Доклады Академии Наук СССР
1954. Том XCIV, № 6

МАТЕМАТИКА

Д. К. ФАДДЕЕВ

ОБ ОДНОЙ ГИПОТЕЗЕ ХАССЕ

(Представлено академиком И. М. Виноградовым 29 XII 1953)

1°. Пусть k — нормальное поле над k_0; $\mathfrak{F}$ — его группа автоморфизмов. Дана конечная группа $\mathfrak{G}$ и ее гомоморфное отображение φ с ядром $\mathfrak{N}$ на группу $\mathfrak{F}$. Проблема погружаемости заключается в установлении условий, которым должно удовлетворять k (при данных $\mathfrak{G}$ и φ) для возможности погружения k в нормальное поле K с группой $\mathfrak{G}$ так, чтобы естественный гомоморфизм $\mathfrak{G}$ на $\mathfrak{F}$ совпадал с наперед заданным φ. Проблема погружаемости может быть ослаблена требованием возможности погружения k в алгебру Галуа K, т. е. в сепарабельную полупростую коммутативную алгебру, допускающую автоморфизмы из $\mathfrak{G}$ и имеющую нормальный базис относительно k_0.

В работе (1) нами установлено некоторое необходимое условие погружаемости, названное нами условием согласности $\mathfrak{G}$ и k (при данном φ). Там же дается несколько равносильных формулировок условия согласности, из которых нам будут нужны следующие две:

А. Для согласности $\mathfrak{G}$ и k необходимо и достаточно, чтобы в групповом кольце $\mathfrak{N}\cdot k$ нашлись элементы l_σ такие, что $l_{\sigma_1}^{\tilde{\sigma}_2}\cdot l_{\sigma_2}=l_{\sigma_1\sigma_2}$ $(\sigma_1,\ \sigma_2\in\mathfrak{G})$ и $l_\tau=\tau^{-1}$ $(\tau\in\mathfrak{N})$. Здесь $\tilde{\sigma}$ есть автоморфизм $\mathfrak{N}\cdot k$, действующий на элементы $\mathfrak{N}$ по формуле $\tau^{\tilde{\sigma}}=\sigma^{-1}\tau\sigma$, а на элементы k как автоморфизм $\varphi(\sigma)$ (теорема из § 10 (1)). Если $\mathfrak{N}$ абелево, то $\tilde{\sigma}$ зависит лишь от $s=\varphi(\sigma)$.

Вторая формулировка требует рассмотрения скрещенного произведения $\mathfrak{A}=\mathfrak{G}\times k$. Это есть алгебра над k_0, элементами которой являются формальные суммы $\sum\limits_{\sigma\in\mathfrak{G}} u_\sigma x_\sigma$, $x_\sigma\in k$, с правилами действий: $u_{\sigma_1}u_{\sigma_2}=u_{\sigma_1\sigma_2}$; $xu_\sigma=u_\sigma x^{\varphi(\sigma)}$ для $x\in k$.

В. Если ядро $\mathfrak{N}$ есть абелева группа, то для согласности $\mathfrak{G}$ и k необходимо и достаточно, чтобы алгебра $\mathfrak{A}=\mathfrak{G}\times k$ была полным кольцом матриц над своим центром (теорема из § 10 (1)).

Хассе в работе (2) исследует вопрос о погружаемости нормального над k_0 поля k в алгебру Галуа в предположениях, что $\mathfrak{N}$ есть абелева группа показателя n_0, характеристика k_0 не делит n_0 и k содержит первообразный корень степени n_0 из 1. Пусть X — группа характеров группы $\mathfrak{N}$, причем значения характеров отождествляются с корнями из 1, лежащими в k. В группе X вводятся операторы $s\in\mathfrak{F}$, по формуле $\chi^s(\tau)=[\chi(\sigma\tau\sigma^{-1})]^s$, где σ — такой элемент из $\mathfrak{G}$, что $\varphi(\sigma)=s$. Далее, пусть $\bar{s}$ — элементы $\mathfrak{G}$ такие, что $\varphi(\bar{s})=s$, по одному для каждого $s\in\mathfrak{F}$, причем $\bar{1}=1$. Тогда $\bar{s}_1\bar{s}_2=\overline{s_1s_2}C_{s_1,s_2}$, где C_{s_1,s_2} — фактор-система.

Хассе устанавливает следующее необходимое условие погружаемости. Для погружаемости k в алгебру Галуа K с группой $\mathfrak{G}$ (при данном гомоморфизме φ) необходимо, чтобы в k существовали элементы $b_{\chi, s}$ такие, что

$$b^{s_2}_{\chi^{s_2^{-1}}, s_1} \quad b_{\chi, s_2} = b_{\chi, s_1 s_2} \cdot \chi(C_{s_1, s_2}). \tag{1}$$

Далее Хассе высказывает предположение, что это условие достаточно для погружаемости k в алгебру Галуа K.

Целью настоящей заметки является опровержение этой гипотезы.

2°. Условие Хассе эквивалентно (для рассматриваемого случая) нашему условию согласности в форме А. Действительно, положим для $z = \sum_{\tau \in \mathfrak{N}} \tau x_\tau \in \mathfrak{N} \cdot k$ $\chi(z) = \sum \chi(\tau) x_\tau$. Тогда $\chi(z_1 \pm z_2) = \chi(z_1) \pm \chi(z_2)$, $\chi(z_1 z_2) = \chi(z_1) \cdot \chi(z_2)$, $z = \sum_\chi \chi(z) e_\chi$, где $e_\chi = \frac{1}{n} \sum_\tau \chi^{-1}(\tau)\tau$. Далее, $\chi(\widetilde{z^s}) = \chi[\chi^{s^{-1}}(z)]^s$.

Пусть выполнено условие согласности (в формулировке А). Тогда $b_{\chi, s} = \chi^{-1}(l_{\bar{s}})$ удовлетворяет (1). Обратно, если существуют $b_{\chi, s}$, то, положив $l_{\bar{s}} = \sum_\chi b_{\chi, s} e_{\chi^{-1}}$ и для $\sigma = \bar{s}\tau$ $l_\sigma = l_{\bar{s}} \tau^{-1}$, получим, что $l_{\sigma_1}^{\widetilde{\sigma_2}} l_{\sigma_2} = l_{\sigma_1 \sigma_2}$ и $l_\tau = \tau^{-1}$. Поэтому предположение Хассе может быть сформулировано так:

Если $\mathfrak{N}$ есть абелева группа показателя n_0, характеристика k_0 не делит n_0 и k содержит первообразный корень степени n_0 из 1, то условие согласности является достаточным для погружаемости.

3°. Теорема. *Если k_1 согласно с $\mathfrak{G}_1$ при гомоморфизме φ_1 группы $\mathfrak{G}_1$ на группу автоморфизмов k_1, k_2 — нормальное поле с группой $\mathfrak{G}_2$ и $k_2 \cap k_1 = k_0$, то поле $k = k_1 k_2$ согласно с прямым произведением $\mathfrak{G}$ групп $\mathfrak{G}_1$ и $\mathfrak{G}_2$ при гомоморфизме φ, $\varphi(\sigma_1\sigma_2) = \varphi_1(\sigma_1)\sigma_2$, $\sigma_1 \in \mathfrak{G}_1$, $\sigma_2 \in \mathfrak{G}_2$.*

Доказательство. Положим для $\sigma = \sigma_1\sigma_2$, $\sigma_1 \in \mathfrak{G}_1$, $\sigma_2 \in \mathfrak{G}_2$, $l_\sigma = l_{\sigma_1}$.

4°. Теорема. *Если в условиях предыдущей теоремы k погружаемо (в соответствии с гомоморфизмом φ) в поле K с группой $\mathfrak{G} = \mathfrak{G}_1\mathfrak{G}_2$, то k_1 погружаемо (в соответствии с гомоморфизмом φ_1) в поле K_1 с группой $\mathfrak{G}_1$.*

Доказательство. K_1 есть подполе K, принадлежащее $\mathfrak{G}_2$.

5°. Пусть k_0 — поле с характеристикой $\neq 2$ и пусть $\mathfrak{K} = k_0(\sqrt{a}, \sqrt{b}, \sqrt{ab})$, $a, b \in k_0$; $k_1 = k_0(\sqrt{a})$, $k_2 = k_0(\sqrt{b})$, $k_3 = k_0(\sqrt{ab})$. Пусть τ_1 — нетривиальный автоморфизм $\mathfrak{K}$, оставляющий инвариантными элементы поля k_1; τ_2 — то же для k_2; $\tau_3 = \tau_1\tau_2$ — то же для k_3.

Теорема. *Если $\lambda \in \mathfrak{K}$ и норма λ есть квадрат элемента из k_0, то $\lambda = \lambda_1\lambda_2\lambda_3$, $\lambda_1 \in k_1$, $\lambda_2 \in k_2$, $\lambda_3 \in k_3$.*

Доказательство. Пусть $N(\lambda) = \lambda^{1+\tau_1+\tau_2+\tau_3} = m^2$, $m \in k_0$. Тогда $(m^{-1}\lambda^{1+\tau_1})^{1+\tau_2} = 1$ и $m^{-1}\lambda^{1+\tau_1} \in k_1$. Следовательно, $m^{-1}\lambda^{1+\tau_1} = \alpha_1^{1-\tau_2}$ при $\alpha_1 \in k_1$. Таким же образом $m^{-1}\lambda^{1+\tau_2} = \alpha_2^{1-\tau_1}$ при $\alpha_2 \in k_2$ и $m^{-1}\lambda^{1+\tau_3} = \alpha_3^{1-\tau_1}$ при $\alpha_3 \in k_3$. Рассмотрим $\mu = \lambda\alpha_1^{-1}\alpha_2^{-1}\alpha_3^{-1}$. Тогда $\mu^{1-\tau_1} = \lambda^{1-\tau_1}\alpha_1^{\tau_1-1}\alpha_2^{\tau_1-1}\alpha_3^{\tau_1-1} = m^2\lambda^{-1-\tau_1-\tau_2-\tau_3} = 1$. Таким же образом $\mu^{1-\tau_2} = \mu^{1-\tau_3} = 1$. Следовательно, $\mu \in k_0$ и $\lambda = (\mu\alpha_1)\alpha_2\alpha_3$, ч. т. д.

Следствие. Если $\lambda \in \mathfrak{K}$ и $\lambda^{1+\tau_1} = m \in k_0$, то $\lambda = \lambda_2\lambda_3$, $\lambda_2 \in k_2$, $\lambda_3 \in k_3$. Действительно, можно взять $\alpha_1 = 1$.

6°. Переходим к конструкции примера, опровергающего предположение Хассе. Сперва построим пример поля k_1, согласного с $\mathfrak{G}_1$, но не погружаемого в алгебру Галуа с группой $\mathfrak{G}_1$, без предположения о том, что k_1 содержит корни степени n_0 из 1. Затем при помощи теорем из 3° и 4° построим пример, опровергающий гипотезу Хассе.

Пусть $\mathfrak{G}_1$ — группа 16-го порядка, заданная образующими α, β и соотношениями $\alpha^8 = 1$, $\beta^2 = \alpha^4$, $\beta^{-1}\alpha\beta = \alpha^7$.

Пусть k_0 — поле с не равной 2 характеристикой, $k_1 = k_0(\theta)$, $\theta^2 = a$ — квадратичное поле. Гомоморфизм группы $\mathfrak{G}_1$ на группу автоморфизмов поля k_1 зададим формулами: $\theta^\alpha = \theta$, $\theta^\beta = -\theta$. Ядром гомоморфизма является циклическая группа $\{a\}$ 8-го порядка. Далее, пусть $\bar{k}_1 = k_0(\theta, \eta)$, $\theta^2 = a$, $\eta^2 = b$ — поле с четверной группой. Гомоморфизм $\mathfrak{G}_1$ на группу автоморфизмов $\bar{k}_1$ определим формулами: $\theta^\alpha = \theta$, $\theta^\beta = -\theta$, $\eta^\alpha = -\eta$, $\eta^\beta = \eta$. Ядром будет циклическая группа $\{a^2\}$ 4-го порядка. Исследуем условия согласности для k_1 и $\bar{k}_1$ с $\mathfrak{G}_1$, используя формулировку В.

Теорема.

$$\mathfrak{G}\times k_1 \approx k_0[1,\ 1] + k_0[1,\ 1] + k_0(\sqrt{-a})[1,\ 1] + k_0(\sqrt{-a},\ \sqrt{2})[-1,\ -1],$$

$$\mathfrak{G}\times \bar{k}_1 = k_0[1,\ 1][1,\ 1] + k_0[b,\ -a][1,\ 1] + k_0(\sqrt{-a})[2,\ \ b][-1,\ \ -1].$$

Здесь через $[p,\ q]$ обозначена алгебра обобщенных кватернионов, т. е. алгебра $k_0(i,\ j)$ при $i^2 = p$, $j^2 = q$, $ij = -ji$. В частности, $[1,\ 1]$ есть алгебра матриц второго порядка, $[-1,\ -1]$ — алгебра обыкновенных кватернионов. Теорема доказывается прямым вычислением, которое мы опускаем.

Из первого утверждения теоремы заключаем, что для согласности $\mathfrak{G}$ и k_1 необходимо и достаточно, чтобы алгебра кватернионов $[-1,\ -1]$ распадалась в поле $k_0(\sqrt{-a},\ \sqrt{2})$.

Из второго утверждения заключаем, что для погружаемости k_1 в поле (или алгебру Галуа) с группой $\mathfrak{G}_1$ необходимо, чтобы нашлось такое $b \in k_0$, что:

I. $[b,\ -a]$ распадается в k_0.

II. $[2,\ b] \approx [-1,\ -1]$ в $k_0(\sqrt{-a})$.

При этом, поскольку речь идет о погружении в алгебру, не исключено и $b = 1$.

Положим, что k_0 есть поле рациональных чисел и $a = 7$.

Условие согласности выполняется, ибо $\sqrt{-14} \in k_0(\sqrt{-7},\ \sqrt{2})$ и $-14 = (i + 2j + 3k)^2$.

Покажем, что не существует числа b, удовлетворяющего требованиям I и II. Легко видеть, что $[2,\ 5] \approx [-1,\ -1]$ в $k_0(\sqrt{-7})$, ибо $2 = \rho_1^2$, где $\rho_1 = \frac{1}{\sqrt{-7}}(i + 2j + 3k)^2$; $5 = \rho_2^2$, где $\rho_2 = \frac{1}{\sqrt{-7}}(i - 5j + 3k)^2$ и $\rho_1\rho_2 = -\rho_2\rho_1$.

Следовательно, для $[2,\ b] \approx [-1,\ -1]$ необходимо и достаточно, чтобы $b = 5N_{\mathfrak{K}/k_1}(\lambda)$, где $\mathfrak{K} = k_0(\sqrt{-7},\ \sqrt{2})$, $k_1 = k_0(\sqrt{-7})$. В силу 5° $\lambda = \lambda_2\lambda_3$ при $\lambda_2 \in k_0(\sqrt{2})$, $\lambda_3 \in k_0(\sqrt{-14})$ и $b = 5(x^2 + 14y^2)(u^2 - 2v^2)$ при $x,\ y,\ u,\ v \in k_0$.

Из I заключаем, что $b = w^2 + 7t^2$ при $w,\ t \in k_0$.

Покажем, что уравнение $5(x^2 + 14y^2)(u^2 - 2v^2) = w^2 + 7t^2$ не имеет решений в рациональных числах. Обозначим через Q множество нечетных простых чисел q, отличных от 7 и для которых $\left(\frac{2}{q}\right) = -1$ и $\left(\frac{-7}{q}\right) = -1$. $5 \in Q$. Числа из Q не могут входить в $u^2 - 2v^2$ и $w^2 + 7t^2$ в нечетных степенях. В поле $k_0(\sqrt{-14})$ имеется два рода, и простые делители чисел из Q принадлежат не главному роду, все же остальные простые идеалы принадлежат главному роду. Следовательно, если простые числа из Q входят в нечетных степенях в форму x^2+14y^2, то их число четное, и в $5(x^2+14y^2)$ входит в нечетной степени по крайней мере одно простое число из Q. Тем самым неразрешимость уравнения доказана, а вместе с тем доказана невозможность погружения $k_1=k_0(\sqrt{7})$ в поле (и алгебру Галуа) с группой $\mathfrak{G}_1$, при данном гомоморфизме $\mathfrak{G}$ на группу автоморфизмов k_1.

7°. Теперь легко опровергнуть и предположение Хассе.

Возьмем $k=k_0(\sqrt{7}, \sqrt{2}, \sqrt{-1})=k_1k_2$, где $k_2=k_0(\sqrt{2}, \sqrt{-1})$ и $\mathfrak{G}=\mathfrak{G}_1\mathfrak{G}_2$, где $\mathfrak{G}_1$ — группа из 6°, $\mathfrak{G}_2$ — группа поля k_2. Гомоморфизм $\mathfrak{G}$ на группу автоморфизмов k определен согласно 3°. В силу 3° $\mathfrak{G}$ согласно с k. В силу 4°, если бы k погружалось в K с группой $\mathfrak{G}$, то k_1 погружалось бы в K_1 с группой $\mathfrak{G}_1$, что невозможно в силу 6°. Ядром гомоморфизма $\mathfrak{G}$ на группу автоморфизмов k является циклическая группа 8-го порядка, и k содержит первообразный корень $\frac{1+\sqrt{-1}}{\sqrt{2}}$ 8-й степени из 1, так что дополнительные предположения Хассе выполнены.

Поступило
29 XII 1953

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] Б. Н. Делоне, Д. К. Фаддеев, Матем. сборн., 17, № 1 (1944). [2] H. Hasse, Math. Nachricht., 1, 1 (1948).