Доклады Академии Наук СССР
1954. Том XCV, № 2

МАТЕМАТИКА

И. Р. ШАФАРЕВИЧ

О РАЗРЕШИМЫХ В РАДИКАЛАХ РАСШИРЕНИЯХ ПОЛЕЙ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

(Представлено академиком И. М. Виноградовым 22 I 1954)

В настоящей заметке излагаются основные этапы доказательства того, что над любым полем алгебраических чисел существует расширение с наперед заданной разрешимой группой Галуа. Доказательство основывается на некоторых арифметических свойствах полей с группой Галуа порядка l^{α}.

Пусть k есть поле алгебраических чисел, K/k — нормальное расширение с группой Галуа G и h — любое целое число, делящееся на все простые делители степени $(K:k)$. Мы будем называть расширение K/k шольцевым относительно h, если выполнены следующие условия: 1) все критические простые дивизоры K/k имеют относительный порядок 1 над k; 2) абсолютные нормы критических простых дивизоров K/k сравнимы с 1 по модулю h; 3) простые делители h полностью распадаются в K/k; 4) вещественные бесконечные дивизоры k распадаются на вещественные в K.

Значение этого класса полей определяется тем, что если: $(K:k)=l^{\nu}$; показатель (максимальный порядок элемента) G есть l^{ν_0}; $l^{\nu_0+1}\,|\,h$ и K/k шольцево относительно h, то K/k можно погрузить в поле K_1/k с любой группой Галуа G_1 порядка $l^{\nu+1}$, гомоморфным образом которой является G, причем так, чтобы предписанный гомоморфизм G_1 на G совпадал с естественным гомоморфизмом группы Галуа поля на группу Галуа подполя [1, 2].

При построении полей с разрешимой группой Галуа мы будем строить поля с некоторыми универсальными группами, из которых все разрешимые группы получаются переходом к фактор-группам.

Обозначим некоторое множество простых чисел $l_1, \ldots, l_r$ через π и определим группу $G_{d,\pi}^{(c)}$ как фактор-группу свободной группы S_d с d образующими по нормальному делителю N_c. При этом $N_0 = S_d$. Если N_{c-1} определено, то пусть $\mathfrak{S}_l / N_{c-1}$ является силовской l_l-подгруппой S_d / N_{c-1} и $N^{(l)}$ — наибольший нормальный делитель S_d, содержащийся в группе $[N_{c-1}, \mathfrak{S}_l]\, N_{c-1}^{l_l}$. Здесь $[A, B]$ означает взаимный коммутант подгрупп A и B, а A^l — подгруппу, порожденную l-ми степенями элементов A. Мы берем за N_c пересечение $N^{(1)}, \ldots, N^{(r)}$. Из теоретико-групповой теоремы, доказанной независимо Д. К. Фаддеевым [3, 4] и Гашютцом [5], следует, что любая конечная разрешимая группа является фактор-группой некоторой группы $G_{d,\pi}^{(c)}$. Таким образом, для построения поля с любой разрешимой группой Галуа достаточно построить поле с любой группой $G_{d,\pi}^{(c)}$.

Обозначим через h число $(l_1 \ldots l_r)^{c+1}$ и построим поле с группой $G_{d,\pi}^{(c)}$, K/k шольцево относительно h. Пусть K/k шольцево относительно h поле с группой $G_{d,\pi}^{(u-1)}$ $(u \leqslant c)$. Выясним, когда его можно погрузить в шольцево поле с группой $G_{d,\pi}^{(u)}$. Обозначим через L_i подполе поля K/k, принадлежащее к некоторой силовской l_i-подгруппе $\mathfrak{G}_i$ его группы Галуа. Предположим, что K содержит корень степени l_i из 1 и для любого автоморфизма σ K/k $\zeta^\sigma = \zeta^{g(\sigma)}$.

Число μ поля K называется l_i-инвариантным в K/L_i, если $\mu^{1-\sigma}$ есть l_i-я степень числа K для любого $\sigma \in \mathfrak{G}_i$. Для l_i-инвариантного числа имеет место разложение

$$(\mu) = \mathfrak{L}^{l_i} \mathfrak{D} \mathfrak{m}, \tag{1}$$

где $\mathfrak{L}$ — дивизор K; $\mathfrak{D}$ — инвариантный дивизор K/L_i, состоящий только из критических множителей, а $\mathfrak{m}$ — дивизор L_i, не содержащий критических в K множителей, причем $\mathfrak{m}$ и $\mathfrak{D}$ не содержат l_i-х степеней. Все l_i-инвариантные числа K/L_i, отличающиеся друг от друга на l_i-ю степень и множитель из L_i, образуют один класс, обозначаемый через X. Классы l_i-инвариантных чисел шольцева поля K/L_i образуют группу, изоморфную группе классов ассоциированных систем множителей на $\mathfrak{G}_i$ со значениями в циклической группе порядка l_i.

Через χ обозначим характер порядка l_i группы $\mathfrak{G}_i$. Ему соответствует такое число $\alpha_\chi \in L_i$, что

$$\sqrt[l_i]{\alpha_\chi} \in K, \quad \sqrt[l_i]{\alpha_\chi}^{\,1-\sigma} = \chi(\sigma) \quad \text{при } \sigma \in \mathfrak{G}_i \text{ (}^6\text{)}.$$

Обозначим через $\mathfrak{p}$ произвольный простой делитель α_χ, входящий в α_χ в степени, не делящейся на l_i, и через $\mathfrak{P}$ — его любой простой делитель в K. Мы имеем тогда разложение

$$(\alpha_\chi) = \prod_{\mathfrak{p}} \mathfrak{P}^{\Sigma \varphi_{\mathfrak{P}}(\sigma)\sigma},$$

причем функции $\varphi_{\mathfrak{P}}(\sigma)$, очевидно, постоянны на правых классах смежности группы $G_{d,\pi}^{(u-1)}$ по $\mathfrak{G}_i$. Предположим, что α_χ таково, что для любого $\mathfrak{p}$

$$(\mathfrak{D}^{\Sigma \varphi^*_{\mathfrak{P}}(S) g(\sigma)\sigma}, \mathfrak{P}) = 1. \tag{2}$$

Здесь в показателе суммирование распространено на любую систему представителей σ левых классов смежности S по подгруппе $\mathfrak{G}_i$, $\varphi^*_{\mathfrak{P}}(S) = \varphi_{\mathfrak{P}}(\sigma^{-1})$ и $\mathfrak{D}$ то же, что и в (1).

Если выполнено (2), то полагаем

$$[\chi, X]^{(i)} = \prod_{\mathfrak{p}} \left(\frac{\mu^{\Sigma \varphi^*_{\mathfrak{P}}(S) g(\sigma)\sigma}}{\mathfrak{P}} \right).$$

Инвариант $[\chi, X]^{(i)}$ зависит только от выбора $\mathfrak{G}_i$, χ и X.

Предположим, что нам дана функция $\psi(\sigma)$ на группе $G_{d,\pi}^{(u-1)}$ со значениями в группе классов вычетов по модулю l_i, постоянная на классах смежности по двойному модулю $(\mathfrak{G}_i, \mathfrak{G}_i)$ и удовлетворяющая условиям:

$$\psi(\sigma^{-1}) = -g(\sigma)\psi(\sigma), \qquad \mu^{\Sigma\psi(S)\sigma} = m_\psi C_\psi^{l_i}, \tag{3}$$

где сумма в показателе распространена на любую систему представителей σ левых классов смежности по подгруппе $\mathfrak{G}_i$, m_ψ есть некоторое число на L_i, а C_ψ — из K. Если выполнено (3) и $(m_\psi)=\prod_{\mathfrak{p}}\mathfrak{p}^{\nu(\mathfrak{p})}$ в L_i, то полагаем

$$[X]_\psi^{(i)}=\prod_{\mathfrak{p}}\left(\frac{\mu}{\mathfrak{P}}\right)^{\nu(\mathfrak{p})},$$

где $\mathfrak{P}$ есть любой один из простых делителей $\mathfrak{p}$ в K.

Инвариант $[X]_\psi^{(i)}$ зависит только от выбора $\mathfrak{G}_i$, ψ и X.

Обозначим через ζ_h первообразный корень h-й степени из 1, а через $L_{h,i}$ — максимальное подполе поля $L_i(\zeta_h)$, являющееся композитом циклических полей степени l_i над L_i. В каждом классе X l_i-инвариантных чисел поля K/L_i можно найти представителя μ_i, являющегося l_i-й степенью в замыкании K по любому простому делителю h. Автоморфизм Фробениуса, к которому принадлежит в поле $L_{h,i}$ дивизор $\mathfrak{m}$ из разложения (1) такого представителя, зависит только от выбора $\mathfrak{G}_i$ и X и будет обозначаться через $(X)_h^{(i)}$. Инвариант $(X)_h^{(i)}$ может принимать только конечное число значений, причем это число зависит только от l_i и h.

Если поле K не содержит корня степени l_i из 1, то, присоединяя его к K, получим расширение $\overline{K}$, инварианты $[\chi, X]^{(i)}$, $[X]_\psi^{(i)}$ и $(X)_h^{(i)}$ для которого будем называть инвариантами расширения K.

Теорема 1. *Для того чтобы шольцево относительно h поле K/k с группой $G_{d,\pi}^{(u-1)}$ можно было погрузить в шольцево поле с группой $G_{d,\pi}^{(u)}$, необходимо и достаточно, чтобы в нем все инварианты $[\chi, X]^{(i)}$, $[X]_\psi^{(i)}$ и $(X)_h^{(i)}$, равнялись* 1.

Из соображений, в основе своей теоретико-групповых, получается следующий результат:

Теорема 2. *Для всякого числа d существует такое $D>d$, что у любого шольцева относительно h поля с группой $G_{D,\pi}^{(u-1)}$ существует подполе с группой $G_{D,\pi}^{(u-1)}$ и всеми инвариантами $[\chi, X]^{(i)}$, $[X]_\psi^{(i)}$ и $(X)_h^{(i)}$, равными* 1.

Применяя индукцию по c (при произвольном d и заданных π и h), мы выводим отсюда существование поля с группой $G_{d,\pi}^{(c)}$ при любых c, d и π. Из этого, в свою очередь получаем:

Теорема 3. *Над любым полем алгебраических чисел существует расширение с наперед заданной разрешимой группой Галуа.*

Поступило
20 I 1954

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] A. Scholz, Math. Zs., **42**, 161 (1936). [2] H. Reichardt, J. reine u. angew. Math., **177**, 1 (1937). [3] Д. К. Фаддеев, Изв. АН СССР, сер. матем., **16**, 17 (1952). [4] Д. К. Фаддеев, ДАН, **92**, 703 (1953). [5] W. Gaschütz, J. reine u. angew. Math., **190**, 93 (1952). [6] E. Witt, ibid., **173**, 43 (1935).