ГЛАВА

ТЕОРИЯ ГАЛУА И ТФКП

4. Неподвижные точки действия конечной группы и ее подгрупп

Линейное пространство над всяким содержит значительно больше чем любое его собственное подпространство. Поэтому пространство не представляется в виде объединения относительно небольшого (меньшего, чем число элементов в поле) числа подпростванств. Докажем два утверждения такого рода.

Лемма 1. *Линейное пространство над полем комплексных чисел не может быт' представлено в виде обьединения счетного числа своилх собственных аффинных подпространств. То же самое верно для линейного пространства над полем вещественных чисел.*

Доказательство. Объеднение счетного числа подпространств имеет нулевую меру в объемлющем пространстве.

Пусть теперь V — аффинное пространство (может быть, бесконечномерное) над полем характеристики нуль.

Лемма 2. *Пространство V не может быть представлено в виде обьединения конечного числа своих собственных аффинных подпространств.*

Доказательство. Индукция по числу аффинных подпространств. Пусть утверждение доказано для объединения менее чем n собственных аффинных подпространств. Допустим, что пространство V представимо в виде объеднинения n собственных аффинных подпространств $V_1, \ldots, V_n$. Рассмотрим любую собственную аффинную гиперплоскость $\hat{V}$ в пространстве V, содержащую первое из этих подпространств V_1. Пространство V является объединением бесконечного семейства непересекающихся аффинных гиперплоскостей, параллельных гиперплоскости $\hat{V}$. Не более чем $(n-1)$ гиперплоскость из этого семейства совпадает с одним из пространств $V_2, \ldots, V_n$. И лишь одна гиперплоскость из этого семейства содержит пространство V_1. Возьмем любую другую гиперплоскость из семейства. К этой гиперплоскости и ее пересечениям с аффинными плоскостями $V_2, \ldots, V_n$ применимо индукционное предположение. Что и доказывает лемму.

Утверждение 1. *Пусть на линейном пространстве над полем комплексных чисел действует не более чем счетная группа линейных преобразований. Тогда найдется вектор a, на орбите которого группа действует свободно. То же самое верно для пространства над полем вещественных чисел.*

Typeset by $\mathcal{AMS}$-TEX

Утверждение 2. *Пусть на линейном пространстве V над полем нулевой характеристики действует конечная группа линейных преобразований. Тогда найдется вектор a, на орбите которого группа действует свободно.*

Доказательство. Множество неподвижных точек линейного преобразования является линейным подпространством. Для нетождественного линейного преобразования это подпространство является собственным. Поэтому утверждение 1 вытекает из леммы 1, а утверждение 2 вытекает из леммы 2. Действительно, в качестве вектора a достаточно взять любой вектор, не принадлежащий объединению неподвижных подпространств нетривиальных преобразований группы.

Для подгруппы G_0 конечной группы G линейных преобразований может не найтись вектора a, неподвижного лишь для преобразования из подгруппы G_0. В качестве примера достаточно рассмотреть нетривиальное линейное действие циклической группы на прямой. Циклическая группа не простого порядка имеет нетривиальные подгруппы, однако,все ненулевые вектора двигаются при действии любого неединичного элемента циклической группы. Таким образом, для существования вектора a, неподвижного лишь для преобразований из подгруппы G_0, нужны дополнительные ограничения. Опишем одно из возможных ограничений такого рода. Но сначала одно определение.

Пусть X — множество, и L — некоторое линейное пространство функций на X со значениями в векторном пространстве над полем рациональных чисел. Скажем, что пространство функций L разделяет два конечных подмножества X_1 и X_2 множества X, содержащих равное число элементов, если найдется функция f из L, для которой выполняется неравенство

$$\sum_{x\in X_1} f(x) \neq \sum_{x\in X_2} f(x).$$

Пространство функций L k-разделяет множество X, если оно разделяет любые два различных подмножества множества X, содержащие по k элементов.

Утверждение 3. *Пусть на линейном пространстве V действует конечная группа линейных преобразований G, и пусть G_0 — подгруппа группы G, содержащая k элементов. Рассмотрим линейное пространство L всех функций на V, принимающих значения в пространстве V и коммутирующих с действием группы G. Допустим, что L k-разделяет пространство V. Тогда существует вектор $x \in V$, который является неподвижным лишь для преобразований подгруппы G_0.*

Доказательство. Под действием подгруппы $G_0 \in G$ пространство V распадается на непересекающиеся орбиты. Рассмотрим оператор π, сопоставляющий каждой функции f из пространства L функцию $\pi(f)$, определенную формулой

$$\pi f(y) = \frac{1}{k} \sum_{g\in G_0} f(g(y)).$$

Согласно утверждению 2 найдется вектор $a \in V$, на орбите которого группа G действует свободно. Пространство L разделяет различные орбиты $O_1, \ldots, O_m$ относительно действия подгруппы G_0, лежащие в орбите

элемента a относительно действия группы G. Действительно, все эти орбиты содержат ровно по k элементов (т.к. на орбите элемента a группа G действует свободно), а функции пространства L k-разделяют пространство V. Поэтому функции f из пространства L, для которых функции $\pi(f)$ совпадают на двух разных орбитах O_i и O_j, $i \neq j$, образуют собственное линейное подпространство $L_{i,j}$ в пространстве L. Согласно лемме 2 подпространства $L_{i,j}$ при $1 \leq i < j \leq n$ не покрывают всего пространства L. Следовательно, существует функция $\varphi \in L$, для которой функция $\pi(\varphi)$ принимает различные значения на всех орбитах $O_1, \ldots, O_m$ элемента a. Ее значение $x = \pi(\varphi(a))$ на элементе a удовлетворяет условию утверждения 2.

В теории Галуа важную роль играет следующая

Теорема. *Пусть P — поле характеристики нуль, и G — некоторая конечная группа его автоморфизмов. Тогда для всякой подгруппы G_0 группы G существует элемент x, остающийся неподвижным при действии подгруппы G_0, но двигающийся при действии любого элемента группы G, не лежащего в подгруппе G_0.*

Доказательство. Покажем, что теорема является следствием утверждения 3. Поле P можно рассматривать как линейное пространство над полем рациональных чисел. Каждому полиному $p(x) = \sum a_l x^l$ с рациональными коэффициентами соответствует отображение поля P в себя, сопоставляющее каждой точке $x \in P$ точку $p(x)$.

Лемма 3. *Пространство L отображений поля P в себя соответствующих полиномам с рациональными коэффициентами k-разделяет поле P для любого натурального k.*

Доказательство. Действительно, пусть X_1 — подмножество поля P, содержащее k элементов. Суммы значений функций x^l по множеству X_1 при $l = 1, \ldots, k$ являются симметрическими функциями Ньютона точек множества X_1. Основные симметрические функции восстанавливаются по симметрическим функциям Ньютона. Следовательно, зная функции Ньютона, мы можем восстановить уравнение $x^k + a_1 x^{k-1} + \cdots + a_n = 0$, корнями которого являются точки множества X_1. Поэтому пространство L k-разделяет поле P.

Теперь теорема сводится к утверждению 3. Действительно, очевидно, что отображение поля P в себя, соответствующее любому полиному с рациональными коэффициентами коммутирует со всяким автоморфизмом поля P.