Теория Галуа 8: Теорема Абеля

Правила: Зачеты по листкам бывают двух типов: когда сданы все (или 1/3, или 2/3) задачи со звездочками, либо все (или 1/3, или 2/3) задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

Если сдана 1/3 задач с (*) и (!), студент получает $2t$ баллов, если 2/3 задач, $6t$ баллов, если все, кроме (максимум) двух – $10t$ баллов.

Если сдана 1/3 задач без звездочек и с (!), студент получает $2t$ баллов, если 2/3 задач, студент получает $6t$ баллов, если все, кроме (максимум) трех – $10t$ баллов.

Эти виды оценок не складываются, то есть больше $10t$ за листочек получить нельзя.

Коэффициент t равен 1.5, если задачи сданы не позже, чем через 20 дней после выдачи, 1, если между 20 и 35 днями, и 0.7, если позже.

Результаты сдачи записываются на листке ведомости, которая выдается студенту, и ее надо хранить до получения окончательных оценок по курсу.

8.1. Разрешимые группы

Задача 8.1. Пусть задан гомоморфизм $G_2 \xrightarrow{\phi} \operatorname{Aut}(G_1)$. Определим на множестве пар $(g_1, g_2) \in G_1 \times G_2$ следующую операцию:

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1\phi(g_2)h_1, g_2h_2).$$

Докажите, что получится группа.

Определение 8.1. Эта группа называется **полупрямым**, или **скрученным** произведением G_1 и G_2 и обозначается $G_1 \rtimes G_2$.

Задача 8.2. В условиях предыдущей задачи докажите, что $(G_1, 1)$ задает нормальную подгруппу в G, а фактор по этой подгруппе изоморфен G_2.

Задача 8.3. Опишите группу S_3 как скрученное произведение двух абелевых групп.

Задача 8.4. Опишите диэдральную группу (группу симметрий правильного многоугольника на плоскости) как скрученное произведение двух абелевых групп.

Задача 8.5 (*). Группой Клейна называется группа кватернионов вида $\pm 1, \pm I, \pm J, \pm K$, с естественной операцией умножения. Можно ли получить группу Клейна как скрученное произведение двух абелевых групп?

Задача 8.6 (!). Пусть $1 \longrightarrow G_1 \longrightarrow G \xrightarrow{\phi} G_2 \longrightarrow 1$ – расширение групп. Предположим, что задан гомоморфизм $G \xrightarrow{\psi} G_2$, такой, что $\psi \circ \phi$ – тождественный автоморфизм G_2 (в такой ситуации говорится, что ϕ **допускает сечение**). Докажите, что G можно получить как скрученное произведение $G_1 \rtimes G_2$.

Определение 8.2. Группа G называется **разрешимой**, если существует последовательность $1 = G_n \subset G_{n-1} \subset \cdots \subset G_0 = G$ нормальных подгрупп, причем все G_i/G_{i-1} абелевы.

Задача 8.7. Докажите, что подгруппа разрешимой группы разрешима.

Задача 8.8. Докажите, что симметрическая группа S_3 разрешима.

Задача 8.9. Докажите, что симметрическая группа S_4 разрешима.

Задача 8.10. Докажите, что группа Клейна $\{\pm 1, \pm I, \pm J, \pm K\}$ разрешима.

Задача 8.11. Пусть G_0 – группа, G_1 – ее коммутант, $G_2 = [G_1, G_1]$ – коммутант коммутанта, и так далее, $G_i = [G_{i-1}, G_{i-1}]$. Докажите, что G_0 разрешима тогда и только тогда, когда на каком-то шаге мы получим $G_n = 1$.

Определение 8.3. Пусть G – группа, LG_1 – ее коммутант, $LG_2 = [G, LG_1]$, $LG_3 = [G, LG_2]$, и так далее. Эта последовательность подгрупп называется **нижним центральным рядом**. Группа, у которой нижний центральный ряд заканчивается группой $LG_n = \{1\}$, называется **нильпотентной**.

Задача 8.12. Докажите, что любая нильпотентная группа разрешима. Приведите пример разрешимой группы, которая не нильпотентна.

Определение 8.4. Обозначим за $Z(G)$ центр группы G. Если $H \subset G$ нормальная подгруппа, обозначим за $Z_H(G)$ все элементы G, которые переходят в $Z(G/H)$ при естественном гомоморфизме $G \longrightarrow G/H$. **Верхний центральный ряд** группы G есть $UG_0 = Z(G)$, $UG_1 = Z_{UG_0}(G)$, $UG_2 = Z_{UG_1}(G)$, и так далее.

Задача 8.13 (**). Докажите, что нижний центральный ряд нильпотентной группы имеет такую же длину, как и ее верхний центральный ряд.

Определение 8.5. Пусть $t, x \in G$ – элементы группы. Элемент вида xtx^{-1} обозначается t^x. Соответствующая операция называется **сопряжением**, **скруткой**, или **подкруткой на** x. Отображение $x \longrightarrow t^x$ есть (очевидно) автоморфизм группы. Такой автоморфизм называется **внутренним**.

Задача 8.14. Пусть $g_1, g_2 \in S_n$ элементы группы перестановок, разложение которых на циклы имеет одинаковую длину. Докажите, что g_1 можно перевести в g_2 внутренним автоморфизмом.

Задача 8.15 (!). Пусть $g_1, g_2 \in A_n$ элементы группы четных перестановок, разложение которых на непересекающиеся циклы имеет одинаковую длину. Всегда ли g_1 можно перевести в g_2 внутренним автоморфизмом?

Задача 8.16. Пусть t – элемент группы G. такой, что множество

$$\{x \in G \ \mid \ \exists g \in G \text{ такой, что } x = t^g t^{-1}\}$$

порождает G. Докажите, что G не разрешима.

Задача 8.17 (!). Докажите, что группа четных подстановок A_n, $n \geqslant 5$ неразрешима.

Указание. Воспользуйтесь предыдущей задачей, взяв $t = (123)$.

Задача 8.18. Докажите, что группа движений $\mathbb{R}^3$ неразрешима.

Указание. Постройте изоморфизм между A_5 и группой поворотов икосаэдра, и воспользуйтесь предыдущей задачей.

Задача 8.19. Пусть G – группа порядка p^n. Докажите, что центр G содержит больше одного элемента.

Указание. Рассмотрим действие G на себе автоморфизмами. Порядок G равен сумме мощностей классов вида x^G, где x^G есть совокупность всех элементов вида x^y, $y \in G$. Докажите сначала, что если x не лежит в центре, то порядок x^G делится на p. Выведите $|G| = 1 + \sum |y_i^G|$, причем если у G нет центра, все $|y_i^G|$ делятся на p.

Задача 8.20 (!). Пусть G – группа порядка p^n. Докажите, что G нильпотентна.

Замечание 8.1. Если вы хотите применить теорему Силова, пожалуйста, изучите и запомните ее доказательство.

Задача 8.21. Пусть G – группа порядка p^2, p простое. Докажите, что G абелева.

Задача 8.22. Приведите пример неабелевой группы порядка p^3, p – любое простое число.

Задача 8.23. Рассмотрим множество S верхнетреугольных матриц $n \times n$ с единицей на диагонали над полем k. Докажите, что такие матрицы образуют подгруппу в $GL(n, k)$. Докажите, что эта группа разрешима. Найдите ее порядок для $k = \mathbb{Z}/p\mathbb{Z}$.

8.2. Теорема Абеля

Теорема Абеля утверждает, что общий многочлен пятой степени неразрешим в радикалах; иначе говоря, решение общего уравнения пятой степени нельзя выразить посредством алгебраических операций (умножения, сложения, деления) и операции извлечения корня n-й степени. В этом разделе я приведу пример уравнения, неразрешимого в радикалах.

Задача 8.24. Пусть $[K : k]$ – расширение Галуа. Докажите, что подгруппа $G' \subset \operatorname{Gal}([K : k])$ нормальна тогда и только тогда, когда $[K^{G'} : k]$ – расширение Галуа.

Указание. Из основной теоремы теории Галуа сразу следует это.

Задача 8.25. Пусть $G' \subset \operatorname{Gal}([K : k])$ – нормальная подгруппа. Докажите, что группа $\operatorname{Gal}([K^{G'} : k])$ изоморфна фактору $\operatorname{Gal}([K : k])/G'$.

Задача 8.26 (!). Пусть k – поле характеристики 0, а $[K : k]$ – поле разложения многочлена $t^n - a$. Докажите, что группа Галуа $\operatorname{Gal}([K : k])$ разрешима.

Указание. Если k содержит корни n-й степени из 1, мы все доказали. Если нет, докажите, что K их содержит. Рассмотрите промежуточное расширение K', полученное добавлением этих корней к k, и докажите, что $[K : K']$ и $[K' : k]$ – расширения Галуа с абелевыми группами Галуа.

Задача 8.27 (!). Пусть группа Галуа $[K : k]$ разрешима, а k содержит все корни из единицы. Докажите, что $[K : k]$ можно представить в виде последовательности расширений Галуа $k = K_0 \subset K_1 \subset ... \subset K_n = K$, таким образом, что для каждого i, $\operatorname{Gal}([K_i : K_{i-1}])$ - циклическая группа.

Задача 8.28 (!). (теорема Галуа) Докажите, что расширение Галуа $[K : k]$ порождается последовательным добавлением решений уравнения $t^n - a = 0$ тогда и только тогда, когда группа $\operatorname{Gal}[K : k]$ разрешима.

Замечание 8.2. Пусть $P(t) \in k[t]$ – многочлен. **Группой Галуа** P называется группа Галуа его поля разложения. Теорема Галуа утверждает, что уравнение $P(t) = 0$ разрешимо в радикалах тогда и только тогда, когда группа Галуа $P(t)$ разрешима.

Определение 8.6. Пусть группа G действует на множестве Σ. Действие называется **транзитивным**, если любой $x \in \Sigma$ можно перевести в любой $y \in \Sigma$ применением подходящего $g \in G$.

Задача 8.29. Пусть $G \subset S_n$, – подгруппа, содержащая транспозицию и действующая транзитивно на $\{1, 2, 3, \dots, n\}$.

а. (!) Докажите, что $G = S_n$ для $n = 5$.

б. (*) Докажите, что $G = S_n$ для любого простого n.

Задача 8.30. Пусть $P \in k[t]$ – неприводимый многочлен, $\xi_1, \dots, \xi_n$ – его корни, и пусть все эти корни различны. Докажите, что группа Галуа P действует на $\{\xi_1, \dots, \xi_n\}$ транзитивно.

Указание. Разобьем $\{\xi_1, \dots, \xi_n\}$ на смежные классы по действию $\operatorname{Gal}(P)$. Пусть S такой класс. Докажите, что полином $\prod_{\xi_i \in S}(t - \xi_i)$ имеет коэффициенты в k, и делит P.

Задача 8.31 (!). Пусть $P \in \mathbb{Q}[t]$ – неприводимый многочлен степени n, у которого ровно $n - 2$ вещественных корня. Докажите, что его группа Галуа равна S_n.

Указание. Докажите, что $\operatorname{Gal}(P)$ транзитивно действует на корнях P, а комплексное сопряжение сохраняет поле разложения P и действует на множестве корней как транспозиция.

Задача 8.32. (теорема Эйзенштейна) Пусть $Q = t^n + t^{n-1}a_{n-1} + t^{n-2}a_{n-2} + \dots + a_0$ – такой многочлен с целыми коэффициентами, что все a_i делят заданное простое число p, а $a_0 \not\vdots\, p^2$. Докажите, что Q неприводим над $\mathbb{Q}$.

Задача 8.33. Докажите, что $Q(t) = x^5 - 10x + 5$ – неприводимый (над $\mathbb{Q}$) многочлен, у которого ровно 3 вещественных корня. Выведите из этого, что его группа Галуа это S_5.

Задача 8.34 (!). Докажите, что уравнение $x^5 - 10x + 5 = 0$ неразрешимо в радикалах.

Задача 8.35 (*). Постройте расширение Галуа $[K : \mathbb{Q}]$ с группой Галуа $(\mathbb{Z}/5\mathbb{Z})^2$.

Задача 8.36 (**). Пусть n – число вершин правильного n-угольника в $\mathbb{R}^2$, который можно построить циркулем и линейкой. Докажите, что каждый простой делитель n имеет вид $2^k + 1$.

Задача 8.37 (*). Докажите, что для любого n существует расширение Галуа $[K : \mathbb{Q}]$ с группой Галуа S_n (симметрической группой).

Задача 8.38 (*). Пусть G – конечная группа. Постройте конечное расширение $[K : k]$ с группой Галуа G.

Задача 8.39 (*). Пусть $[K : \mathbb{Q}]$ – расширение Галуа с группой Галуа $(\mathbb{Z}/2\mathbb{Z})^2$. Докажите, что $K = \mathbb{Q}[\alpha, \beta]$, где $\alpha = \sqrt{x}$, $\beta = \sqrt{y}$, а x, y – взаимно простые целые числа, или найдите контрпример.

Задача 8.40 (**). Пусть $[K : \mathbb{Q}]$ – конечное расширение, а Z – множество всех корней из единицы, лежащих в K. Докажите, что Z конечно.