -\sqrt{2} \end{array}\right.$

Первый случай соответствует тождественному автоморфизму $e$ ,



поскольку $f(a+b\sqrt{2}) = f(a)+f(b)\cdot f(\sqrt{2}) =$

$$= a+b\sqrt{2} = e(a+b\sqrt{2}) , \quad a,b\in Q$$

Второй случай осуществляется автоморфизмом $z$ таким, что $z(a+b\sqrt{2}) = a-b\sqrt{2}$ . Проверим, что это действительно автоморфизм. То, что $z$ - биекция, очевидно. Для произвольных чисел $a_1+b_1\sqrt{2}$ и $a_2+b_2\sqrt{2}$ из нашего расширения имеем:

$$z((a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})) = z((a_1+a_2)+(b_1+b_2)\sqrt{2}) =$$

$$= (a_1+a_2)-(b_1+b_2)\sqrt{2} = (a_1-b_1\sqrt{2})+(a_2-b_2\sqrt{2}) =$$

$$= z(a_1+b_1\sqrt{2}) + z(a_2+b_2\sqrt{2});$$

$$z((a_1+b_1\sqrt{2})\cdot(a_2+b_2\sqrt{2})) = z((a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}) =$$

$$= (a_1a_2+2b_1b_2)-(a_1b_2+a_2b_1)\sqrt{2} = (a_1-b_1\sqrt{2})(a_2-b_2\sqrt{2}) =$$

$$= z(a_1+b_1\sqrt{2})\cdot z(a_2+b_2\sqrt{2}).$$

Наконец, $\forall q\in Q$ , $z(q)=z(q+0\cdot\sqrt{2})=q$ . Итак, $z$ - автоморфизм. Все другие автоморфизмы, у которых $f(\sqrt{2})=\sqrt{2}$ или $f(\sqrt{2})=-\sqrt{2}$ , совпадают либо с тождественным $e$ , либо с $z$ по замечанию I. Таким образом, группа автоморфизмов данного расширения состоит из двух элементов $e$ и $z$ , которые перемножаются по правилу:

$$e\cdot e=e;\ e\cdot z=z\cdot e=z;\ z\cdot z=e.$$

ТЕОРЕМА II. Пусть $P[\alpha]$ - простое алгебраическое расширение поля $P$ размерности $n$ , $|G_{P[\alpha]}|=n$ . Тогда $P[\alpha]$ - нормальное расширение $P$ .

ДОКАЗАТЕЛЬСТВО: Как и в предыдущей теореме, устанавливаем соответствие $\varphi: G_{P[\alpha]} \to T=\{\beta_1,\ldots,\beta_n\}$ , где $T$ - множество корней минимального полинома $p(x)$ для $\alpha$ относительно $P$ , по правилу:

$$\forall f\in G_{P[\alpha]} \quad \varphi(f)=f(\alpha)$$

По предложению 2 $f(\alpha)\in T$ ; по замечанию I $\varphi$ - инъекция. Известно, что инъективное отображение между равномощными множествами (в данном случае, $G_{P[\alpha]}$ и $T$ содержат по $n$ элементов) биективно, в том числе это означает сюръективность $\varphi$

$$\forall \beta_j \in T, \ \exists f_j \in G_{P[\alpha]} : \varphi(f_j) = f_j(\alpha) = \beta_j \qquad (2)$$

$f_j(\alpha) \in P[\alpha]$ по определению автоморфизма, следовательно, $\beta_j \in P[\alpha]$ по (2), а тогда по критерию нормальности расширения $P[\alpha]$ - нормальное расширение $P$ . Теорема доказана.

Замечание 2. Из теорем I и II следует, что только у нормального расширения размерность совпадает с количеством элементов в группе автоморфизмов (ее называют группой Галуа нормального расширения $P[\alpha]$ ).

## 12. Промежуточные расширения

Определение. Пусть $P$ - числовое поле. Числовое поле $\Gamma$ называется промежуточным расширением поля $P$ , если $P \subset \Gamma \subset P[\alpha]$ где $P[\alpha]$ - простое расширение $P$ .

Свойства промежуточных расширений.

① Пусть $\Gamma$ - промежуточное расширение поля $P$ , а $P[\alpha]$ - простое алгебраическое расширение $P$ . Тогда $P[\alpha]$ - простое алгебраическое расширение поля $\Gamma$ .

Доказательство: докажем, что $P[\alpha] = \Gamma(\alpha)$ (1); так как $P \subset \Gamma \subset \Gamma[\alpha]$, то $P[\alpha] \subset \Gamma[\alpha]$ (мы использовали здесь $\alpha \in \Gamma[\alpha]$ предложение I из 9). $\Gamma[\alpha] \subset P[\alpha]$ по аналогичной причине ( $\Gamma \subset P[\alpha], \alpha \in P[\alpha]$ ) . Так как $\Gamma[\alpha]$ - простое алгебраическое расширение поля $\Gamma$ ( $\alpha$ алгебраично относительно $P$ по условию, т.е. $\alpha$ - корень полинома над $P$ , а следовательно, и над $\Gamma$ (так как $P \subset \Gamma$), таким образом, $\alpha$ алгебраично относительно $\Gamma$ ) и выполняется равенство (I), то $P[\alpha]$ - простое алгебраическое расширение поля $\Gamma$ .

② Пусть $\Gamma$ - промежуточное расширение поля $P$ , а $P[\alpha]$ - нормальное расширение $P$ . Тогда $P[\alpha]$ - нормальное расширение $\Gamma$ .

Доказательство: Учитывая равенство (I), будем доказывать, что $\Gamma[\alpha]$ - нормальное расширение $\Gamma$ . Так как $\alpha$ алгебраично как относительно поля $P$ , так и относительно поля $\Gamma$ , то существуют минимальные полиномы $p(x)$ над полем $P$ и $q(x)$ над полем $\Gamma$ для числа $\alpha$ . Поскольку полином $p(x)$ является в то же самое время и полиномом над $\Gamma$ (так как $P \subset \Gamma$), то по теореме о минимальном полиноме $p(x) \vdots q(x)$ или, что то же



самое, $p(x) = q(x) t(x)$ (2).

Возьмем число $\beta$ , сопряженное с $\alpha$ относительно $\Gamma$ , т.е. число, для которого $q(\beta) = 0$ , тогда из (2) следует, что и $p(\beta) = 0$ , т.е. $\beta$ - сопряженное с $\alpha$ относительно $P$ , а тогда по критерию нормальности $\beta \in P[\alpha] \underset{(1)}{=} \Gamma[\alpha]$ . Следовательно, по тому же критерию нормальности, примененному уже в обратную сторону, получаем, что $\Gamma[\alpha]$ - нормальное расширение $\Gamma$ , что и требовалось доказать.

ПРИМЕР. $Q \subset Q[\sqrt{2}] \subset Q[\sqrt{2}+\sqrt{5}]$ , так что $\Gamma = Q[\sqrt{2}]$ - промежуточное расширение поля $Q$ . Действительно, по предложению I из 9 $Q \subset Q[\sqrt{2}]$; $Q[\sqrt{2}] \subset (Q[\sqrt{2}])[\sqrt{5}]$ , а по теореме о примитивном элементе $Q[\sqrt{2},\sqrt{5}] = Q[\sqrt{2}+\sqrt{5}]$ , откуда и получаем, что

$$P = Q \subset \Gamma = Q[\sqrt{2}] \subset P[\alpha] = Q[\sqrt{2}+\sqrt{5}]$$
$$(\alpha = \sqrt{2}+\sqrt{5})$$

Лемма I. Пусть $\Gamma$ - промежуточное расширение поля $P$ , $P[\alpha]$ - простое алгебраическое расширение $P$ . Известно, что размерность $P[\alpha]$ относительно поля $P$ ( $\dim_P P[\alpha]$ ) равна $k$ ; размерность $P[\alpha]$ относительно $\Gamma$ ( $\dim_\Gamma P[\alpha]$ ) равна $\ell$ ; а размерность $\Gamma$ относительно $P$ ( $\dim_P \Gamma$ ) равна $s$ . Тогда $k = \ell \cdot s$ .

Замечание. То, что $P[\alpha]$ и $\Gamma[\alpha]$ - конечномерные линейные пространства над $P$ и над $\Gamma$ , ясно из теоремы об освобождении от иррациональности в знаменателе и свойства I . Можно проверить, что $\Gamma$ является линейным пространством над полем $P$ (по определению линейного пространства). $\Gamma$ конечномерно по теореме о том, что подпространство конечномерного пространства конечномерно, известной из курса алгебры.

Доказательство леммы: Пусть $\sigma_1, \dots, \sigma_\ell$ - базис $P[\alpha]$ относительно $\Gamma$ , а $\varepsilon_1, \dots, \varepsilon_s$ - базис $\Gamma$ относительно $P$ . Докажем, что система элементов, состоящая из всевозможных произведений $\sigma_i \cdot \varepsilon_j$ ( $i = 1 \div \ell$ , $j = 1 \div s$) является базисом $P[\alpha]$ относительно $P$ . Это и будет означать требуемое, так как в этом случае базис будет состоять из $\ell \cdot s$ элементов, а тогда $k = \dim_P P[\alpha] = \ell \cdot s$ .

а) проверим сначала линейную независимость этих элементов. Для этого напишем их линейную комбинацию и приравняем ее к нулю:

$$\alpha_{11}\sigma_1\varepsilon_1+\alpha_{12}\sigma_1\varepsilon_2+\ldots+\alpha_{1s}\sigma_1\varepsilon_s+\alpha_{21}\sigma_2\varepsilon_1+\alpha_{22}\sigma_2\varepsilon_2+\ldots+$$
$$+\alpha_{2s}\sigma_2\varepsilon_s+\ldots+\alpha_{l1}\sigma_l\varepsilon_1+\alpha_{l2}\sigma_l\varepsilon_2+\ldots+\alpha_{ls}\sigma_l\varepsilon_s=0,$$
$$(\alpha_{11}\varepsilon_1+\alpha_{12}\varepsilon_2+\ldots+\alpha_{1s}\varepsilon_s)\sigma_1+(\alpha_{21}\varepsilon_1+\alpha_{22}\varepsilon_2+\ldots+\alpha_{2s}\varepsilon_s)\sigma_2+$$
$$+\ldots+(\alpha_{l1}\varepsilon_1+\alpha_{l2}\varepsilon_2+\ldots+\alpha_{ls}\varepsilon_s)\sigma_l=0.$$

Однако $\sigma_1,\ldots,\sigma_l$ линейно независимы (это базис $P[\alpha]$ относительно $\Gamma$), значит, по определению линейной независимости получаем:

$$\begin{cases}\alpha_{11}\varepsilon_1+\alpha_{12}\varepsilon_2+\ldots+\alpha_{1s}\varepsilon_s=0,\\ \alpha_{21}\varepsilon_1+\alpha_{22}\varepsilon_2+\ldots+\alpha_{2s}\varepsilon_s=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\\ \alpha_{l1}\varepsilon_1+\alpha_{l2}\varepsilon_2+\ldots+\alpha_{ls}\varepsilon_s=0.\end{cases}$$

$\varepsilon_1,\ldots,\varepsilon_s$ тоже линейно независимы (это базис $\Gamma$ относительно $P$), поэтому можно заключить, что $\alpha_{ij}=0$ $(i=1\div l, j=1\div s)$, что и означает линейную независимость всевозможных элементов вида $\sigma_i\cdot\varepsilon_j$.

б) осталось показать, что любой элемент из простого алгебраического расширения $P[\alpha]$ линейно выражается через эти элементы $\sigma_i\varepsilon_j$ (с коэффициентами из $P$): возьмем произвольное $\xi\in P[\alpha]$;
$\xi=\gamma_1\sigma_1+\gamma_2\sigma_2+\ldots+\gamma_l\sigma_l$, где $\gamma_i\in\Gamma$ $(i=1\div l)$
В свою очередь, $\gamma_i$ линейно выражаются через $\varepsilon_1,\ldots,\varepsilon_s$ с коэффициентами из $P$, откуда и следует, что $\xi$ линейно выражается через $\sigma_i\varepsilon_j$ $(i=1\div l, j=1\div s)$ с коэффициентами из $P$.

ТЕОРЕМА I. Пусть $P[\alpha]$ – нормальное расширение поля $P$.
$$\Gamma=\{\xi\in P[\alpha]\mid \forall f\in G_{P[\alpha]},\ f(\xi)=\xi\}$$
Тогда $\Gamma=P$.

ДОКАЗАТЕЛЬСТВО: Сначала докажем, что $\Gamma$ определенное в условии теоремы является промежуточным расширением $P$.
$\Gamma$ – числовое поле. Это устанавливается непосредственной проверкой его замкнутости относительно четырех арифметических дей-



ствий:

пусть $\xi_1,\xi_2\in\Gamma$; рассмотрим разность $\xi_1-\xi_2$
$\xi_1\in P[\alpha]$, $\xi_2\in P[\alpha]$, $P[\alpha]$ – поле, следовательно,
$\xi_1-\xi_2\in P[\alpha]$ и $\forall f\in G_{P[\alpha]}$
$$f(\xi_1-\xi_2)=f(\xi_1+(-\xi_2))=f(\xi_1)+f(-\xi_2)=\xi_1-\xi_2.$$

значит, $\xi_1-\xi_2\in\Gamma$. $P\subset\Gamma$, так как $\forall\omega\in P$ $\omega\in P[\alpha]$ и $f(\omega)=\omega$ (по определению автоморфизма), значит, $\omega\in\Gamma$. Кроме того, $\Gamma\subset P[\alpha]$ (по построению $\Gamma$).

Итак, мы установили, что $\Gamma$ – числовое поле и $P\subset\Gamma\subset P[\alpha]$, значит, $\Gamma$ – промежуточное расширение $P$.

Согласно лемме I $\dim_P P[\alpha]=\dim_\Gamma P[\alpha]\cdot\dim_P\Gamma$.
Учитывая замечание 2 из II и то, что $P[\alpha]=\Gamma[\alpha]$ (свойство (I)), имеем: $\dim_P P[\alpha]=|G_{P[\alpha]}|$,
$$\dim_\Gamma P[\alpha]=\dim_\Gamma\Gamma[\alpha]=|G_{\Gamma[\alpha]}|$$
(здесь мы использовали также нормальность $\Gamma[\alpha]$, вытекающую из свойства (2)). Докажем, что $G_{P[\alpha]}=G_{\Gamma[\alpha]}$.
$\forall f\in G_{P[\alpha]}, \forall\xi\in\Gamma$, $f(\xi)=\xi$ (по выбору $\Gamma$) $\Rightarrow f\in G_{\Gamma[\alpha]}$
Обратно: $\forall f\in G_{\Gamma[\alpha]}, \forall\xi\in\Gamma$, $f(\xi)=\xi$ по определению автоморфизма, а тогда $\forall\omega\in P$, $f(\omega)=\omega$ (так как $P\subset\Gamma$), значит, $f\in G_{P[\alpha]}$.

Мы проверили только одно условие из определения автоморфизма. Остальные проверять не нужно, так как $P[\alpha]=\Gamma[\alpha]$.

Итак, показано, что $G_{P[\alpha]}=G_{\Gamma[\alpha]}$, тогда
$|G_{P[\alpha]}|=|G_{\Gamma[\alpha]}|$, т.е. $\dim_P P[\alpha]=\dim_\Gamma P[\alpha]$. Вытекает, что $\dim_P\Gamma=1$.

$\Gamma$ – конечномерное линейное пространство над $P$,
$P\subset\Gamma$ – его подпространство, $\dim_P P=1$ (очевидно), а тогда по известной из курса алгебры теореме о подпространства $\Gamma=P$ (теорема говорит о том, что если размерность подпространства $\bar Z$ совпадает с размерностью самого пространства $Z$, то $Z=\bar Z$). Теорема доказана.

<u>Лемма 2.</u> Пусть $P[\alpha]$ – простое алгебраическое расширение поля $P$; $H=\{h_1,h_2,\ldots,h_m\}$ – подгруппа $G_{P[\alpha]}$.

Обозначим $h_i(\xi)=\varepsilon_i$, $(\xi\in P[\lambda]$, $i=1\div m)$ и рассмотрим полином $f(x)=(x-\varepsilon_1)(x-\varepsilon_2)\cdot\ldots\cdot(x-\varepsilon_m)\equiv$
$\equiv a_0x^m+a_1x^{m-1}+\ldots+a_m$
Тогда $\forall h_i\in H$, $\forall a_j$, $h_i(a_j)=a_j$, $i=1\div m$, $j=1\div m$

Доказательство: $a_0=1\in P$, значит, $h_i(a_0)=a_0$ $(i=1\div m)$ по определению автоморфизма.

По известным из алгебры формулам Виета

$$a_1=-(\varepsilon_1+\varepsilon_2+\ldots+\varepsilon_m)$$
$$a_2=\sum\varepsilon_k\varepsilon_\ell$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_m=(-1)^m\varepsilon_1\ldots\varepsilon_m$$

$$h_i(\varepsilon_j)=h_i(h_j(\xi))=(h_i\circ h_j)(\xi)=h_t(\xi)=\varepsilon_t$$

(мы использовали здесь, что $H$ – подгруппа). Так как $h_i$ – инъекции, то они лишь переставляют $\varepsilon_j$ местами при воздействии на них, а так как $a_1,\ldots,a_m$ – симметрические полиномы от $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_m$, то они не меняются при любой перестановке.

ТЕОРЕМА 2. Пусть $P[\lambda]$ – нормальное расширение поля $P$.

$$H=\{h_1,h_2,\ldots,h_m\}\text{ – подгруппа } G_{P[\lambda]}.$$
$$\Gamma=\{\delta\in P[\lambda]\mid\forall h_i\in H,\ h_i(\delta)=\delta\}$$

Тогда $G_{\Gamma[\lambda]}=H$

Доказательство: Нужно доказать два включения.

I) Докажем сначала, что $H\subset G_{\Gamma[\lambda]}$. Установим, что $\Gamma$ – промежуточное расширение поля $P$: То, что $\Gamma$ – числовое поле, показывается аналогично тому, как это было сделано в теореме I. Кроме того, $P\subset\Gamma$, так как $\forall\delta\in P$, $\delta\in P[\lambda]$ $h_i(\delta)=\delta$ по определению автоморфизма $\Rightarrow\delta\in\Gamma$ по выбору $\Gamma$. $\Gamma\subset P[\lambda]$ по построению $\Gamma$.

$\forall\xi\in\Gamma$, $h_i(\xi)=\xi$, а тогда $\forall h_i\in H$, $h_i\in G_{\Gamma[\lambda]}$

(остальные свойства автоморфизма не проверяем, так как $\Gamma[\lambda]=P[\lambda]$)

2) Обратно: пусть $|G_{\Gamma[\lambda]}|=k$. Если доказать, что $k\le m$, то с учетом доказанного в I) получим требуемое. Пусть $h_1(\lambda)=\varepsilon_1,\ldots,h_m(\lambda)=\varepsilon_m$. По лемме 2 полином



$f(x)=(x-\varepsilon_1)\cdot\ldots\cdot(x-\varepsilon_i)\cdot\ldots\cdot(x-\varepsilon_m)$ – полином над $\Gamma$ $(h_t(a_j)=a_j\Rightarrow a_j\in\Gamma$ по выбору $\Gamma)$. В подгруппе $H$ есть тождественное преобразование, пусть это будет $h_i$. Тогда $\varepsilon_i=h_i(\lambda)=\lambda$, а потому $f(\lambda)=0$. Получили, что полином степени $m$ над $\Gamma$ имеет $\lambda$ своим корнем, а значит, делится на минимальный полином $p(x)$ для $\lambda$ относительно $\Gamma$, имеющий степень $k$ (почему?), т.е.

$$f(x)\,\vdots\,p(x)\Rightarrow m\ge k$$

Вывод: $G_{\Gamma[\lambda]}=H$. Теорема доказана.

## I3. Связи Галуа

Вначале сделаем выводы из теорем, доказанных в предыдущем параграфе. Итак, пусть $P[\lambda]$ – нормальное расширение поля $P$, $\Gamma$ – промежуточное расширение $P$ (т.е. $P\subset\Gamma\subset P[\lambda]$), $H$ – подгруппа $G_{P[\lambda]}$.

Положим $\mathcal{F}(H)=\Gamma=\{\delta\in P[\lambda]\mid\forall h_i\in H,\ h_i(\delta)=\delta\}$. Это $\Gamma$ – промежуточное расширение по теореме 2 из I2. Положим $\Psi(\Gamma)=G_{\Gamma[\lambda]}$. Тогда: во-первых, $H\xrightarrow{\mathcal{F}}\Gamma\xrightarrow{\Psi}G_{\Gamma[\lambda]}=H$ по теореме 2 из I2, т.е. $\mathcal{F}\circ\Psi=1$; во-вторых,

$$\Gamma\xrightarrow{\Psi}G_{\Gamma[\lambda]}\xrightarrow{\mathcal{F}}\Gamma'=\{\mu\in P[\lambda]\mid\forall f\in G_{\Gamma[\lambda]},\ f(\mu)=\mu\}=\Gamma$$

по теореме I из I2, т.е. $\Psi\circ\mathcal{F}=1$.

Итак, $\mathcal{F}$ и $\Psi$ обратны друг другу, т.е. являются биекциями. С их помощью устанавливаются связи Галуа: промежуточному расширению $\Gamma$ соответствует группа $G_{\Gamma[\lambda]}$, а подгруппе $H$ группы $G_{P[\lambda]}$ – промежуточное расширение $\Gamma$, состоящее из всех элементов $P[\lambda]$, остающихся на месте при каждом автоморфизме из $H$. В частности, всей группе $G_{P[\lambda]}$ соответствует поле $P$, т.е. $P$ состоит из всех элементов $P[\lambda]$, остающихся на месте при каждом автоморфизме из группы $G_{P[\lambda]}$.

ТЕОРЕМА I. Пусть $P[\lambda]$ – нормальное расширение $P$, $\varepsilon\in P[\lambda]$, $t(x)$ – минимальный полином для $\varepsilon$ относительно $P$, $\varepsilon'$ – сопряженное с $\varepsilon$ относительно $P$. Тогда

$$\exists f\in G_{P[\lambda]}:\ f(\varepsilon)=\varepsilon'$$

Доказательство: $\forall f\in G_{P[\lambda]}$

$f_1(\varepsilon)=\varepsilon_1$, $f_2(\varepsilon)=\varepsilon_2$, $\ldots$, $f_n(\varepsilon)=\varepsilon_n$

Составляем полином $F(x)=(x-\varepsilon_1)(x-\varepsilon_2)\cdot\ldots\cdot(x-\varepsilon_n)$. По лемме

2 из I2, где в качестве $H$ берется вся группа $G_{P[\alpha]}$, и только что сказанному о "структуре" поля $P$, $F(x)$ – полином над $P$. Он имеет $\varepsilon$ своим корнем (в $G_{P[\alpha]}$ есть тождественное преобразование $f_i$ ; $f_i(\varepsilon)=\varepsilon$ ; поэтому $\varepsilon$ есть среди $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$ и $F(\varepsilon)=0$ ), а тогда по теореме о минимальном полиноме $F(x)=t(x)p(x)$ . По условию $t(\varepsilon')=0 \Rightarrow$ $\Rightarrow F(\varepsilon')=0$ , все корни $F(x)$ – есть результаты воздействия автоморфизмов из $G_{P[\alpha]}$ на $\varepsilon$ , т.е.

$\exists f \in G_{P[\alpha]}$ : $f(\varepsilon)=\varepsilon'$

Теорема доказана.

Следствие. В нормальном расширении $P[\alpha]$ элементы $\varepsilon$ и $\varepsilon'$ сопряжены тогда и только тогда, когда $\exists f \in G_{P[\alpha]}: f(\varepsilon)=\varepsilon'$ (мы учли здесь предложение 2 из II).

ТЕОРЕМА 2. Пусть $P[\alpha]$ – нормальное расширение поля $P$, $\Gamma$ – промежуточное расширение $P$ . Для того, чтобы $\Gamma$ было нормальным расширением необходимо и достаточно, чтобы группа $G_{\Gamma[\alpha]}$ была нормальным делителем группы $G_{P[\alpha]}$.

Доказательство:

I. Необходимость.

Пусть $\Gamma$ – нормальное расширение $P$ . По замечанию 3 из 9 $\Gamma = P[\beta]$ . По критерию нормальности все $\beta' \in P[\beta]$ ( $\beta'$ – сопряженное с $\beta$ относительно $P$ ).

Нужно доказать, что $\forall x \in G_{\Gamma[\alpha]}, \forall y \in G_{P[\alpha]}, y^{-1}xy \in G_{\Gamma[\alpha]}$

Это и будет означать, что $G_{\Gamma[\alpha]}$ – нормальный делитель $G_{P[\alpha]}$ (по теореме 2 из I).

Возьмем $\beta \in \Gamma$ ; $y(\beta)=\beta' \in \Gamma$ (см. следствие из теоремы I). Тогда $y^{-1}xy(\beta) = y^{-1}x(\beta') = y^{-1}(\beta') = \beta$

(мы здесь использовали то, что $x \in G_{\Gamma[\alpha]}$ , $\beta' \in \Gamma \Rightarrow x(\beta')=\beta'$ )

Получается, что $y^{-1}xy$ оставляется на месте все $\Gamma$ (почему?), т.е. $y^{-1}xy \in G_{\Gamma[\alpha]}$

II. Достаточность.

Пусть теперь дано, что $G_{\Gamma[\alpha]}$ – нормальный делитель $G_{P[\alpha]}$ Докажем, что $\Gamma$ – нормальное расширение, используя критерий нормальности. Пусть $\Gamma = P[\beta]$ . По теореме I $\forall \beta'$ ( $\beta'$ – сопряженное с $\beta$ относительно $P$ ) $\exists y \in G_{P[\alpha]}$ $y(\beta)=\beta'$. $\forall x \in G_{\Gamma[\alpha]}$

$x(\beta') = xy(\beta) = yx'(\beta) = y(\beta) = \beta'$ ,где $x' \in G_{\Gamma[\alpha]}$ (мы использовали определение нормального



делителя), т.е. $\beta'$ остается на месте при действии всех автоморфизмов $x \in G_{\Gamma[\alpha]}$ , значит, по определению связей Галуа $\beta' \in \Gamma$ . Теорема доказана.

ТЕОРЕМА 3. Пусть $P[\alpha]$ – нормальное расширение поля $P$ . $\Gamma = P[\beta]$ – нормальное промежуточное расширение $P$ . Тогда $G_{P[\alpha]}/G_{\Gamma[\alpha]}$ изоморфна $G_{P[\beta]}$

Доказательство: Установим гомоморфизм $\varphi$ из $G_{P[\alpha]}$ в $G_{P[\beta]}$ Покажем, что $\operatorname{Im}\varphi = G_{P[\beta]}$ , $\operatorname{Ker}\varphi = G_{\Gamma[\alpha]}$ и, применив теорему 3 из I, получим требуемое. Пусть $f \in G_{P[\alpha]}$ , $f|_\Gamma$ сужение $f$ на $\Gamma$ (т.е. $f(\gamma)=f|_\Gamma(\gamma)$ , $\forall \gamma \in \Gamma$ ). Обозначим $f|_\Gamma \equiv \bar{f}$ . Зададим $\varphi$ так: $f \xrightarrow{\varphi} \bar{f}$

Выясним $\bar{f} \in G_{P[\beta]}$ ? $\bar{f}(\beta)=\beta' \in \Gamma$ по следствию из теоремы I, значит, $\bar{f}$ действует из $\Gamma$ в $\Gamma$ . Покажем, что $\varphi$ – гомоморфизм:

$$\forall \gamma \in \Gamma,\ \forall f_1, f_2 \in G_{P[\alpha]},\quad \big(\varphi(f_1 \circ f_2)\big)(\gamma) = \overline{f_1 \circ f_2}(\gamma) =$$

$$= (f_1 \circ f_2)(\gamma) = f_1(f_2(\gamma)) = f_1(\bar{f}_2(\gamma)) =$$

$$= \bar{f}_1(\bar{f}_2(\gamma)) = (\bar{f}_1 \circ \bar{f}_2)(\gamma) = \big(\varphi(f_1) \circ \varphi(f_2)\big)(\gamma).$$

Итак, $\varphi(f_1 \circ f_2) = \varphi(f_1) \circ \varphi(f_2)$

Докажем теперь, что $\operatorname{Ker}\varphi = G_{\Gamma[\alpha]}$ . Пусть

$f \in \operatorname{Ker}\varphi \Rightarrow \varphi(f) = \bar{f} = \bar{e}$ – тождественное на $\Gamma$ , значит, поскольку $f = \bar{f}$ на $\Gamma$ , то $f \in G_{\Gamma[\alpha]}$. Обратно: пусть $f \in G_{\Gamma[\alpha]}$ . Рассмотрим $f|_\Gamma = \bar{e}_\Gamma$ . Тогда $f|_\Gamma = \varphi(f) = \bar{e} \Rightarrow f \in \operatorname{Ker}\varphi$ . Осталось доказать, что $\operatorname{Im}\varphi = G_{P[\beta]}$ .

Известно, что $G_{P[\alpha]}/G_{\Gamma[\alpha]} \approx \operatorname{Im}\varphi$ (теорема 3 из I), значит, $\left| G_{P[\alpha]}/G_{\Gamma[\alpha]} \right| = |\operatorname{Im}\varphi|$ (так как есть биекция между этими множествами). Покажем, что $|\operatorname{Im}\varphi| = |G_{P[\beta]}|$

$$|\operatorname{Im}\varphi| = \left| G_{P[\alpha]}/G_{\Gamma[\alpha]} \right| \underset{\text{из 5}}{\overset{\text{лемма}}{=}} \frac{|G_{P[\alpha]}|}{|G_{\Gamma[\alpha]}|} \underset{\text{ние 2 из II}}{\overset{\text{замеча-}}{=}} \frac{\text{размерность } P[\alpha]}{\text{размерность } \Gamma[\alpha]} =$$

лемма I $|G_{P[\beta]}|$, таким образом, поскольку из I2 $Im\,\varphi \subset G_{P[\beta]}$ получаем, что $Im\,\varphi = G_{P[\beta]}$. Теорема доказана.

## I4. Разрешимые группы автоморфизмов

ТЕОРЕМА I. Пусть $P[\alpha]$ – нормальное расширение поля $P$, $\Gamma = P[\beta]$ – нормальное промежуточное расширение $P$. $G_{P[\alpha]}$ разрешима тогда и только тогда, когда разрешимы $G_{\Gamma[\alpha]}$ и $G_{P[\beta]}$.

Доказательство: По теореме 2 из I3 $G_{\Gamma[\alpha]}$ – нормальный делитель $G_{P[\alpha]}$, а по теореме 3 из I3 $G_{P[\alpha]}/G_{\Gamma[\alpha]} \approx G_{P[\beta]}$. Если $G_{P[\alpha]}$ разрешима, то применяем теорему I и следствие I к теореме 2 из 4. В обратную сторону нужно применить теорему 3 и то же самое следствие I из 4.

Теорема доказана.

Определение I. Комплексное число $\xi$ называется корнем $n$-ой степени из I, если $\xi^n = 1$ $(n \in N)$.

Определение 2. Число $\xi \in \mathbb{C}$ называется первообразным корнем -ой степени из I, если

I) $\xi$ – корень $n$-ой степени из I,

2) не существует $i<n$ $(i \in N)$: $\xi^i = 1$.

ПРИМЕР. Корни четвертой степени из I – это $1, -1, i, -i$. Выясним, какие из них являются первообразными.

$1^1 = 1 \Rightarrow 1$ – не первообразный корень,

$(-1)^1 = -1$

$(-1)^2 = 1$, $-1$ – не первообразный корень,

$i^1 = i$, $i^2 = -1$

$i^3 = -i$, $i^4 = 1$, $i$ – первообразный корень

Убедитесь, что $(-i)$ – тоже первообразный корень.

Предложение I. Корень $n$-ой степени из I является первообразным тогда и только тогда, когда $\forall k = \overline{0, n-1}$, $\xi^k$ – корень $n$-ой степени из I, причем все $\xi^k$ различны.

Доказательство: Пусть $\xi$ – первообразный корень $n$-ой степени из I. Тогда $(\xi^k)^n = (\xi^n)^k = 1^k = 1$, значит, $\xi^k$ – корень $n$-ой степени из $1$ $(k = 0, \dots, n-1)$. Если бы



$\xi^k = \xi^\ell$ $(\ell = 0, \dots, n-1)$, то $\xi^{k-\ell} = 1$, где $k-\ell<n$, а это противоречит 2) условию определения 2, значит, все $\xi^k$ различны. Обратно: допустим, что $\xi^k = 1$ $(k<n)$. По условию все $\xi^k$ различны, значит, наше предположение неверно ($\xi^0 = 1$, $\xi^k = 1$). Таким образом, условие 2) определения 2 выполняется. То, что $\xi$ – корень, следует из условия, поэтому $\xi$ – первообразный корень.

Определение 3. Число $z \in \mathbb{C}$ называется корнем $n$-ой степени из числа $a \in \mathbb{C}$, если $z^n = a$. Из курса алгебры известно, что из каждого комплексного $a \neq 0$ можно извлечь $n$ различных корней $n$-ой степени.

Предложение 2. Если $z_1, z_2, \dots, z_n$ – все корни $n$-ой степени из числа $a \in \mathbb{C}$, то $z_i\xi_0, z_i\xi_1, \dots, \xi_{n-1}z_i$ $(i = 1, \dots, n)$ – тоже все корни $n$-ой степени из $a$, где $\xi_0, \xi_1, \dots, \xi_{n-1}$ – все корни $n$-ой степени их I.

Доказательство: $\forall j = \overline{0, n-1}$, $(z_i\xi_j)^n = a$. Здесь все корни, так как их $n$ штук и все они различны (если бы $z_i\xi_\ell = z_i\xi_s$, то сократив на $z_i$, получили бы, что $\xi_\ell = \xi_s$, что невозможно, так как по условию $\xi_0, \xi_1, \dots, \xi_{n-1}$ различны (почему?) ).

Следствие. Из предложений I и 2 следует, что $z_i\varepsilon^0, z_i\varepsilon, \dots, z_i\varepsilon^{n-1}$ все корни $n$-ой степени из $a$, где $\varepsilon$ – первообразный корень $n$-ой степени из I, $z_i$ – один из корней $n$-ой степени из $a$.

ТЕОРЕМА 2. Пусть $P[\alpha]$ – нормальное расширение поля $P$, $P[\alpha] = P[z_1, z_2, \dots, z_n]$, где $z_1, z_2, \dots, z_n$ – все корни полинома $p(x) = x^n - a$ $(n \in N, a \in P)$.

Тогда группа $G_{P[\alpha]}$ разрешима.

Доказательство:

$$P[\alpha] = P[z_1, z_2, \dots, z_n] \underset{\text{следствие}}{=\!=\!=} P[z_1\varepsilon^0, z_1\varepsilon, \dots, z_1\varepsilon^{n-1}],$$

где $\varepsilon$ – первообразный корень $n$-ой степени из I. Тогда $P[\alpha] = P[z_1, \varepsilon]$ (очевидно). Обозначим $\Gamma = P[\varepsilon]$ и рассмотрим минимальный полином $f(x)$ для числа $\varepsilon$ относительно $P$. $\forall \varepsilon'$ ($\varepsilon'$ – сопряженное с $\varepsilon$ относительно $P$) $\varepsilon' = \varepsilon^k$ по предложению I, значит, $\varepsilon' \in \Gamma$, а тогда по критерию нормальности (I0) $\Gamma$ – нормальное расширение $P$.

Возможны три случая:
I) $P \subsetneq \Gamma \subsetneq P[\alpha]$
2) $\Gamma = P[\alpha]$
3) $\Gamma = P$

В первом случае $\Gamma$ – промежуточное расширение $P$ (оно также нормальное по доказанному). По теореме I для разрешимости $G_{P[\alpha]}$ нужно доказать разрешимость $G_{\Gamma[\alpha]}$ и $G_{P[\varepsilon]}$. Во втором случае $\Gamma = P[\varepsilon] = P[\alpha]$, и поэтому вопрос о разрешимости $G_{P[\alpha]}$ сводится к разрешимости $G_{P[\varepsilon]}$.

Итак, докажем, что $G_{P[\varepsilon]}$ и $G_{\Gamma[\alpha]}$ – разрешимые группы. Для этого достаточно показать, что они абелевы (см. пример I из 3).

а) $\forall x, y \in G_{P[\varepsilon]}$

$$x \circ y(\varepsilon) = x(y(\varepsilon)) = x(\varepsilon^k) = (\varepsilon^k)^\ell = \varepsilon^{k\ell}$$

$$y \circ x(\varepsilon) = y(x(\varepsilon)) = y(\varepsilon^\ell) = (y(\varepsilon))^\ell = \varepsilon^{k\ell}$$

Итак, $x \circ y = y \circ x$ на всем $P[\varepsilon]$ (см. замечание I из II).

б) заметим, что

$$\Gamma[\alpha] = P[\alpha] = P[z_1, \varepsilon] = \Gamma[z_1], \text{ поэтому } z_1 \in \Gamma[\alpha]$$

(мы использовали I свойство промежуточного расширения и то, что $\Gamma = P[\varepsilon]$).

$\forall f, g \in G_{\Gamma[\alpha]}$

$$f \circ g(z_1) = f(g(z_1)) = f(z_1 \varepsilon^k) = f(z_1) \cdot f(\varepsilon^k) =$$

$$= f(z_1) \cdot \varepsilon^k = z_1 \cdot \varepsilon^\ell \cdot \varepsilon^k = z_1 \varepsilon^{\ell+k}$$

$$g \circ f(z_1) = g(f(z_1)) = g(z_1 \varepsilon^\ell) = g(z_1) g(\varepsilon^\ell) = z_1 \varepsilon^k \varepsilon^\ell = z_1 \varepsilon^{k+\ell}$$

Итак, и здесь $f \circ g = g \circ f$ на всем $\Gamma[z_1] = \Gamma[\alpha]$.

В процессе доказательства мы опирались на определение автоморфизма ( $\varepsilon^k \in \Gamma, \varepsilon^\ell \in \Gamma$ ) и следствие из теоремы I из I3.

Осталось рассмотреть третий случай: $\Gamma = P[\varepsilon] = P$. Тогда $\varepsilon \in P$, следовательно $P[\alpha] = P[z_1, \varepsilon] = P[z_1]$

$\forall u, v \in G_{P[\alpha]}$, $u \circ v(z_1) = u(v(z_1)) = u(z_1 \varepsilon^k) =$

$= \varepsilon^k u(z_1) = \varepsilon^k \cdot z_1 \cdot \varepsilon^\ell = z_1 \cdot \varepsilon^{k+\ell}$; $v \circ u(z_1) = v(u(z_1)) =$

$= v(\varepsilon^\ell z_1) = \varepsilon^\ell v(z_1) = \varepsilon^\ell \cdot z_1 \cdot \varepsilon^k = z_1 \cdot \varepsilon^{\ell+k}$



(мы использовали то, что $\varepsilon^\ell \in P, \varepsilon^k \in P$ ).

Итак, $u \circ v = v \circ u$ на всем $P[z_1] = P[\alpha]$, значит, $G_{P[\alpha]}$ – абелева группа, а следовательно, разрешима (пример I из 3). Теорема доказана.

## Ш. ГРУППЫ ГАЛУА АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ. РАЗРЕШИМОСТЬ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ В РАДИКАЛАХ

### I5. Выражение в радикалах

Определение. Пусть $M$ – некоторое числовое множество, $\alpha$ – некоторое число. Будем говорить, что $\alpha$ выражается в радикалах через $M$, если существуют такие числа $\alpha_0, \alpha_1, \dots, \alpha_n$, что $\alpha_0 \in M$, $\alpha_n = \alpha$ и $\forall i \in N, i \le n$ $\exists \alpha_j, \alpha_k$ $(j, k \in N; j, k < i)$: $(\ell \in N)$, $\alpha_i = \sqrt[\ell]{\alpha_j}$, или $\alpha_i = \alpha_j * \alpha_k$, или $\alpha_i \in M$ ( $*$ – одно из действий "+", "–", " ", ":").

Примечание. Выражение " $\alpha$ выражается в радикалах через $M$ " означает фактически, что $\alpha$ выражается через элементы $M$ с помощью четырех арифметических действий и извлечения корня.

ПРИМЕР. Пусть $M = \{2, 3\}$, $\alpha = \frac{1}{\sqrt[5]{\sqrt{5}-2}}$.

Число $\alpha$ выражается в радикалах через $M$ : "разрешающей цепочкой" для него будет:

$\alpha_0 = 2 \in M$, $\alpha_1 = 3 \in M$, $\alpha_2 = 3-2 = 1$, $\alpha_3 = 3+2 = 5$, $\alpha_4 = \sqrt{5}$, $\alpha_5 = \sqrt[5]{\sqrt{5}-2}$, $\alpha_6 = \frac{1}{\sqrt[5]{\sqrt{5}-2}} = \alpha$

Лемма. Пусть $P$ – числовое поле, $\alpha$ алгебраично относительно $P$. Тогда $\forall n \in N$ $\sqrt[n]{\alpha}$ алгебраичен относительно $P$.

Доказательство:

I) Пусть $\alpha \in P$. Полином $x^n - \alpha$ – полином над $P$. Он имеет своим корнем $\sqrt[n]{\alpha}$ $\Rightarrow$ $\sqrt[n]{\alpha}$ алгебраичен относительно $P$.

2) Пусть $\alpha \notin P$. Так как $\alpha$ алгебраично относительно $P$, то существует полином $\varphi(x) = a_0 x^k + \dots + a_k$, $\varphi(\alpha) = 0$, $(a_i \in P)$.

Рассмотрим полином $f(x) = a_0 x^{nk} + \dots + a_k x^n + a_k$. Это полином над полем $P$ и $f(\sqrt[n]{\alpha}) = \varphi(\alpha) = 0 \Rightarrow \sqrt[n]{\alpha}$ алгебраичен относительно $P$.

Предложение. Пусть $P$ – некоторое числовое поле, $\alpha$ выражается в радикалах через $P$. Тогда $\alpha$ алгебраично относительно $P$.

Доказательство (индукцией по длине цепочки $\alpha_0, \alpha_1, \ldots, \alpha_n$);

а) Если цепочка состоит только из $\alpha_0 \in P$, то $\alpha_0 = \alpha$ алгебраично относительно $P$ ( $x - \alpha_0$ - полином над $P$, имеющий $\alpha_0$ своим корнем).

б) Пусть все $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ алгебраичны относительно $P$. Докажем, что $\alpha_n = \alpha$ также алгебраично. Если $\alpha_n \in P$, то все доказано. Если $\alpha_n = \sqrt[k]{\alpha_i}$ $(i, k \in N, i < n)$, то $\alpha_n$ алгебраично по лемме. Если же $\alpha_n = \alpha_i * \alpha_j$ $(i, j \in N; i, j < n)$, то $\alpha_n$ алгебраично по предложению 2 из 9.

<u>Свойства</u>.

1° $\forall \alpha \in M$, $\alpha$ выражается в радикалах через $M$.
Действительно, здесь в качестве цепочки можно взять само $\alpha$.

2° Пусть $\alpha$ выражается в радикалах через $M$, т.е. есть "разрешающая" цепочка для $\alpha$ относительно $M$:
$\alpha_0 \in M, \alpha_1, \ldots, \alpha_n = \alpha$ ( $\alpha_i \in M$, или $\alpha_i = \alpha_j * \alpha_k$, или $\alpha_i = \sqrt[k]{\alpha_j}$ ).
Тогда $\alpha_{n-1}, \alpha_{n-2}, \ldots, \alpha_0$ выражаются в радикалах через $M$.
В самом деле, $\alpha_0 \in M \Rightarrow \alpha_0$ выражается в радикалах через $M$, для $\alpha_1$ цепочка будет $\alpha_0 \in M, \alpha_1$, для $\alpha_2$ - $\alpha_0 \in M, \alpha_1, \alpha_2$ и т.д. (т.е. берем частичные цепочки большой цепочки $\alpha_0, \alpha_1, \ldots, \alpha_n$ ).

3° (транзитивность). Пусть $\alpha$ выражается в радикалах через $M$, $\forall \gamma \in M$, $\gamma$ выражается в радикалах через $N$. Тогда $\alpha$ выражается в радикалах через $N$.

Доказательство: $\alpha$ выражается в радикалах через $M$, следовательно, существует цепочка $\alpha_0 \in M, \alpha_1, \ldots, \alpha_n = \alpha$. $\alpha_0 \equiv \gamma_1$ выражается в радикалах через $N$, значит, существует цепочка $a_0 \in N, a_1, \ldots, a_m = \alpha_0$. $\gamma_2$ выражается в радикалах через $N$, значит, существует цепочка $b_0 \in N, b_1, \ldots, b_s = \gamma_2$ . . . . . $\gamma_k$ выражается в радикалах через $N$, значит существует цепочка $c_0 \in N, c_1, \ldots, c_t = \gamma_k$.

Пусть $\alpha_i \in M$, $\alpha_i \equiv \gamma_2; \ldots; \alpha_j \in M$, $\alpha_j \equiv \gamma_k$.
Разрешающей для $\alpha$ относительно $N$ будет тогда цепочка
$a_0 \in N, a_1, \ldots, a_m = \alpha_0 \equiv \gamma_1, \alpha_1, \ldots, \alpha_{i-1}, b_0, b_1, \ldots, b_s =$



$= \gamma_2 = \alpha_i, \alpha_{i+1}, \ldots, c_0 \in N; c_1, \ldots, c_t = \gamma_k =$
$= \alpha_j, \ldots, \alpha_n = \alpha$.

4° Сумма, разность, произведение, частное и корень любой степени из чисел, выражающихся в радикалах через $M$, сами выражаются в радикалах через $M$.

Доказательство: Пусть $\alpha_0$ выражается в радикалах через $M_1 \Rightarrow \exists a_0 \in M, a_1, \ldots, a_n = \alpha_0$, $\alpha_1$ выражается в радикалах через $M_1 \Rightarrow \exists b_0 \in M, b_1, \ldots, b_m = \alpha_1$. Построим цепочку $a_0 \in M, a_1, \ldots, a_n = \alpha_0, b_0 \in M, b_1, \ldots, b_m = \alpha_1, \alpha_0 + \alpha_1$

Ясно, что она нас устраивает, т.е. $\alpha_0 + \alpha_1$ выражается в радикалах через $M$.

Аналогично для других действий (сделать самим). Для корня: строим цепочку $a_0 \in M, a_1, \ldots, a_n = \alpha_0, \sqrt[k]{\alpha_0} (k \in N)$. Эта цепочка - разрешающая, т.е. $\sqrt[k]{\alpha_0}$ выражается в радикалах через $M$.

ТЕОРЕМА. Если $P$ - числовое поле и $\alpha$ выражается в радикалах через $P$; $\alpha^*$ - число, сопряженное с $\alpha$ относительно $P$, то $\alpha^*$ выражается в радикалах через $P$.

Доказательство: Так как $\alpha$ выражается в радикалах через $P$, то для $\alpha$ есть "разрешающая" цепочка $\alpha_0 \in P, \alpha_1, \ldots, \alpha_n = \alpha$.
По предложению и свойству 2° все члены цепочки выражаются в радикалах через $P$, а потому алгебраичны относительно $P$, т.е.

$\forall \alpha_i \; (i = 0 \div n) \; \exists p_i(x)$ ( $p_i(x)$ полином над $P$): $p_i(\alpha_i) = 0$

Рассмотрим полином $f(x) = p_1(x) p_2(x) \ldots p_n(x)$. Пусть $\beta_1, \ldots, \beta_t$ - его корни. $P[\beta_1, \ldots, \beta_t] = P[\delta]$ - нормальное расширение (по определению). По следствию из теоремы I из I3 $\exists \varphi \in G_{P[\delta]}$ : $\varphi(\alpha) = \alpha^*$, тогда "разрешающей" цепочкой для $\alpha^*$ относительно $P$ будет $\delta_0 = \varphi(\alpha_0), \ldots, \delta_n = \varphi(\alpha_n)$. (проверьте, что эта цепочка удовлетворяет необходимым требованиям, используя определение автоморфизма). Теорема доказана.

<u>I6. Теорема о циклической группе автоморфизмов</u>

Пусть $P_1 = P[\alpha]$ - нормальное расширение поля $P$, $G_{P[\alpha]} = \{a, a^2, \ldots, a^n = e\}$ (циклическая группа). Тогда любой элемент, принадлежащий $P_1$ выражается в радикалах через $P$

Доказательство: Рассмотрим расширение $\Gamma = P[\varepsilon]$, где $\varepsilon$ – первообразный корень $n$ -ой степени из I, а также расширение $P_2 = P[\alpha,\varepsilon] = \Gamma[\varepsilon] = P_1[\varepsilon]$. Ясно, что $P\subset P_1, \Gamma\subset P_2, P_1\subset P_2$. Возьмем $G_{\Gamma[\alpha]}$ – подгруппу $G_{P[\alpha,\varepsilon]}$ (автоморфизмы, тождественные на $\Gamma$, тождественны и на $P$, так как $P\subset\Gamma$). Пусть $y\in G_{\Gamma[\alpha]}$, $y(\alpha)$ – сопряженный с $\alpha$ относительно $\Gamma$ (по предложению 2 из II). Подействуем всеми автоморфизмами из $G_{P[\alpha]}$ на $\alpha$:

$$a(\alpha), a^2(\alpha), \ldots, a^n(\alpha) \qquad , \quad a^i(\alpha)\neq a^j(\alpha),\ i\neq j$$

(иначе по замечанию I из II $a^i = a^j$, что не так).

Все числа $a(\alpha), a^2(\alpha), \ldots, a^n(\alpha)$ – сопряженные с $\alpha$ относительно $P$. Поскольку корни минимального полинома для $\alpha$ относительно $\Gamma$ являются корнями минимального полинома для $\alpha$ относительно $P$ (почему?), а числа $a(\alpha), a^2(\alpha), \ldots, a^n(\alpha)$ исчерпывают все корни минимального полинома для $\alpha$ относительно $P$ (объясните), то $y(\alpha) = a^k(\alpha)$ (1)

Рассмотрим

$$u_p = \alpha + \varepsilon^p a(\alpha) + \varepsilon^{2p} a^2(\alpha) + \varepsilon^{3p} a^3(\alpha) + \ldots + \varepsilon^{(n-1)p} a^{n-1}(\alpha)$$
$$0\le p<n$$

Тогда $\forall y\in G_{\Gamma[\alpha]}$

$$y(u_p) = y(\alpha) + \varepsilon^p y(a(\alpha)) + \varepsilon^{2p} y(a^2(\alpha)) + \ldots + \varepsilon^{(n-1)p} y(a^{n-1}(\alpha))$$

Так как $y(\alpha) = a^k(\alpha)$ (по равенству (I)), то

$\forall \gamma\in P[\alpha]$ $\quad y(\gamma) = a^k(\gamma)$ (учитывая замечание I из II).

Имеем:

$$y(u_p) = a^k(\alpha) + \varepsilon^p a^{k+1}(\alpha) + \ldots + \varepsilon^{(n-1)p} a^{k+n-1}(\alpha) =$$

$$= \frac{1}{\varepsilon^{kp}}\left(\varepsilon^{kp} a^k(\alpha) + \varepsilon^{(k+1)p} a^{k+1}(\alpha) + \ldots + \varepsilon^{(k+n-1)p} a^{k+n-1}(\alpha)\right) =$$

$$= \frac{1}{\varepsilon^{kp}} \sum_{j=0}^{n-1} \varepsilon^{(k+j)p} a^{k+j}(\alpha) = \frac{1}{\varepsilon^{kp}} \sum_{s_j=0}^{n-1} \varepsilon^{s_j p} a^{s_j}(\alpha) = \frac{1}{\varepsilon^{kp}} u_p \quad (2)$$



( $k+j = nq + s_j$, $0\le s_j<n$ – мы использовали также то, что $G_{P[\alpha]}$ – циклическая).

А тогда $\quad y(u_p^n) = (y(u_p))^n \underset{(2)}{=} u_p^n \quad$ (так как $\varepsilon^n = 1$ )

Итак, $\quad y(u_p^n) = u_p^n$, значит, по связям Галуа $u_p^n\in\Gamma$.

Пусть $\xi_i$ – корень $n$ -ой степени из I. По предложению I из I4

$$\xi_i = \varepsilon^i$$

$$\xi_i^n - 1 = (\xi_i - 1)(\xi_i^{n-1} + \xi_i^{n-2} + \ldots + 1) = 0 \ (\text{ибо } \xi_i^n = 1) \Rightarrow \text{(почему?)}$$
$$\Rightarrow \xi_i^{n-1} + \xi_i^{n-2} + \ldots + \xi_i + \xi_i^0 = 0 \qquad (3)$$

Выпишем все $u_p$ и сложим их:

$$u_0 = \alpha + \varepsilon^0 a(\alpha) + \varepsilon^0 a^2(\alpha) + \ldots + \varepsilon^0 a^{n-1}(\alpha)$$
$$u_1 = \alpha + \varepsilon^1 a(\alpha) + \varepsilon^2 a^2(\alpha) + \ldots + \varepsilon^{n-1} a^{n-1}(\alpha)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$u_{n-1} = \alpha + \varepsilon^{n-1} a(\alpha) + \varepsilon^{2(n-1)} a^2(\alpha) + \ldots + \varepsilon^{(n-1)^2} a(\alpha)$$

$$u_0 + u_1 + \ldots + u_{n-1} \underset{(3)}{=} n\alpha \quad \text{, откуда}$$

$$\alpha = \frac{u_0 + u_1 + \ldots + u_{n-1}}{n} \Longrightarrow \alpha \text{ выражается в радикалах через}$$

$u_0, u_1, \ldots, u_{n-1}, P$

$u_p^n\in\Gamma \Rightarrow u_p = \sqrt[n]{\gamma_p}$,

где $\gamma_p\in\Gamma$ значит, $u_0, u_1, \ldots, u_{n-1}$ выражаются в радикалах через $\Gamma = P[\varepsilon]$, следовательно, по 3° свойству из I5 $\alpha$ выражается в радикалах через $\Gamma$. $\varepsilon = \sqrt[n]{1}$ – выражается в радикалах через $P$, а тогда $\forall\beta\in\Gamma = P[\varepsilon]$, $\beta$ выражается в радикалах через $P$, что по транзитивности приводит к выражению в радикалах $\alpha$, а значит, и всего $P[\alpha]$ через $P$. Теорема доказана.

## I7. Критерий разрешимости группы автоморфизмов

ТЕОРЕМА. Пусть $P_1 = P[\alpha]$ – нормальное расширение поля $P$. Для того чтобы все элементы из $P_1$ выражались в радикалах через $P$ необходимо и достаточно чтобы группа автоморфизмов $G_{P[\alpha]}$ была разрешимой.

Доказательство:

I. <u>Необходимость</u>. Пусть дано нормальное расширение $P_1 = P[\alpha]$, все элементы которого выражаются в радикалах через $P$. Докажем, что $G_{P[\alpha]}$ – разрешимая группа автоморфизмов. $\alpha \in P[\alpha]$, значит, $\alpha$ выражается в радикалах через $P$, т.е. существует "разрешающая цепочка"

$$\alpha_0 \in P, \alpha_1, \dots, \alpha_n = \alpha \; : \; \alpha_i = \sqrt[t]{\alpha_j}, \text{ или } \alpha_i = \alpha_j * \alpha_k$$

или $\alpha_i \in P$.

Доказательство будем проводить методом математической индукции по числу $m$ членов цепочки, не лежащих в $P$.

а) база индукции: $m=0$, т.е. все члены цепочки лежат в $P$, тогда $\alpha \in P \Rightarrow P[\alpha] = P$ (см. 9), значит, степень минимального полинома для $\alpha$ относительно $P$ равна I, следовательно, по теореме I (II) $G_{P[\alpha]} = \{e\}$, а такая группа разрешима.

б) пусть для $\ell < m \; (\ell \in N)$ утверждение теоремы доказано. Докажем для $\ell = m$.

Допустим, что $\alpha_s \notin P$, а $\alpha_0, \alpha_1, \dots, \alpha_{s-1} \in P$.

$\alpha_s = \sqrt[t]{\alpha_i} \; (i<s)$ ($\alpha_s \neq \alpha_i * \alpha_j$, так как $P$ – поле если бы $\alpha_s = \alpha_i * \alpha_j$, то $\alpha_s \in P$).

Рассмотрим полином $H(x) = x^t - \alpha_i$, корнем которого является $\alpha_s$. Пусть $T = \{\beta_1, \beta_2, \dots, \beta_t\}$ – все корни $H(x)$.

Построим $\Gamma = P[\beta_1, \dots, \beta_t]$. $\Gamma$ – нормальное расширение $P$ (по определению). По теореме 2 из I4 $G_{P[\beta_1, \dots, \beta_t]}$ – разрешимая группа.

Теперь построим расширение $P_2 = \Gamma[\alpha] = P[\beta_1, \dots, \beta_t, \alpha] = P_1[\beta_1, \dots, \beta_t]$. Ясно, что $P \subset P_1 = P[\alpha] \subset P_2$,

$P \subset \Gamma \subset P_2$. Докажем, что, во-первых, $P_2$ – нормальное расширение $\Gamma$ и, во-вторых, $P_2$ – нормальное расширение $P$.

I) Так как $P_1$ – нормальное расширение $P$, то по критерию нормальности все $\alpha_i$, сопряженные с $\alpha$ относительно $P$, принадлежат $P_1$, а значит, и $P_2$.

Пусть $p(x)$, $q(x)$ – минимальные полиномы для числа $\alpha$ относительно $P$ и $\Gamma$ соответственно. В этом случае $p(x) = q(x) s(x)$ (объясните), все корни $p(x)$ лежат в $P_2$ (смотри выше), а значит, все корни $q(x)$, являющиеся корнями $p(x)$, тоже лежат в $P_2$. Применяя все тот же критерий нормальности, получаем, что $P_2$ – нормальное расширение $\Gamma$.

2) $\forall \gamma \in P_2 \quad \gamma = F(\alpha, \beta_1, \dots, \beta_t) =$ ($F$ – полином над $P$)

$$= F(\gamma_1, \dots, \gamma_m, \beta_1, \dots, \beta_t) \Rightarrow \gamma \in P[\gamma_1, \dots, \gamma_m, \beta_1, \dots, \beta_t]$$

($\gamma_1, \dots, \gamma_m$ – все корни полинома $p(x)$, минимального для $\alpha$ относительно $P$; среди них есть и само $\alpha$).

Обратно:

$$\forall \gamma \in P[\gamma_1, \dots, \gamma_m, \beta_1, \dots, \beta_t] \Rightarrow \gamma = \Phi(\gamma_1, \dots, \gamma_m, \beta_1, \dots, \beta_t)$$

($\Phi$ – полином над $P$)

$\gamma_1, \dots, \gamma_m \in P_1 \subset P_2; \beta_1, \dots, \beta_t \in \Gamma \subset P_2$, следовательно, $\gamma \in P_2$.

Таким образом, $P_2 = P[\gamma_1, \dots, \gamma_m, \beta_1, \dots, \beta_t]$, значит, $P_2$ – нормальное расширение $P$ (по определению). $\alpha$ выражается в радикалах через $P$, $P \subset \Gamma$, следовательно, $\alpha$ выражается в радикалах через $\Gamma$. Количество элементов цепочки, не лежащих в $\Gamma$, меньше, чем на лежащих в $P$. Действительно, $\alpha_s \in \Gamma$ по построению $\Gamma$, но $\alpha_s \notin P$. Тогда по индукционному предположению $G_{\Gamma[\alpha]}$ разрешима.

$\Gamma$ – нормальное промежуточное расширение $P$. По теоремам 2 и 3 из I3.

$$G_{P[\beta_1, \dots, \beta_t, \alpha]} / G_{\Gamma[\alpha]} \approx G_{P[\beta_1, \dots, \beta_t]}$$

$G_{\Gamma[\alpha]}$ разрешима по доказанному, $G_{P[\beta_1, \dots, \beta_t]}$ разрешима (см. выше), а тогда по теореме 3 из 4 $G_{P[\alpha, \beta_1, \dots, \beta_t]}$ разрешима.

$P_1$ – нормальное промежуточное расширение $P$. По теоремам 2 и 3 из I3

$$G_{P[\alpha, \beta_1, \dots, \beta_t]} / G_{P_1[\beta_1, \dots, \beta_t]} \approx G_{P[\alpha]}$$

Мы показали, что $G_{P[\alpha,\beta_1,\ldots,\beta_{t-1}]}$ разрешима. Тогда по следствию 2 из теоремы 2 из 4) $G_{P[\alpha]}$ разрешимая группа.

II. Достаточность. Пусть теперь группа автоморфизмов $G_{P[\alpha]}$ нормального расширения $P[\alpha]$ разрешима. Докажем, что все элементы из $P[\alpha]$ выражаются в радикалах через $P$.

Если $G_{P[\alpha]}$ – циклическая группа, то по теореме из I6 получаем требуемое. Пусть $G_{P[\alpha]}$ – не циклическая группа. Докажем, что у нее тогда существует собственный нормальный делитель $N$ ( $N\neq e$ , $N\neq G_{P[\alpha]}$ ). Доказываем от противного. Возьмем коммутант $G_{P[\alpha]}$. По теореме I из 2 он является нормальным делителем $G_{P[\alpha]}$. По нашему предположению $K=e$ или $K=G_{P[\alpha]}$. Если $K=G_{P[\alpha]}$, то мы никогда в ряду коммутантов не получим $e$, а это противоречит разрешимости $G_{P[\alpha]}$. Если же $K=e$, то группа $G_{P[\alpha]}$ – абелева (по свойству коммутанта – 2), у абелевой группы любая подгруппа – нормальный делитель. По нашему предположению получается, что у нее нет собственных подгрупп, а тогда $G_{P[\alpha]}$ – циклическая (почему?). Получили противоречие.

Итак, доказано, что в этом случае у $G_{P[\alpha]}$ есть собственный нормальный делитель.

Дальше доказываем методом математической индукции относительно количества элементов в $G_{P[\alpha]}$.

а) база индукции: $|G_{P[\alpha]}|=1$, тогда $\alpha\in P$ (так как размерность расширения тоже равна единице) и $\alpha$ выражается в радикалах через $P$, а тогда $\forall\gamma\in P[\alpha]$ выражается в радикалах через $P$ (объяснить самим).

б) пусть утверждение справедливо для всех $k<n$ ($k\in N$). Докажем его для $k=n$.

Рассмотрим собственный нормальный делитель $N$ группы $G_{P[\alpha]}$ (он существует по доказанному). По связям Галуа найдется промежуточное расширение $\Gamma$ : $P\subset\Gamma\subset P[\alpha]$ : $G_{\Gamma[\alpha]}=N$. По теореме 2 из I3 $\Gamma$ – нормальное расширение поля $P$. По теореме 3 из I3.

$G_{P[\alpha]}/G_{\Gamma[\alpha]}\approx G_\Gamma$, что означает разрешимость $G_{\Gamma[\alpha]}$ и $G_\Gamma$ по теореме I и следствию 2 (4).



Если $\dim_P P[\alpha]=n$, $\dim_\Gamma P[\alpha]=\ell$, $\dim_P\Gamma=s$, то по лемме I из I2 $n=\ell s$, $\ell<n$, $s<n$ ($\ell\neq 1$ и $\ell\neq n$ так как $N=G_{\Gamma[\alpha]}$ – собственная подгруппа $G_{P[\alpha]}$ ). Применяем индуктивное предположение. По нему $\forall\gamma\in P[\alpha]$, $\gamma$ выражается в радикалах через $\Gamma$ $\forall\delta\in\Gamma$, $\delta$ выражается в радикалах через $P$, тогда по транзитивности $\forall\gamma\in P[\alpha]$, $\gamma$ выражается в радикалах через $P$. Теорема доказана.

## I8. Группы Галуа алгебраических уравнений

Определение I. Пусть имеется алгебраическое уравнение $a_0x^n+a_1x^{n-1}+\ldots+a_n=0$, где $a_i\in P$ ($i=0\div n$); $\alpha_1,\ldots,\alpha_n$ – корни этого уравнения.
Группа автоморфизмов $G_{P[\alpha_1,\ldots,\alpha_n]}$ расширения $P[\alpha_1,\ldots,\alpha_n]$ называется группой Галуа данного уравнения.

Заметим, что $P[\alpha_1,\ldots,\alpha_n]$ – нормальное расширение поля $P$.

Лемма. Пусть $p$ – простое число и дано уравнение $x^p+a_1x^{p-1}+\ldots+a_p=0$ с корнями $\alpha_1,\ldots,\alpha_p$, $f(x)\equiv x^p+a_1x^{p-1}+\ldots+a_p$ – полином над полем $Q$, неприводимый и имеющий ровно два невещественных корня. Тогда $G_{Q[\alpha_1,\ldots,\alpha_p]}\approx S_p$ ( $S_p$ – группа подстановок множества $\{\alpha_1,\ldots,\alpha_p\}$ )

ДОКАЗАТЕЛЬСТВО: Рассмотрим автоморфизм $f\in G_{Q[\alpha_1,\ldots,\alpha_p]}$. Пусть $T=\{\alpha_1,\ldots,\alpha_p\}$, $f(\alpha_i)=\alpha_j$ (по предложению 2 из II). Установим соответствие $\Psi: G_{Q[\alpha_1,\ldots,\alpha_p]}\to S_p$ следующим образом $f\longrightarrow\Psi(f)$, где $(\Psi(f))(\alpha_i)=f(\alpha_i)$, $\Psi(f)\in S_p$ так как $\Psi(f)$ – инъекция на конечном множестве $T$, т.е. биекция и $\Psi(f)$ действует из $T$ в $T$. Покажем, что $\Psi$ – изоморфизм:

I) пусть $\Psi(f_1)=\Psi(f_2)\Rightarrow\forall\alpha_i\in T$ $f_1=f_2\Rightarrow f_1=f_2$ на всем $Q[\alpha_1,\ldots,\alpha_p]$ (см. замечание I из II), значит, $\Psi$ – инъекция.

2) то, что $\Psi$ – функция и отображение, очевидно (показать самим).

3) $\Psi$ – гомоморфизм:

$$(\Psi(\xi_1\circ\xi_2))(\alpha_i) = (\xi_1\circ\xi_2)(\alpha_i) = \xi_1(\xi_2(\alpha_i)) \quad (*)$$

$$(\Psi(\xi_1)\circ\Psi(\xi_2))(\alpha_i) = \Psi(\xi_1)(\Psi(\xi_2)(\alpha_i)) =$$

$$= \Psi(\xi_1)(\underbrace{\xi_2(\alpha_i)}_{\in T}) = \xi_1(\xi_2(\alpha_i)) \quad (**)$$

$$(*) = (**)$$

Изоморфизм - биективное отображение, являющееся гомоморфизмом.

4) покажем, что $\Psi$ - сюръекция.

$\Psi(G_{Q[\alpha_1,\dots,\alpha_p]})$ - подгруппа $S_p$ по предложению 3 из I. Таким образом, $\Psi(G_{Q[\alpha_1,\dots,\alpha_p]})$ - группа преобразований множества $T$. Покажем, что она транзитивна: Возьмем произвольные $\alpha_i, \alpha_j \in T$. По теореме I из I3

$$\exists t' \in G_{Q[\alpha_1,\dots,\alpha_p]} : t'(\alpha_i) = \alpha_j$$

$$\Psi(t') = t \Rightarrow t(\alpha_i) = \Psi(t')(\alpha_i) = t'(\alpha_i) = \alpha_j, \text{ т.е.}$$

$\exists t \in \Psi(G_{Q[\alpha_1,\dots,\alpha_p]}) : t(\alpha_i) = \alpha_j$, что и означает транзитивность $\Psi(G_{Q[\alpha_1,\dots,\alpha_p]})$.

По следствию из 7 $\Psi(G_{Q[\alpha_1,\dots,\alpha_p]})$ примитивна.

Докажем, что $\Psi(G_{Q[\alpha_1,\dots,\alpha_p]})$ содержит транспозицию, т.е. цикл $(i\,j) = \begin{pmatrix} \dots i \dots j \dots \\ \dots j \dots i \dots \end{pmatrix}$.

Рассмотрим для этого отображение $\tilde{\xi} : \alpha \in \mathbb{C} \to \bar{\alpha} \in \mathbb{C}, \forall \gamma \in \mathbb{C}$

$$\tilde{\xi}\circ\tilde{\xi}(\gamma) = \tilde{\xi}(\tilde{\xi}(\gamma)) = \bar{\bar{\gamma}} = \gamma \Rightarrow \tilde{\xi}\circ\tilde{\xi} = e \Rightarrow \tilde{\xi} = \tilde{\xi}^{-1}$$

т.е. $\tilde{\xi}$ обратимо, а значит является биекцией.

$\tilde{\xi}$ переводит сумму в сумму, произведение в произведение, так как сопряженное суммы равно сумме сопряженных, сопряженное произведения равно произведению сопряженных. Таким образом, $\tilde{\xi}$ - автоморфизм множества $\mathbb{C}$. Пусть $\tilde{\xi}_0$ - сужение $\tilde{\xi}$ на $Q[\alpha_1,\dots,\alpha_p]$. $\tilde{\xi}_0$ - инъекция (так как $\tilde{\xi}$ - инъекция), сумму переводит в сумму, произведение - в произведение и

$$\forall q \in Q \quad \tilde{\xi}_0(q) = \bar{q} = q$$

Покажем теперь, что $\tilde{\xi}_0(Q[\alpha_1,\dots,\alpha_p]) = Q[\alpha_1,\dots,\alpha_p]$, т.е. что $\tilde{\xi}_0$ - сюръективное преобразование.



а) пусть $\delta \in Q[\alpha_1,\dots,\alpha_p] \Rightarrow \delta = \varphi(\alpha_1,\dots,\alpha_p)$ ($\varphi$ - полином над $Q$). Все $\alpha_i$, кроме $\alpha_1\alpha_2$ остаются неизменными при действии $\tilde{\xi}_0$ (они вещественные, а $\alpha_1$ и $\alpha_2$ переходят друг в друга (так как они сопряжены), поэтому $\tilde{\xi}_0(\delta)$ - тоже значение полинома от $\alpha_1,\dots,\alpha_p$ т.е. $\tilde{\xi}_0(\delta) \in Q[\alpha_1,\dots,\alpha_p]$

б) $\forall \varepsilon = F(\alpha_1,\alpha_2,\dots,\alpha_p)$ ( $F$ -полином над $P$ )

$\exists \delta = F(\alpha_2,\alpha_1,\dots,\alpha_p) : \tilde{\xi}_0(\delta) = \varepsilon$ (сопряженные переходят друг в друга).

Итак, $\tilde{\xi}_0$ - автоморфизм $Q[\alpha_1,\dots,\alpha_p]$, т.е. $\tilde{\xi}_0 \in G_{Q[\alpha_1,\dots,\alpha_p]}$. Тогда $\Psi(\tilde{\xi}_0)(\alpha_i) = \tilde{\xi}_0(\alpha_i)$

$$\Psi(\tilde{\xi}_0) = \begin{pmatrix} \alpha_1\alpha_2\alpha_3\dots\alpha_p \\ \alpha_2\alpha_1\alpha_3\dots\alpha_p \end{pmatrix} = (\alpha_1\,\alpha_2) ; \Psi(\tilde{\xi}_0) \in \Psi(G_{Q[\alpha_1,\dots,\alpha_p]})$$

т.е. $\Psi(G_{Q[\alpha_1,\dots,\alpha_p]})$ содержит транспозицию. Теперь используем теорему II из 8. Согласно этой теореме, если $\Psi(G_{Q[\alpha_1,\dots,\alpha_p]}) \neq S_p$, то $\Psi(G_{Q[\alpha_1,\dots,\alpha_p]})$ импримитивна, но было показано, что она примитивна, значит $\Psi(G_{Q[\alpha_1,\dots,\alpha_p]}) = S_p$, а тогда $\Psi$ - изоморфизм $G_{Q[\alpha_1,\dots,\alpha_p]}$ на $S_p$. Лемма доказана.

Определение 2. Пусть дано уравнение $a_0x^n + a_1x^{n-1} + \dots + a_n = 0$ с корнями $\alpha_1,\dots,\alpha_n$. Оно называется разрешимым в радикалах, если все его корни $\alpha_1,\dots,\alpha_n$ выражаются в радикалах через $Q[a_0,\dots,a_n]$.

Пусть $P = Q[a_0,\dots,a_n]$, $\forall \gamma \in P[\alpha_1,\dots,\alpha_n]$ выражается в радикалах через $P = Q[a_0,\dots,a_n] \Longleftrightarrow G_{P[\alpha_1,\dots,\alpha_n]}$ разрешима (по теореме из I7). Таким образом, для того, чтобы показать, что уравнение неразрешимо в радикалах, нужно доказать, что его группа Галуа $G_{P[\alpha_1,\dots,\alpha_n]}$ неразрешима (ибо тогда по критерию разрешимости (I7) не все элементы из $P[\alpha_1,\dots,\alpha_n]$ могут выражаться в радикалах через $P = Q[a_0,\dots,a_n]$, а значит, не все корни $\alpha_1,\dots,\alpha_n$ могут выражаться в радикалах через $P = Q[a_0,\dots,a_n]$. Для установления же примера уравнения неразрешимого в радикалах, была доказана лемма, ведь мы показали, что группы подстановок $S_n$ $(n \geq 5)$ неразрешимы (5).

## 19. Дополнительные сведения, необходимые для построения уравнения, неразрешимого в радикалах

### 19.1. Критерий Эйзенштейна

**Лемма.** Пусть $p$ – простое число такое, что у полиномов

$$f_1(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$ и
$$f_2(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m$$

не все коэффициенты делятся на $p$.
Если у $f_1(x)\cdot f_2(x) = c_0x^{m+n} + c_1x^{m+n-1} + \ldots + c_{m+n-1}x + c_{m+n}$

$c_1 \vdots p, c_2 \vdots p, \ldots, c_{m+n-1} \vdots p, c_{m+n} \vdots p$, то у исходных полиномов должны делиться на $p$ $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m$.

Доказательство: Пусть о полинома $f_1(x)$, $a_r$ – коэффициент с наибольшим номером, не делящийся на $p$, а у полинома $f_2(x)$, $b_s$ коэффициент с наибольшим номером, не делящийся на $p$. Рассмотрим $c_{r+s}$. Этот коэффициент представляет собой сумму слагаемых $a_i b_j$, у которых $i+j = r+s$.
Все $a_i b_j$, у которых $i>r$, делятся на $p$ по выбору $r$.
Все $a_i b_j$, у которых $j>s$ делятся на $p$ по выбору $s$.
Что касается $a_r b_s$, то оно на $p$ не делится, так как $p$ – простое, а $a_r \not\vdots p$, $b_s \not\vdots p$. Таким образом, $c_{r+s}$ равно сумме слагаемых, которые все, кроме одного, делятся на $p$, поэтому $c_{r+s} \not\vdots p$. По условию это возможно, если $r+s=0$, т.е. когда $r=0, s=0$. Но это и означает, что все $a_i$ при $i>0$ и все $b_j$ при $j>0$ делятся на $p$.

ТЕОРЕМА 1. Полином $f(x)$ с целыми коэффициентами, приводимый над полем $Q$, разлагается на произведение полиномов ненулевой степени с целыми коэффициентами.

Доказательство: Полином $f(x)$ по условию может быть разложен на произведение двух полиномов ненулевой степени с рациональными коэффициентами. Умножим $f(x)$ на $n \in N$, чтобы указанное разложение превратилось в разложение полинома $nf(x)$ на произведение полиномов ненулевой степени, коэффициенты которых – целые числа:

$$nf(x) = f_1(x) f_2(x) \qquad (1)$$

Пусть $n$ – наименьшее из натуральных чисел, требующихся нам для выполнения равенства (1). Нужно доказать, что $n=1$.
Допустим, что $n>1$. Обозначим через $p$ простое



число такое, что $n \vdots p$. Если бы все коэффициенты $f_1(x)$ делились бы на $p$, то сократив на $p$ равенство (1), получили бы опять требуемое разложение, но с первым множителем $\frac{n}{p} < n$,

что противоречит выбору $n$. Значит, не все коэффициенты полинома $f_1(x)$ делятся на $p$. То же самое можно доказать и про $f_2(x)$. Что касается коэффициентов полинома $nf(x)$, то они все делятся на $p$ (так как $n \vdots p$). По лемме все коэффициенты $f_1(x)$ и $f_2(x)$, кроме старших, делятся на $p$. Однако это противоречит тому, что произведение старших коэффициентов $f_1(x)$ и $f_2(x)$ равно старшему коэффициенту полинома $nf(x)$ делящемуся на $p$. Теорема доказана.

ТЕОРЕМА 2 (Критерий Эйзенштейна).
Пусть дан полином $f(x) = a_0x^n + \ldots + a_n$, где $a_i \in Z$ $(i = 0 \div n)$
Если существует такое простое число $p$, что $a_0 \not\vdots p$, $a_i \vdots p$, $(i=1 \div n)$
$a_n \not\vdots p^2$, то $f(x)$ неприводим над $Q$.

Доказательство: Допустим, что $f(x)$ приводим над $Q$, тогда он разлагается на два множителя меньшей степени с целыми коэффициентами (по теореме 1):

$$f(x) = (b_0x^k + \ldots + b_k)(c_0x^l + \ldots + c_l), \text{ где } k<n, l<n.$$

По единственности нормальной формы получаем:

$$a_n = b_k c_l$$
$$a_{n-1} = b_k c_{l-1} + c_l b_{k-1}$$
$$\ldots\ldots\ldots\ldots$$
$$a_0 = b_0 c_0$$

Так как $a_n \vdots p$, то одно из чисел $b_k, c_l$ должно делиться на $p$ ($p$ – простое!). Оба они не могут делиться на $p$ одновременно, так как $a_n \not\vdots p^2$.

Пусть $b_k \vdots p$, тогда $(c_l, p) = 1$. Перейдем ко второму равенству. Его левая часть $a_{n-1} \vdots p$, следовательно, $b_{k-1}c_l \vdots p$. В силу сказанного выше $b_{k-1} \vdots p$ и т.д.
Получим в конце концов, что $b_0 \vdots p$, т.е. $a_0 \vdots p$, чего нет по условию. Значит, наше предположение было неверным и $f(x)$ неприводим над $Q$.

ПРИМЕР. Полином $f(x) = x^4 - 8x^3 + 12x^2 - 6x + 2$ с целыми коэффициентами неприводим над $Q$, так как

$\exists p=2$ :

$1 \not| 2,\ -8 \vdots 2,\ 12 \vdots 2,\ -6 \vdots 2,\ 2 \vdots 2,\ 2 \not| 4$

## 19.2. Теорема Штурма

Определение. Пусть $f(x)=a_0x^n+\ldots+a_n$ – многочлен, где $a_i \in R\ (i=0 \div n)$, не имеющий кратных корней. Упорядоченная система отличных от нуля многочленов $f(x)=f_0(x), f_1(x), \ldots, f_s(x)$ называется системой Штурма для многочлена $f(x)$, если

1) соседние многочлены этой системы не имеют общих корней,

2) последний многочлен $f_s(x)$ не имеет вещественных корней,

3) если $\alpha \in R$ – корень одного из промежуточных многочленов $f_i(x)$ $(1 \le i \le s-1)$, то $f_{i-1}(\alpha)$ и $f_{i+1}(\alpha)$ имеют разные знаки,

4) если $\alpha \in R$ – корень $f(x)$, то $f(x) \cdot f_1(x)$ меняет знак с "–" на "+" при переходе $x$ через $\alpha$.

Рассмотрим $c \in R: f(c) \neq 0$. Составим последовательность $f_0(c), f_1(c), \ldots, f_s(c)$. Вычеркнем из нее числа, являющиеся нулями и выпишем знаки оставшихся чисел. Через $W(c)$ обозначают число перемен знаков в системе Штурма для многочлена $f(x)$ при $x=c$.

ТЕОРЕМА ШТУРМА. Пусть $a, b \in R$. Если $a, b\ (a<b)$ не являются корнями многочлена $f(x)$, не имеющего кратных корней, то $W(a) \ge W(b)$ и $W(a)-W(b)$ равна числу вещественных корней многочлена $f(x)$, заключенных между $a$ и $b$.

Доказательство: Рассмотрим, как меняется число $W(x)$ при возрастании $x$. Пока $x$, возрастая, не встретит корня ни одного из многочленов системы Штурма, знаки многочленов этой системы не будут меняться (теорема Больцано–Коши из курса математического анализа), и $W(x)$ останется без изменения. Поэтому, учитывая 2) условие из определения системы Штурма, нам остается рассмотреть 2 случая:

а) переход $x$ через корень одного из промежуточных многочленов $f_i(x)$ $(1 \le i \le s-1)$

б) переход $x$ через корень самого многочлена $f(x)$

Рассмотрим первый случай.



Пусть $\alpha$ – корень многочлена $f_k(x)$, $1 \le k \le s-1$. Тогда по I) условию из определения $f_{k-1}(\alpha) \neq 0$ и $f_{k+1}(\alpha) \neq 0$. Следовательно, по теореме о сохранении знака непрерывной функции $\exists \varepsilon>0: f_{k-1}(x) \neq 0$ и $f_{k+1}(x) \neq 0$, $\forall x \in [\alpha-\varepsilon, \alpha+\varepsilon]$, причем сохраняют постоянный знак. По 3) условию определения эти знаки различны. Отсюда следует, что каждая из систем чисел

$$f_{k-1}(\alpha-\varepsilon),\ f_k(\alpha-\varepsilon),\ f_{k+1}(\alpha-\varepsilon) \qquad (1) \text{ и}$$

$$f_{k-1}(\alpha+\varepsilon),\ f_k(\alpha+\varepsilon),\ f_{k+1}(\alpha+\varepsilon) \qquad (2)$$

обладает ровно одной переменной знаков независимо от того, каковы знаки чисел $f_k(\alpha-\varepsilon)$ и $f_k(\alpha+\varepsilon)$, так как если, например, $f_{k-1}(x)$ на рассматриваемом отрезке отрицателен, а $f_{k+1}(x)$ положителен и если $f_k(\alpha-\varepsilon)>0, f_k(\alpha+\varepsilon)<0$, то системам (I) и (2) соответствуют системы знаков: –, +, +

–, –, +

Таким образом, при переходе $x$ через корень одного из промежуточных многочленов системы Штурма перемены знаков в этой системе могут лишь перемещаться, но не возникают вновь и не исчезают, поэтому число $W(x)$ останется без изменения.

Рассмотрим теперь второй случай.

Пусть $\alpha$ – корень многочлена $f(x)$. По I) условию определения $f_1(\alpha) \neq 0$. По той же теореме о сохранении знака непрерывной функции $\exists \varepsilon>0: \forall x \in [\alpha-\varepsilon, \alpha+\varepsilon],\ f_1(x) \neq 0$ и сохраняет постоянный знак. Если этот знак положителен, то по 4) условию определения сам многочлен $f(x)$ при переходе $x$ через $\alpha$ меняет знак с минуса на плюс, т.е. $f(\alpha-\varepsilon)<0, f(\alpha+\varepsilon)>0$

Системам чисел $f(\alpha-\varepsilon), f_1(\alpha-\varepsilon)$ (3) и $f(\alpha+\varepsilon), f_1(\alpha+\varepsilon)$ (4) соответствуют системы знаков –, +

+, +

Таким образом, в системе Штурма теряется одна перемена. Если же знак $f_1(x)$ на $[\alpha-\varepsilon, \alpha+\varepsilon]$ отрицателен, то снова по 4) условию определения $f(x)$ меняет знак с плюса на минус при переходе $x$ через $\alpha$, т.е. $f(\alpha-\varepsilon)>0, f(\alpha+\varepsilon)<0$. В этом случае системам чисел (3) и (4) соответствуют системы знаков +, –

–, –

То есть в системе Штурма теряется одна перемена. Итак, число

$W(x)$ меняется (при возрастании $x$ ) лишь при переходе $x$ через корень многочлена $f(x)$ , причем в этом случае оно уменьшается на единицу.

Этот вывод и доказывает теорему Штурма.

Докажем теперь, что каждый многочлен над полем , не имеющий квадратных корней, обладает системой Штурма. При этом мы получим и алгоритм построения такой системы.

$$f_0(x) \equiv f(x)$$

$$f_1(x) = f'(x)$$

4) условие из определения системы Штурма выполняется: если $f(\alpha)=0 \ (\alpha \in R)$ , то $f'(\alpha) \neq 0$ (так как $f(x)$ не имеет кратных корней). Допустим, что $f'(\alpha)>0$ . Тогда по теореме о сохранении знака непрерывной функции $f'(x)>0$ в некоторой окрестности $x=\alpha$ , следовательно $f(x)$ меняет знак с минуса на плюс при переходе $x$ через $\alpha$ , и поэтому $f(x)\cdot f'(x)$ тоже меняет знак с минуса на плюс при переходе $x$ через $\alpha$ .

Аналогично рассматривается случай $f'(\alpha)<0$ :

Поделим с остатком $f(x)$ на $f_1(x)$ и в качестве $f_2(x)$ возьмем остаток от деления с противоположным знаком:

$$f(x) = f_1(x)q_1(x) - f_2(x)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$f_{i-1}(x) = f_i(x)q_i(x) - f_{i+1}(x) \qquad (5)$$

Будем продолжать этот процесс.

Последний отличный от нуля остаток (как в алгоритме Евклида) есть $НОД(f(x), f'(x))$. Поскольку $f(x)$ не имеет кратных корней, то $НОД(f(x), f'(x)) = const$ , а значит, выполняется 2) условие из определения системы Штурма: $f_s(x)$ не имеет вещественных корней ( $f_s(x)$ – последний многочлен), так как $f_s(x)=const$ . Проверим, что выполняется 3) условие из определения системы Штурма:

Если $\alpha$ – корень $f_i(x)$ $(1 \le i \le s-1)$, то $f_i(\alpha)=0$ и из равенства (5) $f_{i-1}(\alpha) = -f_{i+1}(\alpha)$

Осталось проверить лишь выполнимость I) условия из определения: допустим, что соседние многочлены $f_i(x)$, $f_{i+1}(x)$ имеют общий корень, тогда по (5) его имеет и $f_{i-1}(x)$ . Поднимаясь вверх по равенствам, получим, что общий корень будут иметь $f_1(x)=f'(x)$ и $f_0(x)=f(x)$ , что не-



возможно (см. выше)

ПРИМЕР. Построим систему Штурма для многочлена $f(x) = x^3+3x^2-1$ и найдем число его действительных корней на $[-1,1]$

$$f_0(x) = f(x) = x^3+6x^2-1$$

$$f_1(x) = f'(x) = 3x^2+6x$$

$$\begin{array}{r|l} x^3+3x^2-1 & 3x^2+6x \\ -\underline{x^3+2x^2} & \frac{1}{3}x+\frac{1}{3} \\ x^2-1 & \\ -\underline{x^2+2x} & \\ -2x-1 & \end{array} \qquad \begin{array}{r|l} 3x^2+6x & 2x+1 \\ -\underline{3x^2+\frac{3}{2}x} & \frac{3}{2}x+\frac{9}{4} \\ \frac{9}{2}x & \\ -\underline{\frac{9}{2}x+\frac{9}{4}} & \\ -\frac{9}{4} & \end{array}$$

$f_2(x) = 2x+1$ (изменение знака!)

$f_3(x) = 1$ (для удобства, ведь мы знаем, что у любых двух многочленов есть бесконечно много $НОД$ , но все они отличаются друг от друга постоянным множителем).

Найдем число перемен знаков в этой системе при $x=-1$ и $x=1$

| | $f(x)$ | $f_1(x)$ | $f_2(x)$ | $f_3(x)$ | $W(x)$ |
|---|---|---|---|---|---|
| -I | + | – | – | + | 2 |
| I | + | + | + | + | 0 |

Следовательно, многочлен $f(x)$ на $[-1,1]$ обладает двумя действительными корнями.

## 20. Пример уравнения, неразрешимого в радикалах

Рассмотрим уравнение $x^5 - px + p = 0$ , где $p$ – простое число. Покажем, что оно удовлетворяет условиям леммы из I8 (пусть у нас $p \geq 13$ ). Многочлен $f(x) = x^5 - px + p$ неприводим над $Q$ по критерию Эйзенштейна: в самом деле, если в качестве простого числа в условиях критерия будет взято само $p$ из примера, то $1 \not\vdots p$, $-p \vdots p$, $p \vdots p$, $p \not\vdots p^2$ $(p \in N)$

Построим систему Штурма для многочлена $f(x)$ . При этом в процессе деления многочленов мы будем умножать и сокращать лишь на произвольные положительные числа, так как знаки остатков играют здесь основную роль.

$$f_0(x) = f(x) = x^5 - px + p$$
$$f_1(x) = f'(x) = 5x^4 - p$$
$$\begin{array}{l|l} -\dfrac{x^5 - px + p}{x^5 - \frac{1}{5}xp} & \dfrac{5x^4 - p}{\frac{1}{5}x} \\ \quad -\frac{4}{5}px + p & \end{array}$$

Домножая на $\dfrac{5}{p}$ , получим $f_2(x) = 4x - 5$

(остатки от деления берутся с противоположным знаком)

$$\begin{array}{l|l} -\dfrac{5x^4 - p}{5x^4 - \frac{25}{4}x^3} & \dfrac{4x-5}{\frac{5}{4}x^3 + \frac{25}{16}x^2 + \frac{125}{64}x + \frac{625}{256}} \\ -\dfrac{\frac{25}{4}x^3 - p}{\frac{25}{4}x^3 - \frac{125}{16}x^2} & \\ -\dfrac{\frac{125}{16}x^2 - p}{\frac{125}{16}x^2 - \frac{625}{64}x} & \\ -\dfrac{\frac{625}{64}x - p}{\frac{625}{64}x - \frac{3125}{256}} & \\ \quad \frac{3125}{256} - p & \end{array}$$

$\dfrac{3125}{256} - p = 12\dfrac{53}{256} - p < 0$, так как $p \geq 13$.

Домножая на обратные этому числу, взятому по модулю, получим -1, а значит, $f_3(x) = 1$

$f(x)$ не имеет кратных корней, так как $1 = f_3(x) = \text{НОД}(f(x), f'(x))$

Итак, система Штурма для многочлена $f(x)$ имеет вид

$x^5 - px + p$ , $5x^4 - p$, $4x - 5$, $1$

Пусть теперь в теореме Штурма $a = -\infty$ , $b = +\infty$ Заметим, что при "больших" $x$ знак многочлена

$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$



совпадает со знаком старшего члена.

Составим таблицу:

| | $f(x)$ | $f_1(x)$ | $f_2(x)$ | $f_3(x)$ | $W(x)$ |
|---|---|---|---|---|---|
| $a = -\infty$ | − | + | − | + | 3 |
| $b = +\infty$ | + | + | + | + | 0 |

Итак, по теореме Штурма многочлен $f(x)$ имеет ровно три вещественных корня $(W(a) - W(b) = 3)$ , поэтому поскольку всего корней у многочлена $x^5 - px + p$ пять (причем кратных нет), то невещественных получается ровно два.

Итак, условия леммы выполнены, $G_{Q[\alpha_1,\ldots,\alpha_5]} \approx S_5$, $S_5$ неразрешима, значит, $G_{Q[\alpha_1,\ldots,\alpha_5]}$ неразрешима, а тогда по критерию разрешимости (17) уравнение неразрешимо в радикалах.

Существуют и другие уравнения, неразрешимые в радикалах.

Замечание. Если хотя бы один корень неприводимого уравнения выражается в радикалах, то уравнение разрешимо в радикалах (по теореме из 15). Поэтому у уравнений, удовлетворяющих условиям леммы из 18, в том числе у уравнений $x^5 - px + p = 0$ , в радикалах не выражается ни один корень.

Таким образом, над полем рациональных чисел $\mathbb{Q}$ существуют неразрешимые в радикалах уравнения пятой степени (причем бесконечно много). Так как если все уравнения некоторой степени разрешимы в радикалах, то разрешимы в радикалах и все уравнения любой меньшей степени (почему?), то тем самым доказано, что над полем рациональных чисел существуют неразрешимые в радикалах уравнения любой степени, большей или равной пяти.

Для построения таких уравнений достаточно, например, многочлен $x^5 - px + p$ умножить на произвольный многочлен некоторой степени.

## Рекомендуемая литература

1. Постников М.М. Теория Галуа. М., 1963.
2. Курош А.Г. Курс высшей алгебры. М., 1971.
3. Ляпин Е.С., Евсеев А.Е. Алгебра и теория чисел. М.,1974. Ч. I, II.
4. Элементы теории групп и ее приложение :Методическая разработка по современной алгебре. Л., 1990.
5. Ляпин Е.С., Айзенштат А.Я., Лесохин М.М. Упражнения по теории групп. М., 1967.
6. Чеботарев Н.Г. Основы теории Галуа. М., 1934.
7. Ван дер Варден. Алгебра. М., 1976.

О Г Л А В Л Е Н И Е





МЕТОДИЧЕСКАЯ РАЗРАБОТКА ПО ТЕМЕ
«ЭЛЕМЕНТЫ ТЕОРИИ ГАЛУА»

Технический редактор К. П. Орлова

Подписано к печати 12.10.92. Формат $60\times84^{1}/_{16}$. Объем: 4,0 уч.-изд. л., 4,0 усл.-печ. л. Тираж 300 экз. Бумага писчая. Печать офсетная. Заказ № 735

Издательство «Образование». 191186, С.-Петербург, наб. р. Мойки, 48
РТП. Тип. ВИР.