Лекции по курсу "Теория Галуа"

Белоусов Григорий Николаевич

Оглавление

Мы будем придерживаться следующих обозначений.

Обозначения 0.1. Мы будем придерживаться следующих обозначений:

- $\mathbb{N}$ — множество натуральных чисел.
- $\mathbb{Z}$ — множество целых чисел.
- $\mathbb{Q}$ — множество рациональных чисел.
- $\mathbb{R}$ — множество вещественных чисел.
- $\forall$ — для любого.
- $\exists$ — существует.
- $\in$ — принадлежит.
- ∞ — бесконечность.

Глава 1

Группы

1. Коммутант группы

Пусть G — группа. *Коммутатором* двух элементов $a, b \in G$ называется произведение

$$[a, b] = aba^{-1}b^{-1}.$$

Непосредственно из определения следуют следующие свойства

(1) $ab = [a, b]ba$;
(2) $ab = ba[a^{-1}, b^{-1}]$;
(3) $[a, b]^{-1} = [b, a]$;
(4) $[a, b] = e$ тогда и только тогда, когда $ab = ba$.

Определение 1.1. *Коммутантом* группы G называется подгруппа K, порожденная всеми коммутантами. Обозначается $[G, G] = K$.

Теорема 1.2. *Пусть H — нормальная подгруппа в группе G. Тогда $[H, H] \triangleleft G$.*

Доказательство. Заметим, что

$$g[a, b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) =$$
$$(gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1}, gbg^{-1}].$$

Пусть $h \in [H, H]$ и $g \in G$. Тогда

$$h = [h_1, h'_1][h_2, h'_2] \cdots [h_n, h'_n],$$

где все $h_i, h'_i \in H$. Следовательно,

$$ghg^{-1} = g[h_1, h'_1][h_2, h'_2] \cdots [h_n, h'_n]g^{-1} =$$
$$= (g[h_1, h'_1]g^{-1})(g[h_2, h'_2]g^{-1}) \cdots (g[h_n, h'_n]g^{-1}) =$$
$$= [gh_1g^{-1}, gh'_1g^{-1}][gh_2g^{-1}, gh'_2g^{-1}] \cdots [gh_ng^{-1}, gh'_ng^{-1}].$$

Поскольку H — нормальная подгруппа в группе G, то все $gh_ig^{-1}, gh'_ig^{-1} \in H$. Отсюда, $g^{-1}hg \in [H, H]$ □

Следствие 1.3. *Коммутант K группы G является нормальной подгруппой.*

Теорема 1.4. *Пусть K — коммутант группы G. Тогда группа G/K абелева.*

Доказательство. Действительно,
$$(aK)(bK) = abK = ba[a^{-1}, b^{-1}]K = baK = (bK)(aK).$$
□

Теорема 1.5. *Пусть H — нормальная подгруппа группы G, и пусть G/H абелева. Тогда $K \subset H$, где K — коммутант группы G.*

Доказательство. Если G/H абелева, то $abH = baH$, или, поскольку H — нормальная подгруппа, $Hab = Hba$. Следовательно, существует $h \in H$ такой, что $ab = hba$, т.е. $h = aba^{-1}b^{-1} = [a, b]$. □

2. Разрешимые и нильпотентные группы

Определение 1.6. Последовательность подгрупп
$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$$
называется *рядом подгрупп*. Если для любого i $G_i \triangleleft G$, то ряд называется *нормальным*. Группа G называется *разрешимой*, если существует нормальный ряд подгрупп
$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$$
такой, что для любого i, G_i/G_{i+1} — абелева группа.

Пусть $K_0 = G$, $K_1 = [K_0, K_0]$, $K_2 = [K_1, K_1]$ и т.д. Тогда имеет место следующая теорема.

Теорема 1.7. *Группа G разрешима тогда и только тогда, когда существует n такое, что $K_n = \{e\}$.*

Доказательство. Предположим, что $K_n = \{e\}$. Из теорем 1.2 1.4 следует, что $G = K_0 \supset K_1 \supset K_2 \supset \cdots \supset K_n = \{e\}$ — нормальный ряд подгрупп, и K_i/K_{i+1} — абелева группа. Следовательно, в одну сторну утверждение доказано. Предположим, что существует нормальный ряд подгрупп
$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m = \{e\},$$
и для любого i, G_i/G_{i+1} — абелева группа. Из теоремы 1.5 следует, что $K_1 \subset G_1$. Докажем по индукции, что $K_i \subset G_i$. Предположим, что $K_{i-1} \subset G_{i-1}$. Тогда $[K_{i-1}, K_{i-1}] \subset [G_{i-1}, G_{i-1}]$. С другой стороны, по теореме 1.5 $[G_{i-1}, G_{i-1}] \subset G_i$. Отсюда, $K_i \subset G_i$. □

Пример 1.8. Рассмотрим группу S_n $(n \geq 5)$. Заметим, что $[\sigma_1, \sigma_2] = \sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}$ — четная перестановка. Следовательно, $[S_n, S_n] \subset A_n$. С другой стороны,

$$[(ij), (jk)] = (ij)(jk)(ij)(jk) = (ikj).$$

Следовательно, любые циклы длины три лежат в $[S_n, S_n]$. Тогда $[S_n, S_n] = A_n$. Теперь посчитаем коммутант A_n. Рассмотрим перестановки $(ij)(kl)$ и $(ij)(km)$. Получаем

$$[(ij)(kl), (ij)(km)] = (ij)(kl)(ij)(km)(ij)(kl)(ij)(km) = (klm).$$

Следовательно, $[A_n, A_n] = A_n$. Таким образом, группы S_n и A_n не разрешимы при $n \geq 5$.

Пример 1.9. Рассмотрим группу S_4. Аналогично, $[S_4, S_4] = A_4$. Теперь посчитаем коммутант A_4. Для этого рассмотрим подгруппу

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}.$$

Заметим, что V_4 — нормальная подгруппа в A_4, и $A_4/V_4 \simeq \mathbb{Z}_3$, т.е. A_4/V_4 — абелева группа. Согласно теореме 1.5 $[A_4, A_4] \subset V_4$. С другой стороны,

$$[(ijk), (ijl)] = (ijk)(ijl)(ikj)(ilj) = (ij)(kl).$$

Таким образом, $[A_4, A_4] = V_4$. Поскольку V_4 — абелева группа, то S_4 и A_4 разрешимы.

Определение 1.10. Пусть G — группа. Тогда множество $Z(G) := \{a \in G \mid ag = ga \text{ для всех } g \in G\}$ называется *центром* группы G.

Очевидно, что центр группы является нормальной подгруппой.

Определение 1.11. *Центральным рядом подгрупп* называется нормальный ряд подгрупп

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$$

такой, что $G_i/G_{i+1} \subset Z(G/G_{i+1})$. Группа, обладающая центральным рядом подгрупп, называется *нильпотентной группой.*

Поскольку центр — абелева группа, то нильпотентная группа является разрешимой. Обратное неверно (см. группу S_4).

Определение 1.12. Группа G называется *конечной p-группой*, если p — простое и $|G| = p^n$.

Лемма 1.13. *Пусть G — конечная p-группа. Тогда $Z(G) \neq \{e\}$.*

Доказательство. Пусть группа G действует на себе посредством сопряжения. Тогда $|G| = |Z(G)| + \sum |\operatorname{Orb}(g_i)|$, где все $|\operatorname{Orb}(g_i)| > 1$. Заметим, что $|\operatorname{Orb}(g_i)|$ является делителем порядка группы G. Следовательно, $|\operatorname{Orb}(g_i)|$ делится на p. Отсюда, $|Z(G)|$ делится на p. Следовательно, $Z(G) \neq \{e\}$. □

Теорема 1.14. *Любая конечная p-группа нильпотентна.*

Доказательство. Пусть G — конечная p-группа. Согласно лемме 1.13, $Z(G) \neq \{e\}$. Пусть $G_1 = Z(G)$. Рассмотрим $G_1' = G/G_1$. Тогда G_1' — также конечная p-группа. Следовательно, $Z(G_1') \neq \{e\}$. Пусть G_2 — прообраз $Z(G_1')$ при естественном гомоморфизме $f\colon G \to G/G_1$. Заметим, что G_2 — нормальная подгруппа в G. Действительно, пусть $h \in G_2$, $g \in G$. Тогда

$$f(ghg^{-1}) = f(g)f(h)(f(g))^{-1} = f(h)f(g)(f(g))^{-1} = f(h).$$

Следовательно, $ghg^{-1} \in G_2$. Рассмотрим $G_2' = G/G_2$. Тогда G_2' — также конечная p-группа. Следовательно, $Z(G_2') \neq \{e\}$. Пусть G_3 — прообраз $Z(G_2')$ при естественном гомоморфизме $f\colon G \to G/G_2$. Аналогично, G_3 — нормальная подгруппа в G. Продолжая эти действия, мы получим искомый центральный ряд. □

3. Теоремы Силова

Теорема 1.15 (1-я теорема Силова). *Пусть G — произвольная конечная группа и $|G| = mp^k$, где $(m,p) = 1$. Тогда существует подгруппа $H \subset G$ такая, что $|H| = p^k$ (такие подгруппы называются* силовскими подгруппами*).*

Доказательство. Докажем утверждение индукцией по порядку группы. Предположим, утверждение верно для всех порядков меньших $n = mp^k$. Рассмотрим два случая:

1) $p \mid |Z(G)|$. Тогда существует подгруппа $H \subset Z(G)$ такая, что $|H| = p^s$. Заметим, что $H \lhd G$. Пусть $G' = G/H$. Тогда, по предположению индукции, в G' существует подгруппа A порядка p^{k-s}. Пусть B — прообраз A в G. Тогда B — подгруппа G и $|A| = |B|/|H|$. Отсюда, $|B| = p^k$.

2) Порядок центра $|Z(G)|$ не делится на p. Рассмотрим разбиение группы G на классы сопряженности. Мы получим

$$|G| = |Z(G)| + \sum |\operatorname{Orb}(g_i)|.$$

Поскольку $|Z(G)|$ не делится на p, то существует $\mathrm{Orb}(g_i)$ такая, что $|\mathrm{Orb}(g_i)|$ не делится на p тогда $|\mathrm{St}(g_i)| = lp^k$, где $l < m$. Следовательно, по предположению индукции, существует подгруппа $H \subset \mathrm{St}(g) \subset G$ такая, что $|H| = p^k$. $\square$

Теорема 1.16 (2-я теорема Силова). *Пусть G — конечная группа и $|G| = mp^k$, где $(m,p) = 1$. Тогда любая p-подгруппа H содержится в силовской подгруппе S и все силовские подгруппы сопряжены.*

Доказательство. Согласно теореме 1.15 существует силовская p-подгруппа S_1. Рассмотрим полигон $\{S_1, g_1S_1, \dots\}$ левых смежных классов. Пусть H действует на нем умножением (т.е. $(h, gS_1) \mapsto hgS_1$). Все орбиты состоят либо из одного элемента, либо число элементов делится на p. Поскольку число смежных классов по подгруппе S_1 равно m и $(m,p) = 1$, то существует одноэлементная орбита g_iS_1. Таким образом $Hg_iS_1 = g_iS_1$. Отсюда, $H \subset g_iS_1g_i^{-1}$. Заметим, что $g_iS_1g_i^{-1}$ — силовская подгруппа. Таким образом, первое утверждение теоремы доказано. Возьмем в качестве H силовскую подгруппу, мы получим второе утверждение теоремы. $\square$

Замечание 1.17. Из 2-й теоремы Силова следует, что силовская p-подгруппа нормальна тогда и только тогда, когда она единственна.

Теорема 1.18 (3-я теорема Силова). *Пусть G — произвольная группа и $|G| = mp^k$, где $(m,p) = 1$. Пусть l — число силовских подгрупп порядка p^k. Тогда l является делителем m и $l = 1 + qp$.*

Доказательство. Пусть $\{S_1, \dots, S_l\}$ — множество силовских подгрупп. Пусть группа G действует на $\{S_1, \dots, S_l\}$ сопряжением. Тогда $\{S_1, \dots, S_l\}$ образуют одну орбиту. Отсюда, l является делителем порядка группы G. Теперь, пусть S_1 действует на $\{S_1, \dots, S_l\}$ сопряжением. Заметим, что у этого действия только один неподвижный элемент, сама S_1. Действительно, предположим, что S_2 — тоже неподвижный элемент. Тогда S_1 лежит в нормализаторе S_2. Рассмотрим S_1S_2. Заметим, что S_2 — нормальная подгруппа в S_1S_2. Следовательно,

$$S_1S_2/S_2 \simeq S_1/(S_1 \cap S_2).$$

Отсюда, S_1S_2 — конечная p-группа. Противоречие. Следовательно, множество $\{S_1, \dots, S_l\}$ разбивается на одну орбиту из одного элемента и некоторого числа орбит, порядок которых делится на p. Отсюда, $l = 1 + qp$. $\square$

4. Простые группы

Определение 1.19. Группа G называется *простой*, если в ней нет нормальных подгрупп, кроме тривиальной (состоящей из единицы) и самой группы.

Теорема 1.20. *Пусть G — конечная группа и $|G| = pq$, где p и q — простые числа. Тогда группа G не простая.*

Доказательство. Пусть $q > p$. Рассмотрим силовские q-подгруппы. Согласно 3-й теореме Силова их число делит pq и дает, при делении на q, в остатке 1. Следовательно, такая подгруппа одна. По второй теореме Силова она нормальна. □

Теорема 1.21. *Пусть G — конечная группа и $|G| = p^2q$, где p и q — простые числа. Тогда группа G не простая.*

Доказательство. Предположим $p > q$. Рассмотрим силовские p-подгруппы. Согласно 3-й теореме Силова их число делит p^2q и дает, при делении на p, в остатке 1. Следовательно, такая подгруппа одна. По второй теореме Силова она нормальна.

Предположим $q > p$. Рассмотрим силовские q-подгруппы. Согласно 3-й теореме Силова их число делит p^2q и дает, при делении на q, в остатке 1. Следовательно, такая подгруппа либо одна, либо таких подгрупп p^2. Если силовская q-подгруппа одна, то все доказано. Следовательно, мы можем предполагать, что существуют p^2 таких подгрупп. Заметим, что любая силовская q-подгруппа изоморфна $\mathbb{Z}_q$. Тогда любые две из них имеют тривиальное пересечение (т.е. пересекаются по единицы), и все их элементы, кроме единицы, имеют порядок q. Посчитаем число элементов порядка q в группе G, получаем $p^2(q-1) = p^2q - p^2$. С другой стороны силовская p-подгруппа состоит из p^2 элементов и не содержит элементы порядка q. Отсюда следует, что существует единственная силовская p-подгруппа. Тогда она нормальна. □

Теорема 1.22. *Пусть G — конечная группа и $|G| = pqr$, где p, q, r — простые числа. Тогда группа G не простая.*

Доказательство. Пусть $r > q > p$. Рассмотрим силовские r-подгруппы. Согласно 3-й теореме Силова их число делит pqr и дает, при делении на r, в остатке 1. Следовательно, такая подгруппа либо одна, либо таких подгрупп pq. Если силовская r-подгруппа одна, то все доказано. Следовательно, мы можем предполагать, что существуют pq таких подгрупп. Заметим, что любая силовская r-подгруппа изоморфна $\mathbb{Z}_r$. Тогда любые две из них имеют тривиальное пересечение (т.е. пересекаются по единицы), и все их элементы, кроме единицы, имеют порядок r. Посчитаем число элементов порядка r в группе G, получаем $pq(r-1) = pqr-pq$. Рассмотрим силовские q-подгруппы. Мы можем предполагать, что такая подгруппа не единственна. Согласно 3-й теореме Силова их, как минимум, r штук. Заметим, что каждая силовская q-подгруппа изоморфна $\mathbb{Z}_q$. Тогда все они имеют тривиальное пересечения. Аналогично, посчитаем число элементов порядка q. Получаем, что их, как минимум, $r(q-1)$. Суммируя число элементов порядка r и порядка q, получаем

$$pqr - pq + r(q-1) > pqr.$$

Противоречие. □

Теорема 1.23. *Группа A_n проста при $n \geq 5$.*

Сначала, докажем следующую лемму.

Лемма 1.24. *Пусть нормальная подгруппа H группы A_n содержит цикл дины три. Тогда $H = A_n$.*

Доказательство. Если $n = 3$, то утверждение очевидно. Пусть $n > 3$ и H содержит перестановку (ijk). Пусть $\sigma = (ij)(km)$, Тогда

$$\sigma(ijk)\sigma^{-1} = (ij)(km)(ijk)(ij)(km) = (imj).$$

Более того, $(ijk)(imj) = (imk)$. Отсюда легко видеть, что все циклы длины три содержаться в H. Следовательно, $H = A_n$. □

Теперь докажем теорему 1.23. Пусть H — нормальная подгруппа группы A_n. Пусть $\sigma \in H$ — элемент подгруппы H, содержащий минимальное количество номеров, при разложении в произведение циклов. Предположим, что σ содержит цикл, длины больше трех, т.е. $\sigma = (i_1 i_2 \cdots i_{n-3} i_{n-2} i_{n-1} i_n) \cdots$. Пусть $\tau = (i_{n-2} i_{n-1} i_n)$. Тогда

$$\sigma_1 = \tau\sigma\tau^{-1} = (i_{n-2} i_{n-1} i_n)(i_1 i_2 \cdots i_{n-3} i_{n-2} i_{n-1} i_n)(i_{n-2} i_n i_{n-1}) \cdots =$$

$$= (i_1 i_2 \cdots i_{n-3} i_{n-1} i_n i_{n-2}) \cdots .$$

С другой стороны,

$$\sigma^{-1}\sigma_1 = (i_1 i_n i_{n-1} \cdots i_3 i_2)(i_1 i_2 \cdots i_{n-3} i_{n-1} i_n i_{n-2}) \cdots$$

оставляет неподвижным номер i_{n-1}. Таким образом, мы можем считать, что σ состоит из циклов длины два и три. Предположим, что σ содержит цикл длины три. Возводя в квадрат мы можем считать, что σ состоит из циклов длины три. Предположим, что σ содержит два таких цикла, т.е. $\sigma = (ijk)(lmp)\cdots$. Пусть $\tau = (ij)(kl)$. Тогда

$$\sigma_1 = \tau\sigma\tau^{-1} = (ij)(kl)(ijk)(lmp)(ij)(kl)\cdots = (ilj)(kmp)\cdots .$$

С другой стороны,

$$\sigma_1\sigma^{-1} = (ilj)(kmp)(ikj)(lpm)\cdots$$

оставляет на месте номер p. Следовательно, σ содержит лишь один цикл длины три. Тогда по лемме 1.24 получаем, что $H = A_n$. Предположим, что σ состоит из циклов длины два (транспозиций). Поскольку σ четная, то σ состоит из четного числа транспозиций, т.е. $\sigma = (ij)(kl)\cdots$. Поскольку $n \geq 5$, рассмотрим $\tau = (ij)(km)$. Тогда

$$\sigma_1 = \tau\sigma\tau^{-1} = (ij)(km)((ij)(kl)\cdots)(ij)(km) = (ij)(lm)\cdots .$$

Отсюда,

$$\sigma\sigma_1 = ((ij)(kl)\cdots)((ij)(lm)\cdots)$$

оставляет на месте номера i, j. Противоречие.

5. Транзитивные и примитивные группы

Определение 1.25. Группа перестановок G множества M называется *транзитивной* над M, если в M существует элемент a такой, что для любого $x \in M$ существует $g \in G$ такое, что $x = ga$. Также говорят, что G действует *транзитивно* на M.

Утверждение 1.26. *Пусть группа G действует транзитивно на множестве M. Тогда для любых двух элементов $x, y \in M$ существует элемент $g \in G$ такой, что $gx = y$.*

Доказательство. Пусть $x = g_1 a$, $y = g_2 a$. Тогда

$$(g_2 g_1^{-1})x = g_2 a = y.$$

□

Если группа G действует не транзитивно на M, то множество M можно разбить на непересекающиеся множества M_α так, что группа G действует транзитивно на каждом множестве M_α. Это разбиение осуществляется по следующему принципу. Два элемента $x, y \in M$ относятся в одно подмножество тогда и только тогда, когда существует $g \in G$ такой, что $y = gx$. Это отношение рефлексивно, симметрично и транзитивно. Действительно,

(1) $x = gx$ при $g = e$ (рефлексивность);
(2) если $y = gx$, то $x = g^{-1}y$ (симметричность);
(3) если $y = g_1 x$ $z = g_2 y$, то $z = (g_2 g_1)x$ (транзитивность).

Определение 1.27. Разбиение множества M на непересекающиеся подмножества M_α называется *разбиением на блоки относительно* G, если для любого M_α и любого $g \in G$ существует M_β такое, что $M_\beta = gM_\alpha$. Очевидно, что всегда существует два тривиальных разбиения — на одноэлементные блоки, и на единственный блок в виде всего множества M. Если нетривиального разбиения на блоки не существует, то группа G называется *примитивной.* В противном случае группа называется *импримитивной.* Множества M_α называются *областями импримитивности.*

Теорема 1.28. *Пусть G действует транзитивно на множестве M, состоящим из n элементов, и пусть задано неизмельчимое разбиение M на блоки. Тогда стабилизатор любого блока M' является подгруппой группы G, примитивно действующей на M'.*

Доказательство. Напомним, что
$$\operatorname{St} M' = \{g \mid g \in G, x \in M', gx \in M'\}.$$
Очевидно, что H — подгруппа. Предположим, что она не примитивна, т.е. существует нетривиальное разбиение M' на блоки $M'_1, \ldots, M'_k$. Пусть $g_1, \ldots, g_l$ — элементы смежных классов $g_1H, \ldots, g_lH$. Тогда исходное разбиение M можно измельчить до разбиения $g_iM'_j$. □

Теорема 1.29. *Пусть G действует транзитивно на множестве M. Пусть $H = \operatorname{St}(x)$, $x \in M$. Тогда если G импримитивна, то существует подгруппа $K \neq H, G$ такая, что $H \subset K \subset G$. Обратно, если существует такая группа, то G импримитивна.*

Доказательство. Предположим, что G импримитивна. Тогда она разбивается на нетривиальные блоки $M_1, M_2, \ldots$. Пусть $x \in M_1$ и $K = \operatorname{St}(M_1)$. Тогда $H \subset K \subset G$. Поскольку G действует транзитивно на множестве M, то существует элемент $g_1 \in G$ такой, что g_1 переводит x в другой элемент множества M_1. Тогда $g_1 \in K$, $g_1 \notin H$. С другой стороны, существует элемент $g_2 \in G$ такой, что g_2 переводит M_1 в M_2, т.е. $g_2 \notin K$ и $K \neq G$.

Обратно, пусть существует подгруппа K такая, что $H \subset K \subset G$ и $K \neq H, G$. Пусть M_1 — орбита элемента x при действии подгруппы K. Поскольку $K \neq H$, то M_1 состоит не только из элемента x. Рассмотрим левые смежные классы по подгруппе K, $g_1K, g_2K \ldots$. Пусть $M_i = g_iM_1$. Докажем, что эти множества не пересекаются. Предположим, что $y \in M_i \cap M_j$. Тогда $y = g_ix_1 = g_jx_2$, где $x_1, x_2 \in M_1$. Следовательно, $y = g_ih_1x = g_jh_2x$, где $h_1, h_2 \in K$. Тогда $h_2^{-1}g_j^{-1}g_ih_1x = x$. Отсюда, $h_2^{-1}g_j^{-1}g_ih_1 \in H \subset K$. Следовательно,

$g_j^{-1}g_i \in K$. Тогда $g_iK = g_jK$. Противоречие. Таким образом, мы получили разбиение на нетривиальные блоки. Следовательно, группа G импримитивна. $\square$

Следствие 1.30. *Для того, чтобы группа G была примитивной необходимо и достаточно, чтобы стабилизатор точки был максимальной подгруппой.*

Теорема 1.31. *Пусть G действует примитивно на множестве M. Пусть H — нормальная подгруппа в G. Тогда либо H действует транзитивно на M, либо H действует тривиально (т.е. оставляет все элементы M на месте).*

Доказательство. Предположим, что H действует нетранзитивно. Тогда множество M можно разбить на множества $M_1, M_2, \ldots$ орбит группы H. Докажем, что любой элемент $g \in G$ переводит одну орбиту в другую. Пусть $x \in M_1$. Предположим, что $gx = y \in M_2$. Рассмотрим $z = h_1y$, где $h_1 \in H$. Тогда

$$t = g^{-1}z = g^{-1}h_1y = g^{-1}h_1gx = h_2x,$$

где $h_2 \in H$. Следовательно, $t \in M_1$ и $gt = z$. Таким образом, мы получили разбиение M на нетривиальные блоки. $\square$

Глава 2

Теория полей

1. Конечные и алгебраические расширения полей

Пусть E, k — два поля, причем $k \subset E$. Тогда поле E называется *расширением* поля k.

Определение 2.1. Расширение E поля k называется *конечным* (*бесконечным*), если E конечномерно (бесконечномерно), как линейное пространства над k. Другими словами, E конечно над k, если существуют $a_1, a_2, \ldots, a_n \in E$ такие, что $\forall x \in E$, $x = \alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_n a_n$, где $\alpha_1, \alpha_2 \ldots, \alpha_n \in k$. *Степенью* E над k мы будем называть размерность E как линейного пространства и обозначать $[E : k]$.

Теорема 2.2. *Пусть E — конечное расширение поля k, F — конечное расширение поля E. Тогда F — конечное расширение поля k и $[F : k] = [E : k][F : E]$.*

Доказательство. Пусть $x_1, x_2, \ldots, x_n$ — базис E над полем k, $y_1, y_2, \ldots, y_m$ — базис F над полем E. Тогда для любого элемента $a \in F$ существует разложение

$$a = \alpha_1 y_1 + \cdots + \alpha_m y_m,$$

где $\alpha_1, \ldots \alpha_m \in E$. Поскольку E — конечное расширение поля k, то

$$\alpha_i = \beta_{i1} x_1 + \cdots \beta_{in} x_n,$$

где $\beta_{ij} \in k$. Таким образом,

$$a = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} x_j y_i.$$

Следовательно, $\{x_j y_i\}$ порождают F над k. Таким образом, F — конечное расширение поля k. Осталось доказать равенство $[F : k] = [E : k][F : E]$. Для этого докажем линейную независимость $\{x_j y_i\}$. Предположим противное, т.е. существуют элементы

c_{ij} такие, что
$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_jy_i = 0.$$
С другой стороны,
$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_jy_i = \left(\sum_{j=1}^{n} c_{1j}x_j\right)y_1 + \left(\sum_{j=1}^{n} c_{2j}x_j\right)y_2 + \cdots + \left(\sum_{j=1}^{n} c_{mj}x_j\right)y_m.$$
Заметим, что $\sum\limits_{j=1}^{n} c_{ij}x_j \in E$. Поскольку $y_1, y_2, \ldots, y_m$ линейно независимы, то все $\sum\limits_{j=1}^{n} c_{ij}x_j = 0$. Поскольку $x_1, x_2, \ldots, x_n$ линейно независимы, то все $c_{ij} = 0$. $\square$

Замечание 2.3. Если $k \subset E \subset F$ и F — конечное расширение поля k, то очевидно, что E — конечное расширение поля k, а F — конечное расширение поля E.

Определение 2.4. Элемент $x \in E$ называется *алгебраическим*, если он является корнем многочлена с коэффициентами из k, т.е. существуют $\alpha_0, \alpha_1 \ldots, \alpha_n \in k$ такие, что $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots \alpha_n x^n = 0$. Расширение E поля k называется *алгебраическим*, если любой элемент E является алгебраическим.

Теорема 2.5. *Любое конечное расширение является алгебраическим.*

Доказательство. Пусть E — конечное расширение поля k, и пусть $a \in E$. Если $a \in k$, то он алгебраичен. Предположим, что $a \notin k$. Рассмотрим $1, a, a^2 \cdots a^n \cdots$. Поскольку E — конечное расширение поля k, то существует n такое, что элементы $1, a, a^2 \cdots a^n$ линейно зависимы. Тогда существуют $\alpha_0, \alpha_1 \ldots, \alpha_n \in k$ такие, что $\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots \alpha_n a^n = 0$. $\square$

Пусть E — расширение поля k, и $a_1, a_2, \ldots, a_n \in E$ обозначим через $k(a_1, a_2, \ldots, a_n)$ наименьшее подполе поля E, содержащее $a_1, a_2, \ldots, a_n$. Очевидно оно состоит из элементов вида
$$\frac{f(a_1, a_2, \ldots, a_n)}{g(a_1, a_2, \ldots, a_n)},$$
где f, g — многочлены с коэффициентами из k и $g(a_1, a_2, \ldots, a_n) \neq 0$.

Теорема 2.6. *Пусть E — расширение поля k и $a \in E$ алгебраичен над k. Тогда $k(a)$ — конечное расширение поля k.*

Доказательство. Пусть $f(x)$ — многочлен с коэффициентами из k такой, что $f(a) = 0$. Предположим, что $f(x)$ приводим над k, т.е. $f(x) = f_1(x)f_2(x)$, где $f_1(x), f_2(x)$ — многочлены над k, степени меньше степени $f(x)$. Тогда либо $f_1(a) = 0$, либо $f_2(a) = 0$. Таким образом, последовательно заменяя $f(x)$ на многочлены меньшей степени, мы можем считать, что $f(x)$ неприводим. Рассмотрим $k[x]$ — множество многочленов от x с коэффициентами из k. Пусть $g(x) \in k[x]$ такой, что $g(a) \neq 0$. Тогда $g(x)$ взаимно прост с $f(x)$. Следовательно, существуют многочлены $p(x), q(x)$ такие, что $f(x)p(x) + g(x)q(x) = 1$. Подставляя a, получаем $g(a)q(a) = 1$. Таким образом, $k[a]$ не только кольцо, но и поле. Очевидно, что размерность $k[a]$ как векторного пространства над k не превышает степени многочлена $f(x)$. □

Замечание 2.7. Заметим, что многочлен $f(x)$ единственен с точностью до умножения на константу. Мы можем считать, что коэффициент при старшей степени у этого многочлена равен 1. Действительно, пусть существует другой неприводимый многочлен $f'(x)$ такой, что $f'(a) = 0$. Поскольку они оба неприводимы, то они взаимно просты. Тогда существуют многочлены $p(x), q(x)$ такие, что $f(x)p(x) + f'(x)q(x) = 1$. Подставляем a, получаем противоречие. Таким образом, мы можем считать, что старший коэффициент многочлена $f(x)$ равен 1. Такой многочлен мы будем называть *минимальным многочленом элемента* a над k, и обозначать $\mathrm{Irr}(a, k, x)$.

Следствие 2.8. *Пусть E — расширение поля k и $a_1, a_2, \dots, a_n \in E$ алгебраичны над k. Тогда $k(a_1, a_2, \dots, a_n)$ — конечное расширение поля k.*

Доказательство. Заметим, что

$$k \subset k(a_1) \subset k(a_1, a_2) \subset \cdots \subset k(a_1, a_2, \dots, a_n).$$

Поскольку $k(a_1, a_2, \dots, a_i, a_{i+1}) = k(a_1, a_2, \dots, a_i)(a_{i+1})$, то согласно теореме 2.6 каждое вложение является конечным расширением. Теперь утверждение следует из теоремы 2.2. □

Теорема 2.9. *Пусть E — алгебраическое расширение поля k и F — алгебраическое расширение поля E. Тогда F — алгебраическое расширение поля k.*

Доказательство. Пусть $x \in F$. Тогда

$$a_0 + a_1 x + \cdots + a_n x^n = 0,$$

где $a_0, a_1, \ldots, a_n \in E$. Рассмотрим $E_0 = k(a_0, a_1, \ldots, a_n)$. Согласно следствию 2.8 E_0 — конечное расширение k. Рассмотрим $F_0 = E_0(x)$. Аналогично, F_0 — конечное расширение E_0. Следовательно, по теореме 2.2, F_0 — конечное расширение k. Заметим, что $x \in F_0$. С другой стороны, согласно теореме 2.5, F_0 — алгебраическое расширение поля k. Следовательно, x алгебраичен. $\square$

Замечание 2.10. Если $k \subset E \subset F$ и F — алгебраическое расширение поля k, то очевидно, что E — алгебраическое расширение поля k, а F — алгебраическое расширение поля E.

Определение 2.11. Пусть E и F — произвольные поля, содержащиеся в поле L. Наименьшее подполе в L, содержащие E и F называется *композитом* и обозначается EF. *Композитом* семейства подполей $\{E_i\}$ в L называется наименьшее подполе в L, содержащее все семейство $\{E_i\}$. Пусть $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ и F — расширение поля k. Предположим, что E и F содержатся в L. Тогда $EF = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Мы будем называть расширение EF поля F *подъемом* E до F.

Теорема 2.12. *Пусть E — конечное расширение поля k и F — любое расширение поля k. Предположим, что существует поле L, содержащее E и F. Тогда EF — конечное расширение поля F.*

Доказательство. Пусть E — конечное расширение поля k. Тогда существуют элементы $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$, алгебраичные над k такие, что $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Согласно 2.8 $EF = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ — конечное расширение F. $\square$

Следствие 2.13. *Пусть E и F — конечные расширения поля k. Предположим, что существует поле L, содержащее E и F. Тогда EF — конечное расширение поля k.*

Доказательство. Следует из2.2 и 2.12. $\square$

Теорема 2.14. *Пусть E — алгебраическое расширение поля k и F — любое расширение поля k. Предположим, что существует поле L, содержащее E и F. Тогда EF — алгебраическое расширение поля F.*

Доказательство. Пусть $\alpha \in E$ — алгебраический элемент над k. Тогда α алгебраичен над F (любой многочлен из $k[x]$ является многочленом в $F[x]$). $\square$

Следствие 2.15. *Пусть E и F — конечные расширения поля k. Предположим, что существует поле L, содержащее E и F. Тогда EF — конечное расширение поля k.*

Доказательство. Следует из2.9 и 2.14. $\square$

2. Нормальные расширения полей

Пусть $p(x)$ — неприводимый многочлен над полем k. Рассмотрим кольцо многочленов $k[x]$. Тогда многочлен $p(x)$ порождает главный идеал $(p(x))$. Поскольку $p(x)$ неприводим, то $(p(x))$ — максимальный идеал. Следовательно, $k[x]/(p(x))$ — поле. Пусть $\sigma\colon k[x] \to k[x]/(p(x))$ — естественный гомоморфизм. Заметим, что σ сюръективен на k. Тогда $\sigma(k)$ — подполе поля $k[x]/(p(x))$ изоморфное k. Мы можем отождествить его с k. Тогда $E = k[x]/(p(x))$ является расширением поля k. Рассмотрим $\xi = \sigma(x)$. Заметим, что ξ является корнем многочлена $p(x)$ в E. Таким образом, мы получили следующее утверждение.

Утверждение 2.16. *Для любого многочлена $p(x) \in k[x]$ существует расширение поля k в котором $p(x)$ имеет корень.*

Определение 2.17. Поле E называется *алгебраически замкнутым*, если любой многочлен $f(x) \in E[x]$ имеет корень.

Теорема 2.18. *Для любого поля k существует алгебраическое расширение $\bar{k}$ такое, что $\bar{k}$ алгебраически замкнуто.*

Пусть k — поле, $\sigma\colon k \to L$ — вложение поля k в алгебраически замкнутое поле L. Пусть $E = k(\alpha)$, $p(x) = \mathrm{Irr}(\alpha, k, x)$. Пусть $p^\sigma(x)$ — образ многочлена $p(x)$ в L, β — корень $p^\sigma(x)$. Заметим, что любой элемент из E можно записать в виде $f(\alpha)$, где $f(x) \in k[x]$. Определим продолжение σ как отображение $f(\alpha) \to f^\sigma(\beta)$. Это отображение не зависит от $f(x) \in k[x]$. Действительно, пусть есть $g(x) \in k[x]$ такой, что $f(\alpha) = g(\alpha)$. Тогда $f(\alpha) - g(\alpha) = 0$. Следовательно, $f(x) - g(x)$ делится на $p(x)$. Отсюда, $f^\sigma(x) - g^\sigma(x)$ делится на $p^\sigma(x)$. Тогда $f^\sigma(\beta) - g^\sigma(\beta) = 0$ и $f^\sigma(\beta) = g^\sigma(\beta)$. Таким образом, мы получили продолжение σ на $E = k(\alpha)$.

Замечание 2.19. Данное продолжение не единственно и зависит от выбора β.

Лемма 2.20. *Пусть E — алгебраическое расширение поля k, и $\sigma\colon E \to E$ — гомоморфизм. Тогда σ — автоморфизм.*

Доказательство. Очевидно, что σ инъективен. Осталось доказать, что он сюръективен. Пусть α — произвольный элемент из E, и $p(x)$ — его минимальный многочлен. Рассмотрим подполе E'

порожденное всеми корнями $p(x)$, лежащими в E. Тогда E' — конечное расширение поля k. Поскольку σ отображает каждый корень многочлена $p(x)$ в корень этого же многочлена, то σ отображает E' в себя. Тогда $\sigma(E')$ — подпространство в E', имеющее ту же размерность, что и E'. Следовательно, $\sigma(E') = E'$. Поскольку $\alpha \in E'$, то α лежит в образе σ. $\square$

Теорема 2.21. *Пусть k — поле, E — алгебраическое расширение поля k, и $\sigma\colon k \to L$ — вложение поля k в алгебраически замкнутое поле L. Тогда существует продолжение σ до вложения E в L. Если L алгебраически замкнуто, и L алгебраично над σk, то любое продолжение σ будет изоморфизмом поля E на L.*

Доказательство. Рассмотрим множество S пар (F, τ), где F — подполе E, содержащие k, τ — продолжение σ до вложения F в L. Мы пишем $(F, \tau) < (F', \tau')$, если $F \subset F'$ и τ' совпадает с τ на F. Заметим, что S не пусто ($(k, \sigma) \in S$). Рассмотрим линейно упорядоченое подмножество (F_i, τ_i). Пусть $F = \cup F_i$, и $\tau = \tau_i$ на каждом F_i. Тогда (F, τ) — верхняя грань этого упорядоченного подмножества. Тогда существует максимальный элемент (K, λ). Мы утверждаем, что $K = E$. Действительно, пусть $K \neq E$. Тогда существует $\alpha \in E$, $\alpha \notin K$. Мы знаем, что λ имеет продолжение на $K(\alpha)$ вопреки максимальности (K, λ). Если L алгебраически замкнуто, и L алгебраично над σk, то σE алгебраически замкнуто и L алгебраично над σE. Отсюда, $L = \sigma E$. $\square$

Пример 2.22. $\bar{\mathbb{R}} = \mathbb{C} = \mathbb{R}[x]/(x^2 + 1)$. Поскольку существуют трансцендентные числа (например e и π), то $\bar{\mathbb{Q}} \neq \mathbb{C}$.

Определение 2.23. Пусть k — поле, $f(x) \in k[x]$. *Полем разложения* многочлена $f(x)$ мы будем называть расширение K поля k, в котором $f(x)$ разлагается на линейные множители, т.е.

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

где все $\alpha_i \in K$ и $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Теорема 2.24. *Пусть K — поле разложения многочлена $f(x) \in k[x]$, и E — другое поле разложения $f(x)$. Тогда существует изоморфизм $\sigma\colon E \to K$, индуцирующий тождественное отображение на k (такой изоморфизм мы будем называть k-изоморфизмом). Более того, если $k \subset K \subset \bar{k}$, то любое вложение E в $\bar{k}$ является k-изоморфизмом E на K.*

Доказательство. Пусть $\bar{K}$ — алгебраическое замыкание поля K. Тогда $\bar{K}$ алгебраичен над k и, следовательно, $\bar{K} = \bar{k}$. Согласно теореме 2.21 существует вложение $\sigma\colon E \to \bar{K}$, индуцирующее тождественное отображение на k. Заметим, что

$$f(x) = c(x - \beta_1)(x - \beta_2) \cdots (x - \beta_n),$$

где $\beta_i \in E$, $c \in k$. Тогда

$$f(x) = f^{\sigma}(x) = c(x - \sigma(\beta_1))(x - \sigma(\beta_2)) \cdots (x - \sigma(\beta_n)).$$

С другой стороны, $f(x)$ имеет в $K[x]$ разложение

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Поскольку разложение многочлена единственно в $\bar{K}[x]$, то $(\sigma(\beta_1), \sigma(\beta_2), \ldots, \sigma(\beta_n))$ отличается от $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ только перестановкой. Отсюда, $\sigma(\beta_i) \in K$ для любого i. Поскольку $E = k(\beta_1, \beta_2, \ldots, \beta_n)$, то $\sigma E \subset K$. С другой стороны, $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n) = k(\sigma(\beta_1), \sigma(\beta_2), \ldots, \sigma(\beta_n))$. Тогда $\sigma E = K$. □

Следствие 2.25. *Пусть $\tau\colon k_1 \to k_2$ — изоморфизм двух полей, $f(x) \in k_1[x]$ — многочлен степени n, $\bar{f}(x) = \tau(f(x)) \in k_2[x]$. Пусть k_1' и k_2' — поля разложения над k_1 и k_2 многочленов $f(x)$ и $\bar{f}(x)$ соответственно. Тогда τ может быть продолжен до изоморфизма $\varrho\colon k_1' \to k_2'$, и любое такое продолжение переводит каждый корень многочлена $f(x)$ в корень многочлена $\bar{f}(x)$.*

Замечание 2.26. Заметим, что всякий многочлен $f(x) \in k[x]$ имеет поле разложения, а именно поле, порожденное всеми его корнями в $\bar{k}$.

Пусть $\{f_i\}$ — семейство многочленов из $k[x]$. *Полем разложения* этого семейства мы будем называть расширение K поля k такое, что любой f_i разлагается на линейные множители в $K[x]$, и K порождается корнями многочленов $\{f_i\}$.

Замечание 2.27. Если семейство $f_1, f_2, \ldots, f_n$ конечно, то полем разложения этих многочленов будет поле разложения одного многочлена

$$f(x) = f_1(x) f_2(x) \cdots f_n(x).$$

Определение 2.28. Расширение K поля k называется *нормальным*, если K — алгебраическое расширение поля k, и любой неприводимый многочлен из $k[x]$, имеющий корень в K разлагается на линейные множители.

Предложение 2.29. *Пусть K — конечное нормальное расширение поля k. Тогда K — поле разложения некоторого многочлена $f(x) \in k[x]$.*

Доказательство. Поскольку K — конечное расширение поля k, то $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Пусть $f_i(x) = \mathrm{Irr}(\alpha_i, k, x)$ — минимальный многочлен элемента α_i. Поскольку K — нормальное расширение поля k, то K содержит поле разложения $f_i(x)$. Тогда K содержит поле разложение многочлена $f(x) = f_1(x)f_2(x)\cdots f_n(x)$. Поскольку K порождается корнями $f(x)$ (а именно $\alpha_1, \alpha_2, \ldots, \alpha_n$), то K — поле разложения многочлена $f(x)$. $\square$

Теорема 2.30. *Поле разложения многочлена $f(x) \in k[x]$ над k является конечным нормальным расширением поля k.*

Доказательство. Пусть K — поле разложения многочлена $f(x) \in k[x]$ над k, и $g(x)$ — любой неприводимый многочлен над k имеющий корень α в поле K. Пусть K' — поле разложения многочлена $g(x)$ над K. Пусть $\beta \in K'$ — корень $g(x)$. Поскольку $g(x)$ неприводим над k, то существует k-изоморфизм τ между $k(\alpha)$ и $k(\beta)$, переводящий α в β. Этот изоморфизм оставляет $f(x)$ на месте. Заметим, что K и $K(\beta)$ — поля разложения $f(x)$ над k и $k(\beta)$ соответственно. Таки образом, согласно следствию 2.25, изоморфизм τ продолжается до изоморфизма ϱ поля K на поле $K(\beta)$. Поскольку ϱ — k-изоморфизм и $f(x)$ разлагается на линейные множители в K, то ϱ переводит множество корней $f(x)$ в себя. Заметим, что множество корней $f(x)$ порождают K. Следовательно, ϱ — автоморфизм поля K. Поскольку $\alpha \in K$, то $\varrho(\alpha) = \beta \in K$. Таким образом, K содержит все корни многочлена $g(x)$. Отсюда следует, что K — нормальное расширение поля k. $\square$

Теорема 2.31. *Пусть K — алгебраическое расширение поля k, и $k \subset K \subset \bar{k}$, где $\bar{k}$ — алгебраическое замыкание k. Тогда K — нормальное расширение поля k тогда и только тогда, когда всякое вложение $\sigma\colon K \to \bar{k}$ над k является автоморфизмом поля K.*

Доказательство. Предположим, что всякое вложение $\sigma\colon K \to \bar{k}$ над k является автоморфизмом поля K. Пусть $f(x) \in k[x]$ — неприводимый многочлен над k, и $\alpha \in K$ — его корень. Пусть $\beta \in \bar{k}$ — другой корень этого многочлена. Тогда существует k-изоморфизм σ полей $k(\alpha)$ и $k(\beta)$. Продолжим этот изоморфизм до вложения K в $\bar{k}$. По предположению, это вложение является автоморфизмом поля K. Отсюда, $\beta \in K$.

Обратно, пусть K — нормальное расширение поля k. Пусть $\sigma\colon K \to \bar{k}$ — вложение над k, и $\alpha \in K$. Пусть $p(x)$ — минимальный многочлен α над k. Поскольку σ — вложение над k, то σ отображает α в корень β многочлена $p(x)$. Поскольку K — нормальное расширение поля k, то $\beta \in K$. Следовательно, σ — автоморфизм поля K (см. 2.20). $\square$

Предложение 2.32. *Пусть E — расширение поля k степени два. Тогда E — нормальное расширение.*

Доказательство. Пусть $f(x) \in k[x]$ — неприводимый многочлен над k, и $\alpha \in E$ — корень $f(x)$. Тогда $E = k(\alpha)$. Пусть K — поле разложения $f(x)$. Заметим, что $E \subset K$. Рассмотрим минимальный многочлен $p(x) \in k[x]$ элемента α. Поскольку E — расширение степени два, то $p(x)$ имеет степень два. Следовательно, существует $\bar{\alpha} \in E$ такой, что $p(\bar{\alpha}) = 0$. Пусть τ — автоморфизм поля E переводящий α в $\bar{\alpha}$. Поскольку τ — k-изоморфизм, то он оставляет $f(x)$ на месте. Следовательно, он продолжается до автоморфизма поля K. Тогда $\bar{\alpha} = \tau(\alpha)$ является корнем $f(x)$. Отсюда следует, что $p(x)$ делит $f(x)$ (т.е. $f(x) = cp(x)$, $c \in k$). Тогда E — поле разложения многочлена $f(x)$. $\square$

Пример 2.33. Алгебраическое замыкание является нормальным расширением.

Пример 2.34. Пусть $E = \mathbb{Q}(\sqrt[4]{2})$. Тогда E не является нормальным расширением поля $\mathbb{Q}$, E не содержит комплексные корни многочлена $x^2 - 2$. С другой стороны, пусть $F = \mathbb{Q}(\sqrt{2})$. Тогда $\mathbb{Q} \subset F \subset E$, при этом F — расширение поля $\mathbb{Q}$ степени два, и E расширение поля F степени два, т.е. оба эти расширения нормальны.

Теорема 2.35. *Пусть $k \subset E \subset K$, и K — нормальное расширение поля k. Тогда K — нормальное расширение поля E.*

Доказательство. Рассмотрим вложение полей $k \subset E \subset K$ в алгебраическое замыкание $\bar{k}$. Пусть $\sigma\colon K \to \bar{k}$ — любое вложение K над E. Тогда σ является вложением и над k. По теореме 2.31 σ является автоморфизмом поля K. По той же теореме, K — нормальное расширение поля E. $\square$

3. Сепарабельные расширения полей

Определение 2.36. Пусть k — поле. Предположим, что существует такое число p, что $p \cdot 1 = 0$, т.е.

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ слагаемых}} = 0.$$

Пусть p — минимальное из таких чисел. Тогда говорят, что p — *характеристика поля* k. Обозначается $char(k)$. Если не существует такого положительного числа p, то говорим, что поле имеет характеристику ноль.

Утверждение 2.37. *Характеристика поля либо ноль, либо простое число.*

Доказательство. Предположим, что характеристика поля $p = mn$. Тогда

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ слагаемых}} = \underbrace{(1 + 1 + \cdots + 1)}_{m \text{ слагаемых}} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{n \text{ слагаемых}} = 0.$$

Отсюда, либо

$$\underbrace{1 + 1 + \cdots + 1}_{m \text{ слагаемых}} = 0,$$

либо

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ слагаемых}} = 0.$$

□

Рассмотрим поле k характеристики p.

Утверждение 2.38. *Пусть k — поле характеристики p. Тогда $(a + b)^p = a^p + b^p$.*

Доказательство. Следует из формулы Бинома–Ньютона и того, что C_p^i делится на p для любого $i \neq 0, p$. □

Определение 2.39. Поскольку $(a + b)^p = a^p + b^p$ и $(ab)^p = a^p b^p$, то отображение $f\colon k \to k^p$ заданное $f(x) = x^p$ является гомоморфизмом. Он называется *морфизмом Фробениуса.*

Определение 2.40. Поле k называется совершенным, если либо k характеристики ноль, либо k характеристики p и совпадает с k^p.

Теорема 2.41. *Пусть k — конечное поле. Тогда k совершенно.*

Доказательство. Заметим, что k^p — подполе в k и k^p изоморфно k. Следовательно, k^p и k имеют одинаковое количество элементов. Тогда они совпадают. $\square$

Рассмотрим $f(x) \in k[x]$, т.е.

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

Пусть $f'(x)$ — обычная производная, т.е.

$$f'(x) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1.$$

Заметим, что если k имеет характеристику ноль, то $f'(x) \neq 0$ при $n \geq 1$. Более того, если k имеет характеристику p, то $f'(x) = 0$ тогда и только тогда, когда $f(x) = \tilde{f}(x^p)$, т.е. $f(x)$ — многочлен от x^p.

Определение 2.42. Неприводимый многочлен $f(x)$ называется *сепарабельным*, если $f'(x) \neq 0$ и *несепарабельным*, если $f'(x) = 0$. Произвольный многочлен $f(x)$ называется *сепарабельным*, если сепарабельны все его неразложимые множители.

Замечание 2.43. Если k имеет характеристику ноль, то любой многочлен сепарабелен.

Рассмотрим более подробно связь между полем k и сепарабельности многочленов $f(x) \in k[x]$.

Теорема 2.44. *Пусть k — поле характеристики p. Если $a \in k$, $\sqrt[p]{a} \notin k$, то $x^{p^m} - a$ неразложим в $k[x]$ для любого m.*

Доказательство. Докажем индукцией по m. Для $m = 0$ утверждение очевидно. Пусть $\varphi(x)$ — приведенный неразложимый множитель многочлена $x^{p^m} - a$ в $k[x]$, и $\varphi^l(x)$ — наивысшая степень $\varphi(x)$, которая делит $x^{p^m} - a$. Таким образом,

$$x^{p^m} - a = \varphi^l(x)\psi(x),$$

где $\varphi(x)$ и $\psi(x)$ взаимно просты. Возьмем производную от обеих частей, получим

$$l\varphi^{l-1}(x)\varphi'(x)\psi(x) + \varphi^l(x)\psi'(x) = 0.$$

Поделим на $\varphi^{l-1}(x)$, получим

$$l\varphi'(x)\psi(x) + \varphi(x)\psi'(x) = 0.$$

Заметим, что $\psi(x)$ должен делить $\varphi(x)\psi'(x)$. С другой стороны, $\varphi(x)$ и $\psi(x)$ взаимно просты, а $\psi'(x)$ имеет меньшую степень чем у $\psi(x)$. Тогда $\varphi(x)\psi'(x) = 0$, и следовательно, $l\varphi'(x)\psi(x) = 0$. Отсюда, $\psi'(x) = 0$ и $l\varphi'(x) = 0$. Из $\psi'(x) = 0$ следует, что $\psi(x) = \psi_1(x^p)$.

Предположим, что l не делится на p. Тогда, из $l\varphi'(x) = 0$ следует, что $\varphi(x) = \varphi_1(x^p)$. Отсюда, заменяя x на x^p, получаем

$$x^{p^{m-1}} - a = \varphi_1^l(x)\psi_1(x).$$

Противоречие с индуктивным предположением. Пусть l делится на p. Тогда $\varphi^l(x) = \varphi_1(x^p)$. Следовательно,

$$x^{p^{m-1}} - a = \varphi_1(x)\psi_1(x).$$

Отсюда, $\psi(x) = 1$ и $x^{p^m} - a = \tilde{\varphi}^p(x)$. С другой стороны, все коэффициенты $\tilde{\varphi}^p(x)$ принадлежат k^p. Противоречие с условием $\sqrt[p]{a} \notin k$. $\square$

Теорема 2.45. *Поле k совершенно тогда и только тогда, когда каждый многочлен положительной степени сепарабелен.*

Доказательство. Мы можем считать, что поле k имеет характеристику p. Предположим, что k совершенно, и $f(x) \in k[x]$ — многочлен такой, что $f'(x) = 0$. Тогда $f(x) \in k[x^p]$, т.е.

$$f(x) = a_n x^{pn} + a_{n-1}x^{p(n-1)} + \cdots + a_1 x^p + a_0.$$

Поскольку k совершенно, то существуют элементы $\alpha_i = \sqrt[p]{a_i} \in k$. Тогда

$$f(x) = (\alpha_n x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0)^p.$$

Следовательно, $f(x)$ разложим.

Предположим, что k несовершенно. Тогда существует элемент $a \in k$ такой, что $\sqrt[p]{a} \notin k$. Согласно теореме 2.44 многочлен $f(x) = x^p - a$ неразложим, но $f'(x) = 0$. $\square$

Определение 2.46. Пусть K — расширение поля k и $\alpha \in K$ — алгебраический элемент. Мы говорим, что α *сепарабелен*, если его минимальный многочлен сепарабелен.

Определение 2.47. Алгебраическое расширение K поля k называется *сепарабельным*, если каждый элемент поля K сепарабелен над k.

Замечание 2.48. Из теоремы 2.45 следует, что если k совершенно, то любое его алгебраическое расширение сепарабельно.

Утверждение 2.49. *Пусть α — алгебраический элемент над k, и $f(x)$ — его минимальный многочлен. Тогда α несепарабелен тогда и только тогда, когда $f'(\alpha) = 0$. Более того, если $g(x) \in k[x]$ — многочлен такой, что $g(\alpha) = 0$, то $g'(\alpha) = 0$.*

Доказательство. Если α несепарабелен, то $f'(x) = 0$. Обратно, если $f'(\alpha) = 0$, то, поскольку $f(x)$ — минимальный многочлен, а $f'(x)$ имеет степень на единицу меньше чем $f(x)$, то $f'(x) = 0$. Пусть α несепарабелен, и $g(x) \in k[x]$ — многочлен такой, что $g(\alpha) = 0$. Тогда $g(x)$ делится на $f(x)$, т.е. $g(x) = h(x)f(x)$. Тогда

$$g'(x) = h'(x)f(x) + h(x)f'(x) = h'(x)f(x).$$

Отсюда, $g'(\alpha) = h'(\alpha)f(\alpha) = 0$. □

Пусть $f(x) \in k[x]$ такой, что $f(\alpha) = 0$, где $\alpha \in K$, K — расширение поля k. Тогда $f(x)$ делится на $x - \alpha$. Пусть s — наибольшая степень $x-\alpha$ такая, что $f(x) = (x-\alpha)^s f_1(x)$. Заметим, что $f_1(\alpha) \neq 0$. Более того, поскольку $f(x) \in k[x]$, то $f_1(x) \in k(\alpha)[x]$. В силу единственности разложения $f(x)$ над $k(\alpha) \subset K$, получаем, что s и $f_1(x)$ не зависят от расширения. Число s называется *кратностью корня* α многочлена $f(x)$. Мы будем говорить, что α — *простой корень*, если $s = 1$, и α — *кратный корень*, если $s > 1$.

Утверждение 2.50. *Пусть α — алгебраический элемент над k, и $f(x) \in k[x]$ — многочлен такой, что $f(\alpha) = 0$. Тогда α —* кратный корень *тогда и только тогда, когда $f'(\alpha) = 0$.*

Доказательство. Пусть $f(x) = (x - \alpha)^s f_1(x)$. Тогда

$$f'(x) = s(x - \alpha)^{s-1} f_1(x) + (x - \alpha)^s f_1'(x).$$

Если $s > 1$, то $f'(\alpha) = 0$. Обратно, если $s = 1$, то $f'(\alpha) = f_1(\alpha) \neq 0$. □

Следствие 2.51. *Пусть α — алгебраический элемент над k, и $f(x)$ — его минимальный многочлен. Тогда α несепарабелен тогда и только тогда, когда α — кратный корень многочлена $f(x)$. Более того, если $g(x) \in k[x]$ — многочлен такой, что $g(\alpha) = 0$, то α — кратный корень многочлена $g(x)$.*

Теорема 2.52. *Пусть α алгебраичен над k, и $f(x)$ — его минимальный многочлен. Если $char(k) = 0$, то все корни $f(x)$ имеют кратность один. Если $char(k) = p > 0$, то существует e такое, что все корни $f(x)$ имеют кратность p^e.*

Доказательство. Пусть α и β — корни многочлена $f(x)$ в замыкании $\bar{k}$. Тогда существует изоморфизм $\sigma\colon k(\alpha) \to k(\beta)$, который продолжается до автоморфизма $\bar{k}$. Следовательно, все корни имеют одинаковую кратность m. Рассмотрим $f'(x)$. Если $m > 1$, то α является корнем многочлена $f'(x)$, степень которого меньше степени $f(x)$. Поскольку $f(x)$ — минимальный многочлен, то $f'(x) = 0$.

Следовательно, если $f(x)$ имеет кратные корни, то $char(k) = p > 0$ и $f(x) = g(x^p)$. Пусть $f(x) = (x-\alpha)^m f_1(x)$, где $f_1(x) \in k(x)$ и $f_1(\alpha) \neq 0$. Тогда

$$f'(x) = m(x-\alpha)^{m-1} f_1(x) + (x-\alpha)^m f_1'(x) = 0.$$

Поделив на $(x-\alpha)^{m-1}$, получим

$$m f_1(x) + (x-\alpha) f_1(x) = 0.$$

Поскольку $f_1(\alpha) \neq 0$, то m делится на p, т.е. $m = m_1 p$. Применив морфизм Фробениуса, получаем

$$f(x) = (x-\alpha)^m f_1(x) = (x^p - \alpha^p)^{m_1} g_1(x^p).$$

Таким образом, все корни многочлена $g(x)$ имеют кратность m_1. Повторяя наше рассуждение, получаем, что либо $m_1 = 1$, либо $m_1 = pm_2$ и $g(x) = h(x^p)$. Продолжая этот процесс, получаем, что все корни имеют кратность p^e. $\square$

Рассмотрим еще одно важное отличие сепарабельных и несепарабельных расширений.

Пусть k — поле и $k(\alpha)$ — расширение, порожденное алгебраическим элементом α, $f(x)$ — минимальный многочлен элемента α. Тогда число вложений $k(\alpha)$ в алгебраическое замыкание $\bar{k}$ равно числу различных корней многочлена $f(x)$. С другой стороны, степень $[k(\alpha) : k] = \deg f$. Таким образом, число вложений $k(\alpha)$ в алгебраическое замыкание $\bar{k}$ не превосходит степени $[k(\alpha) : k]$. Более того, равенство достигается тогда и только тогда, когда α сепарабелен. Пусть E — конечное расширение поля k. Пусть $[E : k]_S$ — количество вложений поля E в алгебраическое замыкание $\bar{k}$. Число $[E : k]_S$ будем называть *сепарабельной степенью* E над k.

Теорема 2.53. *Пусть E — конечное расширение поля k, и F — конечное расширение поля E. Тогда*

$$[E : k]_S [F : E]_S = [F : k]_S.$$

Доказательство. Пусть $\sigma_1, \sigma_2, \ldots, \sigma_n$ — множество вложений E в алгебраическое замыкание $\bar{k}$ над k, и $\tau_{i1}, \tau_{i2}, \ldots, \tau_{im}$ — множество продолжений σ_i до вложения F в $\bar{k}$. Поскольку $\sigma_i \sigma_j^{-1}$ — изоморфизм полей $\sigma_j E$ и $\sigma_i E$, то количество продолжений одинаково для любого σ_i. Таким образом, мы получили nm вложений F в алгебраическое замыкание $\bar{k}$. Обратно, пусть ϱ — вложение F в $\bar{k}$ над k. Тогда ограничение ϱ на E совпадает с одним из σ_i. Следовательно, $\varrho = \tau_{ij}$. $\square$

Теперь рассмотрим один важный критерий сепарабельности.

Теорема 2.54. *Пусть E — конечное расширение поля k. Тогда $[E : k]_S \leq [E : k]$. Более того, $[E : k]_S = [E : k]$ тогда и только тогда, когда E — сепарабельное расширение поля k.*

Доказательство. Поскольку E — конечное расширение поля k, то существует башня полей

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \alpha_2, \ldots, \alpha_n) = E.$$

Согласно теоремам 2.53 и 2.2, получаем

$$[E : k]_S = [k(\alpha_1) : k]_S \cdots [k(\alpha_1, \alpha_2, \ldots, \alpha_n) : k(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})]_S,$$

$$[E : k] = [k(\alpha_1) : k] \cdots [k(\alpha_1, \alpha_2, \ldots, \alpha_n) : k(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})].$$

Мы знаем, что

$$[k(\alpha_1, \alpha_2, \ldots, \alpha_i) : k(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})]_S \leq$$

$$\leq [k(\alpha_1, \alpha_2, \ldots, \alpha_i) : k(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})].$$

Более того, равенство достигается, когда α_i сепарабелен. □

Замечание 2.55. Из теоремы 2.52 следует, что $[E : k] = [E : k]_S p^r$.

Теорема 2.56. *Пусть E — алгебраическое расширение поля k, и F — алгебраическое расширение поля E. Тогда для того, чтобы F было сепарабельным расширением поля k необходимо и достаточно, чтобы E было сепарабельным расширением поля k и F было сепарабельным расширением поля E.*

Доказательство. Пусть F — сепарабельное расширение поля k. Заметим, что все элементы поля E являются элементами поля F, и следовательно, сепарабельны над k. Поскольку каждый элемент из F сепарабелен над k, то он сепарабелен и над E. Обратно, пусть E — сепарабельное расширение поля k и F — сепарабельное расширение поля E. Если E и F — конечные расширения, то утверждение следует из теорем 2.53 и 2.54. Пусть $\alpha \in F$, и $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ — его минимальный многочлен. Положим $E_0 = k(a_0, a_1, \ldots, a_n)$, $F_0 = E_0(\alpha)$. Заметим, что E_0 — конечное расширение поля k, F_0 — конечное расширение поля E_0. Тогда F_0 сепарабельно над k. Следовательно, $\alpha \in F$ — сепарабельный над k элемент. □

Определение 2.57. Пусть k — поле характеристики p. Элемент α называется *чисто несепарабельным* над k, если существует целое $l \geq 0$ такое, что $\alpha^{p^l} \in k$. Расширение K поля k называется *чисто несепарабельным*, если все элементы K чисто несепарабельны.

Теорема 2.58. *Пусть α — одновременно сепарабельный и чисто несепарабельный элемент над k. Тогда $\alpha \in k$.*

Доказательство. Предположим, что α — чисто несепарабельный элемент над k. Пусть l — минимальное число такое, что $\alpha^{p^l} = a \in k$. Тогда $\sqrt[p]{a} \notin k$. Согласно теореме 2.44 $x^{p^l} - a$ неразложим. Следовательно, $f(x) = x^{p^l} - a$ — минимальный многочлен элемента α. С другой стороны, $f'(x) = 0$. Следовательно, α несепарабелен. □

Теорема 2.59. *Пусть K — конечное сепарабельное расширение поля k. Тогда существует элемент $\alpha \in K$ такой, что $K = k(\alpha)$.*

Доказательство. Мы будем предполагать, что k бесконечное поле (доказательство для конечных полей будет дано в следующем параграфе). Предположим, что $K = k(\alpha, \beta)$. Пусть $n = [K : k]$, и $\sigma_1, \sigma_2, \ldots, \sigma_n$ — различные вложения K в $\bar{k}$ над k. Рассмотрим

$$P(x) = \prod_{i \neq j} (\sigma_i \alpha + (\sigma_i \beta)x - \sigma_j \alpha - (\sigma_j \beta)x).$$

Заметим, что $P(x)$ ненулевой многочлен. Тогда существует $c \in k$ такой, что $P(c) \neq 0$. Тогда все элементы $\sigma_i(\alpha + c\beta)$ различны, а следовательно $k(\alpha + c\beta)$ имеет над k степень не меньше n. С другой стороны, $[K : k] = n$. Следовательно, $k(\alpha + c\beta) = K$. □

Если $K = k(\alpha)$, то элемент α называется *примитивным элементом* поля K над k.

4. Конечные поля

В этом параграфе мы рассмотрим конечные поля. Пусть k — поле из q элементов. Очевидно, что $char(k) = p > 0$. Следовательно, поле k содержит $\mathbb{Z}_p$ в качестве подполя. Тогда k является конечным расширением поля $\mathbb{Z}_p$, т.е. $[k : \mathbb{Z}_p] = n$. Таким образом, любой элемент $\alpha \in k$ имеет единственное представление в виде

$$\alpha = a_1 e_1 + a_2 e_2 + \cdots + a_n e_n,$$

где $e_1, e_2, \ldots, e_n$ — базис k как векторного пространства над $\mathbb{Z}_p$, $a_1, a_2, \ldots, a_n \in \mathbb{Z}_p$. Отсюда, число элементов в поле k равно p^n.

Теорема 2.60. *Пусть k^* — мультипликативная группа поля k, т.е. множество $k \setminus \{0\}$ с операцией умножение. Тогда k^* — циклическая группа порядка $p^n - 1$.*

Доказательство. Предположим, что k^* не является циклической группой. Тогда существует $r < p^n - 1$ такое, что $\alpha^r = 1$ для любого $\alpha \in k^*$. Таким образом, все элементы k^* являются корнями многочлена $x^r - 1 = 0$, но этот многочлен имеет не более r корней. Противоречие. $\square$

Замечание 2.61. Фактически мы доказали, что любая конечная мультипликативная группа в поле циклическая.

Замечание 2.62. Именно из этой теоремы следует теорема 2.59 для конечных полей. Действительно, если K — конечное расширение конечного поля k, то K — конечное поле. Тогда его мультипликативная группа K^* — циклическая. Следовательно, существует $\alpha \in K$ порождающий эту группу. Тогда $K = k(\alpha)$.

Рассмотрим поле разложения многочлена $f(x) = x^{p^n} - x$ над полем $\mathbb{Z}_p$. Мы утверждаем, что это поле состоит из корней $f(x)$. Действительно, если α, β — корни $f(x)$, то

$$(\alpha+\beta)^{p^n} - (\alpha+\beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = 0,$$
$$(\alpha\beta)^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0,$$
$$(\alpha^{-1})^{p^n} - \alpha^{-1} = (\alpha^{p^n})^{-1} - \alpha^{-1} = \alpha^{-1} - \alpha^{-1} = 0,$$
$$(-\alpha)^{p^n} - (-\alpha) = -\alpha + \alpha = 0.$$

Заметим, что 0 и 1 — корни $f(x)$. Следовательно, поле разложение многочлена $f(x) = x^{p^n} - x$ состоит из его корней. С другой стороны, $f'(x) = -1$. Следовательно, все корни $f(x)$ различные. Таким образом, мы получили поле состоящее из p^n элементов.

Глава 3

Теория Галуа

1. Группа автоморфизмов поля

Пусть K — поле, и G — группа автоморфизмов поля K. Обозначим через K^G — множество неподвижных элементов относительно группы G. Тогда K^G мы будем называть *неподвижным полем* группы G (или *полем инвариантов* группы G). Очевидно, что K^G является полем.

Алгебраическое расширение K поля k называется *расширением Галуа*, если оно нормально и сепарабельно. Мы будем считать, что K вложено в алгебраическое замыкание k. Группа автоморфизмов поля K над k называется *группой Галуа* поля K над k и обозначается $G(K/k)$.

Теорема 3.1. *Пусть K — расширение Галуа поля k, G — его группа Галуа. Тогда $k = K^G$. Если E — промежуточное поле, $k \subset E \subset K$, то K — расширение Галуа над E. Отображение множества промежуточных полей в множество подгрупп группы G инъективно.*

Доказательство. Пусть $\alpha \in K^G$ и σ — вложение $k(\alpha)$ в $\bar{K}$. Продолжим σ до вложения K в $\bar{K}$. Тогда σ — автоморфизм поля K, и, следовательно, элемент группы G. Поскольку σ оставляет α неподвижным, то $[k(\alpha) : k]_S = 1$. Поскольку α сепарабелен, то $\alpha \in k$.

Пусть E — промежуточное поле. Тогда K нормально и сепарабельно над E (см. теоремы 2.35 и 2.56). Следовательно, K — расширение Галуа поля E. Пусть $H = G(K/E) \subset G$. Тогда $K^H = E$. Пусть E' — другое промежуточное поле и $H' = G(K/E')$. Если $H = H'$, то
$$E = K^H = K^{H'} = E'.$$
Следовательно, отображение $E \to G(K/E)$ — инъективно. $\square$

Следствие 3.2. *Пусть K — расширение Галуа поля k, G — его группа Галуа. Пусть E_1 и E_2 — два промежуточных поля, H_1, H_2*

— группы Галуа поля K над E_1 и E_2 соответственно. Тогда неподвижное поле наименьшей подгруппы, содержащей H_1, H_2, есть $E_1 \cap E_2$.

Следствие 3.3. *Пусть K — расширение Галуа поля k, G — его группа Галуа. Пусть E_1 и E_2 — два промежуточных поля, H_1, H_2 — группы Галуа поля K над E_1 и E_2 соответственно. Тогда $E_2 \subset E_1$ в том и только в том случае, когда $H_1 \subset H_2$.*

Мы будем говорить, что подгруппа $H \subset G$ принадлежит промежуточному полю E, если $H = G(K/E)$.

Лемма 3.4. *Пусть E — алгебраическое сепарабельное расширение поля k. Предположим, что существует натуральное число n такое, что всякий элемент $\alpha \in E$ имеет степень меньше n. Тогда E — конечное расширение поля k и $[E : k] \leq n$.*

Доказательство. Пусть $\alpha \in E$ — элемент максимальной степени m, т.е. $m = [k(\alpha) : k]$ максимальна. Заметим, что $m \leq n$. Предположим, что $k(\alpha) \neq E$. Тогда существует $\beta \in E$ такой, что $\beta \notin k(\alpha)$. Тогда

$$k \subset k(\alpha) \subset k(\alpha, \beta)$$

и $[k(\alpha, \beta), k] > m$. По теореме о примитивном элементе (см. теорема 2.59) существует $\gamma \in k(\alpha, \beta)$ такой, что $k(\gamma) = k(\alpha, \beta)$. Тогда степень элемента γ равна $[k(\gamma), k] > m$. Противоречие. □

Теорема 3.5. *Пусть K — поле и G — конечная группа автоморфизмов поля K, имеющая порядок n. Пусть $k = K^G$. Тогда K — конечное расширение Галуа поля k и его группа Галуа есть G. Более того, $[K : k] = n$.*

Доказательство. Пусть $\alpha \in K$, и пусть $\sigma_1, \sigma_2, \ldots, \sigma_m$ — максимальное множество элементов из G таких, что $\sigma_1\alpha, \sigma_2\alpha, \ldots, \sigma_m\alpha$ различны. Тогда группа G действует на множестве $\{\sigma_1\alpha, \sigma_2\alpha, \ldots, \sigma_m\alpha\}$ (если $\tau \in G$, то τ отображает $\{\sigma_1\alpha, \sigma_2\alpha, \ldots, \sigma_m\alpha\}$ в $\{\tau\sigma_1\alpha, \tau\sigma_2\alpha, \ldots, \tau\sigma_m\alpha\}$). Рассмотрим

$$f(x) = \prod_{i=1}^{m}(x - \sigma_i\alpha).$$

Заметим, что α является корнем этого многочлена и любой элемент группы G оставляет $f(x)$ на месте. Следовательно, коэффициенты $f(x)$ лежат в k. Таким образом, K — алгебраическое расширение поля k. Поскольку все корни многочлена $f(x)$ имеют кратность один, то α сепарабелен над k (см. 2.51). Таким образом, K — сепарабельное расширение поля k. Поскольку $f(x)$ разлагается на линейные множители, то минимальный многочлен любого элемента $\alpha \in K$ над k разлагается на линейные множители. Таким образом, K — нормальное расширение поля k. Следовательно, K — расширение Галуа поля k. Поскольку степень $f(x)$ меньше порядка группы, любой элемент $\alpha \in K$ имеет степень меньшую n. Отсюда, $[K : k] \leq n$. Согласно теореме 2.54 $n \leq [K : k]$. Следовательно, $[K : k] = n$ и G — группа Галуа расширения K над k. □

Следствие 3.6. *Пусть K — конечное расширение Галуа поля k, G — его группа Галуа. Тогда любая подгруппа $H \subset G$ принадлежит некоторому полю E, такому, что $k \subset E \subset K$.*

Доказательство. Пусть $E = K^H$. Согласно теореме 3.5 K — расширение Галуа поля E и $H = G(K/E)$. □

Теорема 3.7. *Пусть K — расширение Галуа поля k, G — его группа Галуа. Пусть E — промежуточное поле, $k \subset E \subset K$, и $H = G(K/E)$. Расширение E над k нормально тогда и только тогда, когда H — нормальная подгруппа в G. Более того, $G(E/k) \cong G/H$.*

Доказательство. Пусть E — нормальное расширение поля k и $G' = G(E/k)$. Тогда отображение ограничения $\sigma \to \sigma|_F$ отображает G в G'. Ядром этого отображения, по определению, является группа H. Следовательно, H — нормальная подгруппа. Пусть $\tau \in G'$. Тогда τ продолжается до вложения K в $\bar{K}$, которое должно быть автоморфизмом поля K. Следовательно, отображение ограничения сюръективно. Отсюда, $G(E/k) \cong G/H$. Предположим, что E не нормально над k. Тогда, согласно теореме 2.31, существует вложение τ поля E в K над k, которое не является автоморфизмом, т.е. $\tau E \neq E$. Продолжим τ до автоморфизма поля K. Пусть $\sigma \in H$. Тогда $\tau\sigma\tau^{-1}$ — элемент группы $G(K/(\tau F))$. Таким образом, группы Галуа $G(K/F)$ и $G(K/(\tau F))$ сопряжены и, принадлежа разным полям, не могут совпадать. □

Определение 3.8. Расширение Галуа называется *абелевым* (*циклическим*), если группа Галуа абелева (циклическая).

Утверждение 3.9. *Пусть K — абелево (циклическое) расширение Галуа поля k, и E — промежуточное поле, $k \subset E \subset K$. Тогда E — абелево (циклическое) расширение Галуа поля k.*

Доказательство. Следует из теоремы 3.7. □

Суммируя доказанные утверждения, мы получаем основную теорему теории Галуа.

Теорема 3.10. *Пусть K — конечное расширение Галуа поля k, G — его группа Галуа. Тогда между множеством подполей E в K, содержащих k, и множеством подгрупп H в G существует биективное соответствие, задаваемое $E = K^H$. Поле E будет расширением Галуа поля k тогда и только тогда, когда H — нормальная подгруппа в G. Более того, $G(E/k) \cong G/H$.*

Пусть k — поле, $f(x) \in k[x]$. Пусть K — поле разложения многочлена $f(x)$, и G — группа Галуа поля K над k. Тогда G называется *группой Галуа многочлена* $f(x)$. Элементы из G переставляют корни многочлена $f(x)$. Таким образом, мы имеем инъективный гомоморфизм группы G в группу S_n.

Пример 3.11. Пусть k — поле и $char(k) \neq 2$, a не является квадратом в k. Тогда многочлен $f(x) = x^2 - a$ неприводим. Поскольку $char(k) \neq 2$, то $f(x)$ сепарабелен. Его группа Галуа — циклическая группа порядка два.

Пример 3.12. Пусть k — поле и $char(k) \neq 2, 3$. Пусть $f(x)$ — неприводимый кубический многочлен, G — его группа Галуа. Если α — корень многочлена $f(x)$. Тогда $[k(\alpha) : k] = 3$. Поскольку G — подгруппа S_3, то G либо $\mathbb{Z}_3$, либо S_3. Пусть $\alpha_1, \alpha_2, \alpha_3$ — различные корни $f(x)$. Рассмотрим

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3), \quad \Delta = \delta^2.$$

Пусть $\sigma \in G$. Заметим, что $\sigma\delta = \pm\delta$, $\sigma\Delta = \Delta$. Следовательно, $\Delta \in k$. Заметим, что множество σ, которые оставляют δ на месте, это в точности четные перестановки. Таким образом, $G = S_3$ тогда и только тогда, когда $\delta \notin k$, т.е. Δ не является квадратом.

Пусть k — поле. Элемент $\zeta \in k$ называется *корнем из единицы* степени n, если $\zeta^n = 1$.

Замечание 3.13. Пусть k — поле характеристики p. Тогда уравнение $x^{p^m} = 1$ имеет только один корень, а именно 1. Следовательно, в поле характеристики p нет корней p^m-й степени из 1, кроме 1.

Пусть n — натуральное число, взаимно простое с характеристикой поля k. Тогда многочлен $x^n - 1$ имеет n различных корней. Действительно, его производная равна nx^{n-1}, и обращается в ноль только при $x = 0$. Таким образом, $x^n - 1$ не имеет кратных корней.

Следовательно, в $\bar{k}$ существуют n различных корней n-й степени из единицы. Они образуют циклическую группу. Образующие этой группы называются *примитивными* или *первообразными* корнями n-й степени из единицы.

Лемма 3.14 (лемма Гаусса). *Пусть $f(x)$ и $g(x)$ — многочлены с целыми коэффициентами. Пусть a — наибольший общий делитель коэффициентов многочлена $f(x)$, b — наибольший общий делитель коэффициентов многочлена $g(x)$, c — наибольший общий делитель коэффициентов многочлена $f(x)g(x)$. Тогда $c = ba$.*

Доказательство. Достаточно доказать, что если $a = b = 1$, то $c = 1$. Предположим, что c делится на простое число p. Пусть

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0.$$

Пусть r — наименьшее число такое, что a_r не делится на p, s — наименьшее число такое, что b_s не делится на p. Рассмотрим коэффициент при x^{r+s} в $f(x)g(x)$. Он равен

$$c_{r+s} = a_r b_s + a_{r+1}b_{s-1} + a_{r+2}b_{s-2} + \cdots + a_{r-1}b_{s+1} + a_{r-2}b_{s+2} + \cdots .$$

Заметим, что все слагаемые, кроме $a_r b_s$ делятся на p, а $a_r b_s$ не делится на p. Тогда c_{r+s} также не делится на p. □

Теорема 3.15. *Пусть ζ — примитивный корень n-й степени из единицы. Тогда $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$, где $\varphi(n)$ — функция Эйлера.*

Доказательство. Пусть $f(x)$ — минимальный многочлен элемента ζ над $\mathbb{Q}$. Тогда $f(x)$ делит $x^n - 1$, т.е. $x^n - 1 = f(x)g(x)$. Из леммы Гаусса следует, что $f(x)$ и $g(x)$ — многочлены с целыми коэффициентами. Пусть p — простое число, не делящее n. Тогда ζ^p — примитивный корень n-й степени из единицы. Более того, все примитивные корни n-й степени из единицы могут быть получены последовательным возведением ζ в простые степени с показателями, не делящими n. Докажем, что ζ^p — корень многочлена $f(x)$. Предположим, что ζ^p не является корнем многочлена $f(x)$. Тогда ζ^p — корень многочлена $g(x)$. Тогда ζ — корень многочлена $g(x^p)$. Следовательно, $g(x^p)$ делится на $f(x)$, т.е. $g(x^p) = f(x)h(x)$. Заметим, что $h(x)$ имеет целые коэффициенты. Поскольку $a^p = a \pmod p$, то $g(x^p) = (g(x))^p \pmod p$. Отсюда,

$$(g(x))^p = f(x)h(x) \pmod p.$$

Тогда многочлены $\bar{f}$ и $\bar{g}$ над $\mathbb{Z}_p$, полученные редукцией по модулю p, не являются взаимно простыми. Следовательно, многочлен

x^n-1 имеет кратные корни в расширении $\mathbb{Z}_p$. С другой стороны, его производная не равна нулю в поле характеристики p. Противоречие. Таким образом, ζ^p — корень многочлена $f(x)$. Следовательно, все примитивные корни n-й степени из единицы являются корнями $f(x)$. Тогда степень $f(x)$ не меньше $\varphi(n)$, а, следовательно, равна $\varphi(n)$. □

Теорема 3.16. *Пусть ζ — примитивный корень n-й степени из единицы. Тогда $G(\mathbb{Q}(\zeta)/\mathbb{Q}) = U(n)$, где $U(n)$ — группа единиц кольца $\mathbb{Z}_n$.*

Замечание 3.17. Группа единиц кольца $\mathbb{Z}_n$ это в точности множество обратимых элементов в $\mathbb{Z}_n$. Поскольку элемент $k \in \mathbb{Z}_n$ обратим тогда и только тогда, когда $(k, n) = 1$, то порядок группы $U(n)$ равен $\varphi(n)$.

Доказательство. Пусть $\sigma \in G$ и ζ — примитивный корень из единицы степени n. Тогда $\sigma(\zeta)$ определяет автоморфизм σ. Заметим, что $\sigma(\zeta) = \zeta^k$ — примитивный корень из единицы степени n. Тогда $(k, n) = 1$. Определим $\psi\colon G \to U(n)$, как $\psi(\sigma) = k$. Если $\sigma'(\zeta) = \zeta^{k'}$, то

$$\sigma'(\sigma(\zeta)) = \sigma'(\zeta^k) = (\zeta^{k'})^k = \zeta^{kk'}.$$

Таким образом, ψ — гомоморфизм. Если $\psi(\sigma) = 1$, то $\sigma(\zeta) = \zeta$ и, следовательно, σ — тождественное отображение. Таким образом, ψ — инъективный гомоморфизм. Поскольку $|G(\mathbb{Q}(\zeta)/\mathbb{Q})| = |U(n)| = \varphi(n)$, то ψ — изоморфизм. □

Теорема 3.18. *Пусть k — поле, содержащее примитивный корень n-й степени из единицы, и n взаимно просто с характеристикой поля. Пусть $a \in k$. Пусть α — корень многочлена $x^n - a$. Тогда $k(\alpha)$ — циклическое расширение степени d и $\alpha^d \in k$. В частности, если $x^n - a$ неприводим, то $G(k(\alpha)/k)$ — циклическая группа порядка n.*

Доказательство. Пусть ζ — примитивный корень n-й степени из единицы. Заметим, что корни $x^n - a$ есть $\alpha\zeta^k$. Поскольку они все принадлежат $k(\alpha)$, то $k(\alpha)$ — нормальное расширение k. Более того, $\sigma(\alpha) = \zeta^k\alpha$. Определим $\psi\colon G \to \mathbb{Z}_n$, как $\psi(\sigma) = k$. Пусть $\sigma'(\alpha) = \alpha\zeta^{k'}$. Поскольку все элементы группы Галуа оставляют поле k на месте, а, следовательно и все корни из единицы, то

$$\sigma'(\sigma(\alpha)) = \sigma'(\alpha\zeta^k) = \alpha\zeta^{k'}\zeta^k = \alpha\zeta^{k+k'}.$$

Таким образом, ψ — гомоморфизм. Если $\psi(\sigma) = 0$, то $\sigma(\alpha) = \alpha$ и, следовательно, σ — тождественное отображение. Таким образом, ψ

— инъективный гомоморфизм. Следовательно, $G(k(\alpha)/k)$ — циклическая группа, порядок который делит n. Пусть $|G(k(\alpha)/k)| = d$, и σ — порождающий элемент группы $G(k(\alpha)/k)$. Пусть $\sigma(\alpha) = \zeta^k\alpha$. Тогда k имеет порядок d в $\mathbb{Z}_n$. Таким образом,

$$\sigma(\alpha^d) = (\zeta^k\alpha)^d = \zeta^{kd}\alpha^d = \alpha^d.$$

Поскольку α^d — неподвижный элемент, то $\alpha^d \in k$. Если $x^n - a$ неприводим, то $[k(\alpha) : k] = n$. Следовательно, $|G(k(\alpha)/k)| = n$. Отсюда, $G(k(\alpha)/k) = \mathbb{Z}_n$. □

Следствие 3.19. *Пусть k — поле, содержащее примитивный корень q-й степени из единицы, где q — простое число, взаимно простое с характеристикой поля. Пусть $a \in k$. Тогда многочлен $x^q - a$ либо неприводим, либо раскладывается на линейные множители.*

2. Норма и след

Пусть K — конечное сепарабельное расширение поля k, $[K : k] = n$. Пусть $\sigma_1, \sigma_2, \ldots, \sigma_n$ — различные вложения K в алгебраическое замыкание $\bar{k}$ поля k. Пусть $\alpha \in K$. Тогда определим *норму* α формулой

$$N_k^K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Аналогично определим *след* α формулой

$$\mathrm{Tr}_k^K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Теорема 3.20. *Норма является мультипликативным гомоморфизмом K^* в k^*. След является аддитивным гомоморфизмом K в k.*

Доказательство. Заметим, что любой автоморфизм σ оставляет норму и след на месте. Следовательно, $N_k^K(\alpha) \in k^*$, если $\alpha \neq 0$, и $\mathrm{Tr}_k^K(\alpha) \in k$. Очевидно, что

$$N_k^K(\alpha_1\alpha_2) = \prod_{i=1}^{n} \sigma_i(\alpha_1\alpha_2) = \prod_{i=1}^{n} \sigma_i(\alpha_1)\sigma_i(\alpha_2) = N_k^K(\alpha_1)N_k^K(\alpha_2).$$

Аналогично,

$$\mathrm{Tr}_k^K(\alpha_1+\alpha_2) = \sum_{i=1}^{n} \sigma_i(\alpha_1+\alpha_2) = \sum_{i=1}^{n} \sigma_i(\alpha_1)+\sigma_i(\alpha_2) = \mathrm{Tr}_k^K(\alpha_1)+\mathrm{Tr}_k^K(\alpha_2).$$

$\square$

Теорема 3.21. *Пусть F — конечное сепарабельное расширение поля k, E — конечное сепарабельное расширение поля F. Тогда*

$$N_k^E = N_k^F \circ N_F^E, \quad \mathrm{Tr}_k^E = \mathrm{Tr}_k^F \circ \mathrm{Tr}_F^E .$$

Доказательство. Пусть $\{\tau_i\}$ — семейство вложений F в $\bar{k}$ над k. Продолжим каждое τ_i до вложения E в $\bar{k}$ (будем обозначать это продолжение также через τ_i). Пусть $\{\sigma_i\}$ — семейство вложений E в $\bar{k}$ над F. Пусть σ — вложение E в $\bar{k}$ над k. Поскольку ограничение σ на F совпадает с некоторым τ_j, то $\tau_j^{-1}\sigma$ оставляет F неподвижным. Таким образом, существует σ_i такое, что $\tau_j^{-1}\sigma = \sigma_i$. Отсюда, $\sigma = \tau_j\sigma_i$. Следовательно, семейство $\{\tau_j\sigma_i\}$ задает все различные вложения E в $\bar{k}$ над k. Отсюда,

$$N_k^E(\alpha) = \prod_{i,j} \tau_j\sigma_i(\alpha) = \prod_j \tau_j \left(\prod_i \sigma_i(\alpha) \right) = N_k^F(N_F^E(\alpha)),$$

$$\mathrm{Tr}_k^E(\alpha) = \sum_{i,j} \tau_j\sigma_i(\alpha) = \sum_j \tau_j \left(\sum_i \sigma_i(\alpha) \right) = \mathrm{Tr}_k^F(\mathrm{Tr}_F^E(\alpha)).$$

$\square$

Теорема 3.22. *Пусть $K = k(\alpha)$ и $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ — минимальный многочлен элемента α. Тогда*

$$N_k^K(\alpha) = (-1)^n a_0, \quad \mathrm{Tr}_k^K(\alpha) = -a_{n-1}.$$

Доказательство. Пусть

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

в $\bar{k}$. Тогда вложение $\sigma\colon k(\alpha) \to \bar{k}$ задается $\sigma(\alpha) = \alpha_i$. Таким образом,

$$N_k^K(\alpha) = \prod_{i=1}^n \sigma_i(\alpha) = \prod_{i=1}^n \alpha_i = (-1)^n a_0.$$

Аналогично,

$$\mathrm{Tr}_k^K(\alpha) = \sum_{i=1}^n \sigma_i(\alpha) = \sum_{i=1}^n \alpha_i = -a_{n-1}.$$

$\square$

Теперь нам понадобятся некоторые факты о характерах группы.

Определение 3.23. Пусть G — группа и K — поле. *Характером* группы G в K называется гомоморфизм $\chi\colon G \to K^*$. Характеры $\chi_1, \chi_2, \ldots, \chi_n$ называются *линейно независимыми* над K, если равенство

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0$$

выполнено тогда и только тогда, когда все $a_i = 0$. Здесь все $a_i \in K$, равенство нулю $a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n$ понимается, как тождественное равенство, т.е.

$$f(g) = a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_n\chi_n(g) = 0,$$

для любого $g \in G$.

Теорема 3.24. *Пусть $\chi_1, \chi_2, \ldots, \chi_n$ — различные характеры G в K. Тогда они линейно независимы над K.*

Доказательство. Докажем по индукции. Один характер, очевидно, линейно независим. Предположим, что мы доказали для $n-1$ характера. Предположим, что выполнено

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0$$

и все $a_i \neq 0$. Поскольку характеры χ_1 и χ_2 различны, то существует $y \in G$ такой, что $\chi_1(y) \neq \chi_2(y)$. Для всех $g \in G$ имеем

$$a_1\chi_1(yg) + a_2\chi_2(yg) + \cdots + a_n\chi_n(yg) = 0.$$

Отсюда,

$$a_1\chi_1(y)\chi_1 + a_2\chi_2(y)\chi_2 + \cdots + a_n\chi_n(y)\chi_n = 0.$$

Разделим это равенство на $\chi_1(y)$ и вычтем из

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0.$$

Получаем

$$\left(a_2 - a_2\frac{\chi_2(y)}{\chi_1(y)}\right)\chi_2 + \cdots + \left(a_n - a_n\frac{\chi_n(y)}{\chi_1(y)}\right)\chi_n = 0.$$

Первый коэффициент отличен от нуля. Таким образом мы получили, что характеры $\chi_1, \chi_2, \ldots, \chi_{n-1}$ линейно зависимы. Противоречие. □

Теорема 3.25 (теорема Гильберта 90). *Пусть K — циклическое расширение поля k с группой Галуа G. Пусть σ — образующая этой группы, и $\beta \in K$. Норма $N_k^K(\beta) = 1$ тогда и только тогда, когда существует $\alpha \neq 0$ в K, такой, что $\beta = \frac{\alpha}{\sigma\alpha}$.*

Доказательство. Предположим, что такой элемент существует. Тогда $N(\beta) = \frac{N(\alpha)}{N(\sigma\alpha)}$. Поскольку норма — это произведение по всем автоморфизмам из G, то применение σ лишь переставляет эти автоморфизмы. Следовательно, $N(\sigma\alpha) = N(\alpha)$. Тогда $N(\beta) = 1$.

Предположим, что $N(\beta) = 1$. Согласно теореме 3.24 отображение

$$id + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \cdots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}$$

не равно тождественно нулю (здесь id — тождественное отображение). Тогда существует $\gamma \in K$ такое, что

$$\alpha = \gamma + \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \cdots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}(\gamma)$$

не равен нулю. Применим $\beta\sigma$ к α. Получаем

$$\beta\sigma(\alpha) = \beta\sigma(\gamma) + \beta\sigma(\beta)\sigma^2(\gamma) + \cdots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}(\beta)\sigma^n(\gamma).$$

Заметим, что

$$\beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}(\beta) = N(\beta) = 1$$

и $\sigma^n(\gamma) = \gamma$. Таким образом, $\beta\sigma(\alpha) = \alpha$. Отсюда, $\beta = \frac{\alpha}{\sigma\alpha}$. □

Теорема 3.26. *Пусть k — поле, содержащее примитивный корень n-й степени из единицы, и n взаимно просто с характеристикой поля. Пусть K — циклическое расширение степени n. Тогда существуют $\alpha \in K$, $a \in k$ такие, что $K = k(\alpha)$ и α — корень уравнения $x^n - a = 0$.*

Доказательство. Пусть ζ — примитивный корень из единицы и K — циклическое расширение поля k. Пусть σ — образующая группы G. Заметим, что $N(\zeta^{-1}) = (\zeta^{-1})^n = 1$. Согласно теореме Гильберта 90, существует $\alpha \in K$ такой, что $\sigma\alpha = \zeta\alpha$. Поскольку $\zeta \in k$, то $\sigma^k\alpha = \zeta^k\alpha$. Следовательно, $[k(\alpha) : k] \geq n$. Поскольку $[K : k] \geq n$, то $K = k(\alpha)$. Более того,

$$\sigma(\alpha^n) = (\sigma(\alpha))^n = (\zeta\alpha)^n = \alpha^n.$$

Отсюда, $\alpha^n \in k$. □

Теперь рассмотрим другой вариант теоремы Гильберта 90.

Теорема 3.27 (теорема Гильберта 90). *Пусть K — циклическое расширение поля k с группой Галуа G. Пусть σ — образующая этой группы, и $\beta \in K$. След $\mathrm{Tr}_k^K(\beta) = 0$ тогда и только тогда, когда существует $\alpha \in K$, такой, что $\beta = \alpha - \sigma\alpha$.*

Доказательство. Предположим, что такой элемент существует. Тогда $\mathrm{Tr}_k^K(\beta) = \mathrm{Tr}_k^K(\alpha - \sigma\alpha)$. Поскольку след — это сумма по всем автоморфизмам из G, то применение σ лишь переставляет эти автоморфизмы. Следовательно, $\mathrm{Tr}(\sigma\alpha) = \mathrm{Tr}(\alpha)$. Тогда $\mathrm{Tr}(\beta) = 0$.

Предположим, что $\mathrm{Tr}(\beta) = 0$. Заметим, что существует $\gamma \in K$ такое, что $\mathrm{Tr}(\gamma) \neq 0$. Положим

$$\alpha = \frac{1}{\mathrm{Tr}(\gamma)}(\beta\sigma(\gamma)+(\beta+\sigma(\beta))\sigma^2(\gamma)+\cdots+(\beta+\sigma(\beta)+\cdots+\sigma^{n-2}(\beta))\sigma^{n-1}(\gamma)).$$

Тогда $\beta = \alpha - \sigma\alpha$. □

3. Резольвента

Определение 3.28. Пусть k — поле, содержащее корни n-й степени из единицы. Предположим, что $char(k) = 0$. Пусть K — циклическое расширение поля k, и σ — порождает группу Галуа $G(K/k)$. Пусть $x \in K$, ζ — корень n-й степени из единицы. Тогда выражение

$$(\zeta, x) = x + \zeta\sigma(x) + \zeta^2\sigma^2(x) + \cdots + \zeta^{n-1}\sigma^{n-1}(x)$$

называется *резольвентой Лагранжа.*

Утверждение 3.29. (1) $\sigma((\zeta, x)) = \zeta^{-1}(\zeta, x)$;
(2) $\sigma((1, x)) = \mathrm{Tr}(x) \in k$;
(3) $(\zeta, x)^n \in k$;
(4) $(\zeta, x)(\zeta^{-1}, x) \in k$.

Доказательство. Первые два свойства очевидны. Докажем (3). Получаем

$$\sigma((\zeta, x)^n) = \sigma^n((\zeta, x)) = (\zeta^{-1}(\zeta, x))^n = (\zeta, x)^n.$$

Следовательно, $(\zeta, x)^n$ — неподвижный элемент, а значит $(\zeta, x)^n \in k$. Докажем (4). Получаем

$$\sigma((\zeta, x)(\zeta^{-1}, x)) = \sigma((\zeta, x))\sigma((\zeta^{-1}, x)) = \zeta^{-1}(\zeta, x)\zeta(\zeta, x) = (\zeta, x).$$

Следовательно, $(\zeta, x)(\zeta^{-1}, x)$ — неподвижный элемент, а значит $(\zeta, x)(\zeta^{-1}, x) \in k$. □

Рассмотрим кубическое уравнение $x^3 + px + q = 0$. Пусть $k = \mathbb{Q}(p, q, j)$, где j — кубический корень из единицы. Заметим, что любое кубическое уравнение приводится к такому виду. Пусть α, β, γ — корни этого уравнения. Пусть $d = (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)$. Заметим, что $k(\alpha, \beta, \gamma) = k(\alpha, d)$ и $d^2 = -4p^3-27q^2$. Предположим, что группа Галуа этого уравнения есть S_3. Пусть K — поле разложение многочлена x^3+px+q, и E — неподвижное поле группы A_3. Тогда E — расширение степени два над k, т.е. $E = k(s)$. Пусть σ — порождающий элемент группы A_3. Мы можем считать, что $\sigma = (\alpha\beta\gamma)$, т.е. σ переставляет по кругу корни уравнения $x^3+px+q = 0$. Поскольку K — нормальное расширение поля k, то K — нормальное расширение поля E. Следовательно, K — расширение Галуа поля E. Заметим, что $G(K/E) = A_3$. Таким образом, K — циклическое расширение поля E. Согласно теореме 3.26 существует элемент $s' \in K$ такой, что $s'^3 \in E$ и $K = E(s')$. Найдем s и s'. Заметим, что $\sigma d = d$. Таким образом, $d \in E$. Поскольку транспозиция $(\alpha\beta)$ переводит d в $-d$, то $d \notin K$. Рассмотрим автоморфизм $\tau = id + j\sigma + j^2\sigma^2$. Согласно теореме 3.24 τ ненулевой. Более того, $\tau(\alpha) \neq 0$. Действительно, если $\tau(\alpha) = 0$, то $\tau(\beta) = \tau(\sigma(\alpha)) = j^2\tau(\alpha) = 0$. Аналогично, $\tau(\gamma) = 0$. Следовательно, $q\tau(1) = \tau(q) = \tau(\alpha\beta\gamma) = 0$ и $\tau = 0$. Рассмотрим $(j, \alpha) = \alpha + j\beta + j^2\gamma = \tau(\alpha)$. Поскольку $\sigma((j, \alpha)) = j^2(j, \alpha) \neq (j, \alpha)$, то $(j, \alpha) \notin E$. Согласно 3.29 $(j, \alpha)^3 \in E$. Отсюда, $K = L((j, \alpha))$.

4. Нормальный базис

Пусть A — абелева группа, k — поле и $\lambda_1, \lambda_2, \cdots, \lambda_n \colon A \to k$ — аддитивные гомоморфизмы. Будем говорить, что $\lambda_1, \lambda_2, \cdots, \lambda_n$ *алгебраически зависимы*, если существует многочлен $f(x_1, x_2, \ldots, x_n)$ над k такой, что

$$f(\lambda_1(a), \lambda_2(a), \ldots, \lambda_n(a)) = 0$$

для всех $a \in A$. Многочлен $f(x_1, x_2, \ldots, x_n)$ называется *аддитивным*, если он индуцирует аддитивный гомоморфизм k^n в k.

Теорема 3.30. *$\lambda_1, \lambda_2, \cdots, \lambda_n \colon A \to k$ — аддитивные гомоморфизмы абелевой группы A в поле k. Если эти гомоморфизмы алгебраически зависимы, то существует аддитивный многочлен $f(x_1, x_2, \ldots, x_n)$ над k такой, что*

$$f(\lambda_1(a), \lambda_2(a), \ldots, \lambda_n(a)) = 0$$

для всех $a \in A$.

Доказательство. Мы докажем эту теорему для случая бесконечного поля. Пусть $f(x_1, x_2, \ldots, x_n)$ — многочлен наименьшей возможной степени такой, что

$$f(\lambda_1(a), \lambda_2(a), \ldots, \lambda_n(a)) = 0$$

для всех $a \in A$. Пусть $X = (x_1, x_2, \ldots, x_n)$, $Y = (y_1, y_2, \ldots, y_n)$, $\Lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$. Рассмотрим $g(X, Y) = f(X+Y) - f(X) - f(Y)$.

Заметим, что

$$g(\Lambda(a), \Lambda(b)) = f(\Lambda(a+b)) - f(\Lambda(a)) - f(\Lambda(b)) = 0$$

для любых $a, b \in A$. Нам нужно доказать, что g — нулевой многочлен. Заметим, что степень $g(X, Y)$ по X строго меньше степени $f(X)$. Аналогично по Y. Предположим, что g не равен тождественно нулю. Рассмотрим два случая.

3.31. Имеем $g(\xi, \Lambda(b)) = 0$ для всех $\xi \in k^n$, $b \in A$. По предположению, существует $\xi \in k^n$ такой, что $g(\xi, Y)$ не равен тождественно нулю. Положим $P(Y) = g(\xi, Y)$. Тогда

$$P(\lambda_1(a), \lambda_2(a), \dots, \lambda_n(a)) = 0$$

для всех $a \in A$. С другой стороны, степень P меньше степени f. Противоречие.

3.32. Существуют $\xi \in k^n$, $b \in A$ такие, что $g(\xi, \Lambda(b)) \neq 0$. Положим $P(X) = g(X, \Lambda(b))$. Тогда $P(X)$ — ненулевой многочлен. С другой стороны, $P(\Lambda(a)) = 0$ для любого $a \in A$, и степень многочлена P меньше степени f. Противоречие.

Таким образом, g индуцирует нулевую функцию. Поскольку поле бесконечно, то g — нулевой многочлен. □

Утверждение 3.33. *Пусть $f(x_1, x_2, \dots, x_n)$ — аддитивный многочлен. Тогда*

$$f(x_1, x_2, \dots, x_n) = f_1(x_1) + f_2(x_2) + \dots + f_n(x_n),$$

где $f_i(x)$ — аддитивные многочлены от одной переменной.

Доказательство. Пусть $f_i(x_i) = f(0, \dots, 0, x_i, 0, \dots, 0)$. Тогда $f_i(x)$ — аддитивные многочлены от одной переменной и

$$f(x_1, x_2, \dots, x_n) = f_1(x_1) + f_2(x_2) + \dots + f_n(x_n).$$

□

Утверждение 3.34. *Пусть $f(x)$ — аддитивный многочлен. Тогда*

$$f(x) = \sum_{i=1}^{m} a_i x^{p^i},$$

где p — характеристика поля. Если $char(k) = 0$, то $f(x) = ax$.

Доказательство. Пусть $f(x) = \sum\limits_{i=1}^{n} a_i x^i$. Тогда

$$g(x, y) = f(x + y) - f(x) - f(y) = \sum_{i=1}^{n} a_i((x + y)^i - x^i - y^i) = 0.$$

Пусть $a_i \neq 0$. Поскольку $(x+y)^i - x^i - y^i$ содержит $ix^{i-1}y$, то $g(x, y)$ содержит $a_i i x^{i-1} y$. С другой стороны, $g(x, y)$ — нулевой многочлен. Следовательно, i делится на характеритику поля. Пусть $i = p^m s$. Тогда

$$(x + y)^i - x^i - y^i = (x^{p^m} + y^{p^m})^s - (x^{p^m})^s - (y^{p^m})^s.$$

Отсюда, рассуждая аналогично, $s = 1$. $\square$

Теорема 3.35. *Пусть K — бесконечное поле и $\sigma_1, \sigma_2, \ldots, \sigma_n$ — различные элементы конечной группы автоморфизмов поля K. Тогда $\sigma_1, \sigma_2, \ldots, \sigma_n$ алгебраически независимы над K.*

Доказательство. В случае характеристики ноль, теорема следует из 3.24, 3.30, 3.33, 3.34. Пусть характеристика $p > 0$, и $\sigma_1, \sigma_2, \ldots, \sigma_n$ алгебраически зависимы. Согласно теореме 3.30 существует аддитивный многочлен $f(x_1, x_2, \ldots, x_n)$ такой, что $f \neq 0$, но

$$f(\sigma_1(a), \sigma_2(a), \ldots, \sigma_n(a)) = 0$$

для любого $a \in K$. В силу 3.33 и 3.34 мы можем записать

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} (\sigma_i(a))^{p^j} = 0$$

для любого $a \in K$. Согласно 3.24 гомоморфизмы $x \to (\sigma_i(x))^{p^j}$ не могут быть различными. Таким образом, существуют i_1, i_2, j_1, j_2 такие, что $(\sigma_{i_1}(x))^{p^{j_1}} = (\sigma_{i_2}(x))^{p^{j_2}}$, при этом либо $i_1 \neq i_2$, либо $j_1 \neq j_2$. Пусть $j_1 \leq j_2$. Заметим, что извлечение корня p-й степени в поле характеристики p однозначно. Тогда $\sigma_{i_1}(x) = (\sigma_{i_2}(x))^{p^{j_2 - j_1}}$. Положим $\sigma = \sigma_{i_2}^{-1} \sigma_{i_1}$. Тогда $\sigma(x) = x^{p^{j_2 - j_1}}$. Поскольку σ — элемент конечной группы, то существует n такое, что $\sigma^n = id$. Тогда $x = x^{p^{n(j_2 - j_1)}}$ для всех $x \in K$. Поскольку K — бесконечное поле, то $j_2 = j_1$. Отсюда, $\sigma_{i_1}(x) = \sigma_{i_2}(x)$ для всех $x \in K$. Противоречие. $\square$

Теорема 3.36. *Пусть K — конечное расширение Галуа поля k, G — его группа Галуа. Пусть $n = |G|$, $\sigma_1, \sigma_2, \ldots, \sigma_n$ — элементы группы G. Тогда существует элемент $w \in K$ такой, что $\sigma_1 w, \sigma_2 w, \ldots, \sigma_n w$ — базис K над k.*

Доказательство. Мы докажем эту теорему для случая бесконечного поля. Рассмотрим множество переменных $x_1 = x_{\sigma_1}, \ldots, x_n = x_{\sigma_n}$. Пусть $f(x_1, x_2, \ldots, x_n) = \det(t_{ij})$, где $t_{ij} = x_{\sigma_i^{-1}\sigma_j}$. Заметим, что $f(x_1, x_2, \ldots, x_n)$ не является тождественным нулем, что видно если подставить 1 вместо x_e и 0 вместо остальных x_i. Согласно теореме 3.35 существует $w \in K$ такое, что $\det(\sigma_i^{-1}\sigma_j(w)) \neq 0$. Докажем, что $\sigma_1 w, \sigma_2 w, \ldots, \sigma_n w$ линейно независимы. Предположим, что существуют $a_1, a_2, \ldots a_n \in k$ такие, что

$$a_1\sigma_1(w) + a_2\sigma_2(w) + \cdots + a_n\sigma_n(w) = 0.$$

Применим σ_i^{-1} к этому соотношению для каждого $i = 1, 2, \ldots, n$. Получим систему линейных уравнений относительно переменных $a_1, a_2, \ldots a_n$,

$$\begin{cases} \sigma_1^{-1}\sigma_1(w)a_1 + \sigma_1^{-1}\sigma_2(w)a_2 + \cdots + \sigma_1^{-1}\sigma_n(w)a_n = 0 \\ \sigma_2^{-1}\sigma_1(w)a_1 + \sigma_2^{-1}\sigma_2(w)a_2 + \cdots + \sigma_2^{-1}\sigma_n(w)a_n = 0 \\ \cdots \quad \cdots \quad \cdots \\ \sigma_n^{-1}\sigma_1(w)a_1 + \sigma_n^{-1}\sigma_2(w)a_2 + \cdots + \sigma_n^{-1}\sigma_n(w)a_n = 0. \end{cases}$$

Определитель этой системы не равен нулю. Следовательно, все $a_i = 0$. □

5. Радикальные расширения

Теорема 3.37 (теорема Артина–Шрейера). *Пусть k — поле характеристики p. Тогда если K — циклическое расширение k степени p, то существует такой элемент $\alpha \in K$ такой, что $K = k(\alpha)$, и α — корень многочлена $x^p - x - a$, $a \in k$. Обратно, для любого $a \in k$ многочлен $f(x) = x^p - x - a$ либо имеет корень в k, и тогда все его корни лежат в k, либо $f(x)$ неприводим. В последнем случае, если α — корень $f(x)$, то $k(\alpha)$ — циклическое расширение k степени p.*

Доказательство. Пусть K — циклическое расширение k степени p. Тогда

$$\mathrm{Tr}(-1) = (-1) + (-1) + \cdots + (-1) = -p = 0.$$

Согласно теореме 3.27 существует $\alpha \in K$ такой, что $-1 = \alpha - \sigma\alpha$. Отсюда, $\sigma\alpha = \alpha + 1$. Тогда $\sigma^i\alpha = \alpha + i$ при $i = 1, 2, \ldots, p$. Таким образом, σ^i — различные вложения поля $k(\alpha)$. Отсюда, $[k(\alpha) : k] \geq p$. Тогда $K = k(\alpha)$. Заметим, что

$$\sigma(\alpha^p - \alpha) = (\sigma(\alpha))^{-}\sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha.$$

Следовательно, $\alpha^p - \alpha \in k$. Таким образом, α — корень многочлена $x^p - x - a$, $a \in k$.

Обратно. Пусть α — корень многочлена $x^p - x - a$, $a \in k$. Заметим, что

$$(\alpha + i)^p - (\alpha + i) - a = \alpha^p + i - \alpha - i - a = \alpha^p - \alpha - a = 0,$$

где $i = 1, 2, \ldots, p$. Следовательно, $\alpha + i$ — корни многочлена $x^p - x - a$. Таким образом, $x^p - x - a$ имеет p различных корней, и если один корень лежит в k, то все его корни лежат в k. Предположим, что ни один корень не лежит в k. Докажем, что многочлен $x^p - x - a$ неприводим. Предположим, что

$$x^p - x - a = f(x)g(x),$$

где $1 \leq \deg f < p$. Поскольку

$$x^p - x - a = (x - \alpha)(x - \alpha - 1)(x - \alpha - 2) \cdots (x - \alpha - (p - 1)),$$

то

$$f(x) = (x - \alpha - i_1)(x - \alpha - i_2) \cdots (x - \alpha - i_d),$$

где $d = \deg f$. Коэффициент при x^{d-1} будет равен $-d\alpha + j$, где j — некоторое целое число, т.е. $j \in k$. Поскольку $d \neq 0$ в k, то $-d\alpha + j$ не принадлежит k. Противоречие. Таким образом, многочлен $x^p - x - a$ неприводим. Все его корни лежат в $k(\alpha)$. Тогда $k(\alpha)$ — нормальное расширение поля k. Так как $x^p - x - a$ не имеет кратных корней, то $k(\alpha)$ — расширение Галуа поля k. Имеется автоморфизм σ поля $k(\alpha)$, такой, что $\sigma\alpha = \alpha + 1$. Степени σ^i автоморфизма σ дают $\sigma^i(\alpha) = \alpha + i$, т.е. σ^i различны для $i = 0, 1, 2, \ldots, p - 1$. Следовательно, группа Галуа состоит из σ^i, а потому является циклической. $\square$

Определение 3.38. Пусть K — расширение поля k. Будем говорить, что K — *разрешимо в радикалах* (*радикальное расширение*), если существует башня расширений

$$k = K_0 \subset K_1 \subset \cdots \subset K_n = K$$

такая, что каждое расширение K_i над K_{i-1} принадлежит одному из следующих типов

(1) получается присоединением корня многочлена $x^n - a$, где $a \in K_{i-1}$, n взаимно просто с характеристикой;
(2) получается присоединением корня многочлена $x^p - x - a$, где $a \in K_{i-1}$, p — характеристика поля.

Пусть $E = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$, K — расширение поля k. Пусть K и E вложены в поле L. Поле

$$F = KE = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

мы будем называть *подъемом* K над F.

Теорема 3.39. *Пусть K — конечное расширение Галуа поля k, F — произвольное расширение поля k, причем K, F — подполя некоторого поля L. Тогда KF — расширение Галуа поля F. Пусть H — группа Галуа KF над F, G — группа Галуа K над k. Пусть $\sigma \in H$. Тогда ограничение σ на K задает вложение H в группу G.*

Доказательство. Докажем, что KF — нормальное расширение поля F. Пусть σ — вложение KF в $\bar{L}$ над F. Тогда σ тождественно на F, а, следовательно, на k. Поскольку K — нормальное расширение k, то σ — автоморфизм K. Таким образом, σ отображает KF в себя. Следовательно, KF — нормальное расширение поля F. Пусть $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Тогда все α_i сепарабельны. Поскольку $KF = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$, то KF — сепарабельное расширение поля F. Таким образом, KF — расширение Галуа поля F. Пусть H — группа Галуа KF над F. Пусть $\sigma \in H$. Рассмотрим ограничение σ на поле K. Если σ тождественно на K, то σ тождественно на KF (так как всякий элемент из KF может быть представлен в виде комбинации сумм, произведений и отношений элементов из K и F). Следовательно, ограничение σ на K задает инъективный гомоморфизм H в группу G. □

Теорема 3.40. *Пусть K_1, K_2 — конечное расширения Галуа поля k, G_1, G_2 — их группы Галуа соответственно. Предположим, что K_1, K_2 — подполя некоторого алгебраически замкнутого поля L. Тогда K_1K_2 — расширение Галуа над k. Пусть G — группа Галуа поля K_1K_2 над k. Тогда ограничение $\sigma \in G$ на K_1 и K_2 задает инъективный гомоморфизм групп $G \to G_1 \times G_2$ посредством $\sigma \to (\sigma|_{K_1}, \sigma|_{K_2})$.*

Доказательство. Согласно теореме 3.39 K_1K_2 — расширение Галуа поля K_2 (т.е. это расширение нормально и сепарабельно. Поскольку K_2 — сепарабельное расширение поля k, то согласно теореме 2.56 K_1K_2 — сепарабельное расширение поля k. Пусть σ — вложение поля K_1K_2 в поле L над k. Тогда ограничения σ на K_1 и K_2 оставляют эти поля на месте. Следовательно, σ — автоморфизм поля K_1K_2 над k. Таким образом, K_1K_2 — нормально расширение поля k. Следовательно, K_1K_2 — расширение Галуа поля k. Отображение $G \to G_1 \times G_2$ посредством ограничений $\sigma \to (\sigma|_{K_1}, \sigma|_{K_2})$ является гомоморфизмом групп. Если σ тождественен на K_1 K_2, то он очевидно тождественен на K_1K_2. Таким образом, наше отображение инъективно. □

Следствие 3.41. *В условиях теоремы 3.40 предположим, что* $K_1 \cap K_2 = k$. *Тогда отображение* $\sigma \to (\sigma|_{K_1}, \sigma|_{K_2})$ *задает изоморфизм* $G \cong G_1 \times G_2$.

Доказательство. Предположим, что $K_1 \cap K_2 = k$. Пусть $\sigma_1 \in G_1$. Тогда σ_1 продолжается на K_1K_2 над K_2. Таким образом, мы получили, что подгруппа $G_1 \times \{e\}$ лежит в образе нашего гомоморфизма. Аналогично, $\{e\} \times G_2$ лежит в образе нашего гомоморфизма. Следовательно, отображение $\sigma \to (\sigma|_{K_1}, \sigma|_{K_2})$ задает изоморфизм $G \cong G_1 \times G_2$. $\square$

Следствие 3.42. *Пусть* $K_1, K_2, \dots, K_n$ *— конечные расширения Галуа поля* k *с группами Галуа* $G_1, G_2, \dots, G_n$ *соответственно. Предположим, что*

$$K_i \cap (K_1K_2 \cdots K_{i-1}K_{i+1} \cdots K_n) = k$$

для любого i. *Тогда группа Галуа* $K_1K_2 \cdots K_n$ *над* k *изоморфна* $G_1 \times G_2 \times \cdots \times G_n$.

Следствие 3.43. *Пусть* K *— конечное расширения Галуа поля* k *с группой Галуа* G. *Предположим, что* $G = G_1 \times G_2$. *Пусть* K_1 *— неподвижное поле группы* $G_1 \times \{e\}$, K_2 *— неподвижное поле группы* $\{e\} \times G_2$. *Тогда* K_1, K_2 *— конечные расширения Галуа над* k, $K_1 \cap K_2 = k$. *Более того,* $K = K_1K_2$.

Доказательство. Поскольку подгруппы $G_1 \times \{e\}$ и $\{e\} \times G_2$ нормальны в G, то K_1, K_2 — конечные расширения Галуа над k. Пусть $\alpha \in K_1 \cap K_2$ и $\sigma \in G$. Тогда $\sigma = (\sigma_1, \sigma_2)$, $\sigma_1 \in G_1$, $\sigma_2 \in G_2$. Тогда

$$\sigma(\alpha) = (\sigma_1, \sigma_2)(\alpha) = (\sigma_1, e)((e, \sigma_2)(\alpha)) = \alpha.$$

Следовательно, $\alpha \in k$. Заметим, что $K_1K_2 \subset K$. С другой стороны, согласно 3.40 и 3.41, K_1K_2 — конечное расширение Галуа над k с группой Галуа $G \cong G_1 \times G_2$. Следовательно, $K = K_1K_2$. $\square$

Следствие 3.44. *Пусть* K *— конечное расширения Галуа поля* k *с группой Галуа* G. *Предположим, что* $G = G_1 \times G_2 \times \cdots \times G_n$. *Пусть* K_i *— неподвижное поле группы*

$$G_1 \times G_2 \times \cdots G_{i-1} \times \{e\} \times G_{i+1} \times \cdots \times G_n.$$

Тогда K_i *— конечное расширение Галуа над* k,

$$K_i \cap (K_1K_2 \cdots K_{i-1}K_{i+1} \cdots K_n) = k$$

для любого i. *Более того,* $K = K_1K_2 \cdots K_n$.

Определение 3.45. Пусть K — конечное сепарабельное расширение поля k. Пусть E — наименьшее расширение Галуа поля k, которое содержит K. Будем говорить, что расширение K над k *разрешимо*, если группа Галуа $G(E/k)$ разрешима.

Теорема 3.46. *Пусть E — разрешимое расширение поля k, F — любое расширение поля k. Причем E и F содержаться в некотором алгебраически замкнутом поле. Тогда EF — разрешимое расширение поля F.*

Доказательство. Пусть K — разрешимое расширение Галуа поля k и $E \subset K$. Тогда KF — разрешимое расширение Галуа поля F и группа $G(KF/F)$ — подгруппа группы $G(K/k)$ (см. 3.39). Поскольку $G(K/k)$ разрешима, то $G(KF/F)$ разрешима. Так как $EF \subset KF$, то EF — разрешимое расширение поля F. □

Теорема 3.47. *Пусть F — расширение поля k, E — расширение поля F. Тогда E — разрешимое расширение поля k тогда и только тогда, когда F — разрешимое расширение поля k и E — разрешимое расширение поля F.*

Доказательство. Пусть F — разрешимое расширение поля k и E — разрешимое расширение поля F. Пусть K — конечное разрешимое расширение Галуа поля k, содержащее F. Согласно теореме 3.46 EK — разрешимо над K. Пусть L — разрешимое расширение Галуа поля K, содержащее EK. Пусть σ — вложение L над k в алгебраически замкнутое поле. Заметим, что $\sigma K = K$. Пусть M — минимальное поле, содержащее все σL, т.е.

$$M = \sigma_1 L \sigma_2 L \cdots \sigma_n L.$$

Заметим, что M — расширение Галуа поля k (оно сепарабельно, поскольку L сепарабельно над k, и нормально, поскольку любое вложение M над k переставляет $\sigma_i L$). В силу теоремы 3.40 группа Галуа поля M над K является подгруппой произведения $\prod_{\sigma} G(\sigma L/K)$. Следовательно, она разрешима. Согласно теореме 3.10 имеет место сюръективный гомоморфизм $G(M/k) \to G(K/k)$. Отсюда, $G(M/k)$ содержит разрешимую нормальную подгруппу, факторгруппа по которой разрешима. Следовательно, $G(M/k)$ разрешима. Поскольку $E \subset M$, то E — разрешимое расширение поля k. □

Теорема 3.48. *Пусть E — сепарабельное расширение поля k. Тогда E — разрешимо в радикалах тогда и только тогда, когда E — разрешимое расширение поля k.*

Доказательство. Предположим, что E — разрешимо. Пусть K — разрешимое расширение Галуа поля k, содержащее E. Пусть m — произведение всех степеней простых чисел, не равных характеристике и делящих $[K:k]$. Положим $F = k(\zeta)$, где ζ — примитивный корень m-й степени из единицы. Заметим, что F — абелево расширение поля k. Поднимем K над F. Согласно 3.46 KF разрешимо над F. Тогда существует башня полей между k и KF такая, что каждый ее этаж — циклическое расширение. В силу теорем 3.18 и 3.37 KF разрешимо в радикалах над k. Следовательно, E — разрешимо в радикалах над k.

Обратно, предположим, что E — разрешимо в радикалах над k. Пусть $\sigma_1, \sigma_2, \ldots, \sigma_n$ — вложения E над k в алгебраическое замыкание $\bar{E}$. Пусть K — наименьшее поле, содержащее все $\sigma_i E$. Тогда K — расширение Галуа разрешимое в радикалах. Пусть m — произведение всех степеней простых чисел, не равных характеристике и делящих $[K:k]$. Положим $F = k(\zeta)$, где ζ — примитивный корень m-й степени из единицы. Заметим, что KF разрешимо над F. Отсюда, KF разрешимо над k. $\square$

6. Теория Куммера

Пусть K — расширение Галуа поля k и m — целое положительное число. Будем говорить, что это расширение *показателя* m, если $\sigma^m = 1$ для всех $\sigma \in G(K/k)$. Пусть m взаимно просто с характеристикой поля. Мы будем обозначать через $a^{\frac{1}{m}}$ любой элемент α, что $\alpha^m = a$. Пусть B — подгруппа k^*, содержащая $(k^*)^m$. Положим $K_B = k(B^{\frac{1}{m}})$ — расширение, порожденное всеми $a^{\frac{1}{m}}$, где $a \in B$. Заметим, что K_B — расширение Галуа. Действительно, любое вложение σ поля K_B в $\bar{k}$ переводит корни любого многочлена $x^m - a$ в себя. Поскольку K_B порождается $a^{\frac{1}{m}}$, то σ автоморфизм. Пусть G — группа Галуа расширения K_B над k. Пусть $\sigma \in G$, $\alpha = a^{\frac{1}{m}}$. Тогда $\sigma\alpha = \zeta\alpha$, где ζ — корень m-й степени из единицы. Отображение $\sigma \to \zeta$ является гомоморфизмом G в $\mathbb{Z}_m$. Заметим, что $\zeta = \frac{\sigma\alpha}{\alpha}$. Пусть $\alpha' = a^{\frac{1}{m}}$ — другой корень m-й степени из a. Тогда $\alpha' = \zeta'\alpha$. Отсюда,

$$\frac{\sigma\alpha'}{\alpha'} = \frac{\sigma(\zeta'\alpha')}{\zeta'\alpha} = \frac{\sigma\alpha}{\alpha} = \zeta.$$

Таким образом, $\frac{\sigma\alpha}{\alpha}$ не зависит от выбора α. Соответствие $(\sigma, a) = \frac{\sigma\alpha}{\alpha}$ задает отображение $G \times B \to \mathbb{Z}_m$. Очевидно, что $(\sigma, a) = 1$, если $a \in (k^*)^m$. Пусть $a, b \in B$ и $\alpha^m = a$, $\beta^m = b$. Тогда $(\alpha\beta)^m = ab$.

Следовательно,

$$(\sigma, ab) = \frac{\sigma(\alpha\beta)}{\alpha\beta} = \frac{\sigma(\alpha)\sigma(\beta)}{\alpha\beta} = \frac{\sigma(\alpha)}{\alpha}\frac{\sigma(\beta)}{\beta} = (\sigma, a)(\sigma, b).$$

Теорема 3.49. *Пусть k — поле, m — целое положительное число взаимно простое с характеристикой, причем примитивный корень m-й степени из единицы лежит в k. Пусть B — подгруппа в k^*, содержащая $(k^*)^m$, $K_B = k(B^{\frac{1}{m}})$. Тогда K_B — абелево расширение Галуа показателя m. Пусть G — его группа Галуа. Имеет место отображение $G \times B \to \mathbb{Z}_m$, задаваемое соответствием $(\sigma, a) = \frac{\sigma\alpha}{\alpha}$. Ядро слева равно 1, ядро справа есть $(k^*)^m$.*

Доказательство. Пусть $\sigma \in G$ и $(\sigma, a) = 1$ для любого $a \in B$. Тогда $\sigma\alpha = \alpha$ для любого α такого, что $\alpha^n = a$. Следовательно, σ действует тождественно на K_B. Таким образом, $\sigma = e$. Пусть $a \in B$ и $(\sigma, a) = 1$ для любого $\sigma \in G$. Рассмотрим подполе $k(a^{\frac{1}{m}})$. Если $a^{\frac{1}{m}}$ не лежит в k, то существует автоморфизм σ поля $k(a^{\frac{1}{m}})$ над k, который не является тождественным. Автоморфизм σ можно продолжить на K_B, т.е. до элемента группы Галуа. С другой стороны, $(\sigma, a) \neq 1$. Противоречие. □

Следствие 3.50. *Расширение K_B над k конечно тогда и только тогда, когда индекс $(B : (k^*)^m)$ конечен, и $[K_B : k] = (B : (k^*)^m)$.*

Теорема 3.51. *Отображение $B \to K_B$ задает биективное соответствие между множеством всех подгрупп B, содержащих $(k^*)^m$, и множеством абелевых расширений над k показателя m.*

Доказательство. Пусть B_1, B_2 — подгруппы в k^*, содержащие $(k^*)^m$. Если $B_1 \subset B_2$, то $k(B_1^{\frac{1}{m}}) \subset k(B_2^{\frac{1}{m}})$. Обратно, предположим, что $k(B_1^{\frac{1}{m}}) \subset k(B_2^{\frac{1}{m}})$. Нам нужно доказать, что $B_1 \subset B_2$. Пусть $b \in B_1$. Тогда $k(b^{\frac{1}{m}}) \subset k(B_2^{\frac{1}{m}})$, причем $k(b^{\frac{1}{m}})$ содержится в некотором конечном подрасширении $k(B_2^{\frac{1}{m}})$. Таким образом, мы можем считать, что B_2/k^* — конечно порожденная, а, следовательно, конечная, группа. Пусть B_3 — группа, порожденная B_2 и k. Тогда $k(B_3^{\frac{1}{m}}) = k(B_2^{\frac{1}{m}})$. С другой стороны, согласно 3.50,

$$(B_2 : (k^*)^m) = [K_{B_2} : k] = [K_{B_3} : k] = (B_3 : (k^*)^m).$$

Следовательно, $B_2 = B_3$. Отсюда, $b \in B_2$. Тогда $B_1 \subset B_2$. Отсюда следует инъективность отображения $B \to K_B$.

Пусть K — абелево расширение поля k показателя m. Предположим, что K конечно. Тогда группа Галуа $G(K/k)$ раскладывается в прямое произведение циклических групп, порядка не выше m. Мы можем применить 3.44. Таким образом, $K = K_1 K_2 \cdots K_n$, где K_i — циклические расширения. Согласно теореме 3.26, K_i может быть получено присоединением корня m-й степени из элемента b_i. Следовательно, K может быть получено присоединением корней m-й степени из элементов $\{b_i\}$. Здесь мы уже можем не предполагать конечность расширения K и числа элементов $\{b_i\}$. Пусть B — подгруппа в k^*, порожденная всеми b и $(k^*)^m$. Тогда $k(B^{\frac{1}{m}}) = K$. $\square$

7. Целые расширения Галуа

В этом параграфе слово "кольцо"будет обозначать коммутативное кольцо с единицей.

Определение 3.52. Пусть A — кольцо и M — A-модуль. Будем говорить, что M *точный*, если из равентсва $aM = 0$ следует, что $a = 0$.

Теорема 3.53. *Пусть A — подкольцо кольца B и $\alpha \in B$. Следующие условия эквивалентны:*

(1) *α есть корень многочлена $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.*
(2) *Подкольцо $A[\alpha]$ — конечно порожденный A-модуль.*
(3) *Существует точный модуль над $A[\alpha]$, являющийся конечно порожденным A-модулем.*

Доказательство. Предположим, что выполнено первое условие. Пусть $f(x) \in A[x]$ — многочлен со старшим коэффициентом единица, для которого $f(\alpha) = 0$. Если $g(x) \in A[x]$, то $g(x) = f(x)q(x) + r(x)$, где $\deg r < \deg f = n$. Тогда $f(\alpha) = r(\alpha)$. Следовательно, $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ являются образующими $A[\alpha]$. Уравнение $f(x) = 0$ называется *целым уравнением* для α над A.

Предположим, что выполнено второе условие. Тогда в качестве точного модуля можно взять само $A[\alpha]$.

Предположим, что выполнено третье условие. Пусть M — точный модуль над $A[\alpha]$, конечнопорожденный над A. Пусть $w_1, w_2, \ldots, w_n$ — его пораждающие. Тогда существуют элементы $a_{ij} \in A$ такие, что

$$\begin{cases} \alpha w_1 = a_{11}w_1 + a_{12}w_2 + \cdots + a_{1n}w_n \\ \alpha w_2 = a_{21}w_1 + a_{22}w_2 + \cdots + a_{2n}w_n \\ \cdots \quad \cdots \quad \cdots \\ \alpha w_n = a_{n1}w_1 + a_{n2}w_2 + \cdots + a_{nn}w_n. \end{cases}$$

Перенесем $\alpha w_1, \alpha w_2, \ldots, \alpha w_n$ вправо. Получаем систему, которая должна иметь ненулевое решение. Тогда

$$d = \begin{vmatrix} a_{11}-\alpha & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-\alpha & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-\alpha \end{vmatrix}$$

аннулирует M, т.е. $dM = 0$. Поскольку M — точный мотуль, то $d = 0$. Тогда

$$f(x) = \begin{vmatrix} a_{11}-x & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-x & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-x \end{vmatrix}$$

задает (с точностью до знака) целое уравнение для α. □

Элемент α, удовлетворяющий этим условиям называется *целым* над A.

Утверждение 3.54. *Пусть A — целостное кольцо, K — его поле частных, и α — алгебраический элемент над K. Тогда существует $d \in A$ такой, что $d\alpha$ — целый элемент над A.*

Доказательство. Пусть $f(x)$ — минимальный многочлен элемента α. Умножая $f(x)$ на наименьшее общее кратное знаменателей его коэффициентов, получаем

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

где $a_i \in A$, $a_n \neq 0$. Умножим это уравнение на a_n^{n-1}, получим

$$(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + \cdots + a_n^{n-2}a_1(a_n\alpha) + a_n^{n-1}a_0 = 0.$$

Таким образом, $a_n\alpha$ — целый элемент над A. □

Пусть кольцо A содержится в кольце B. Мы говорим, что B — *целое кольцо* над A (*целое расширение* кольца A), если любой элемент из B является целым над A.

Утверждение 3.55. *Пусть B — целое расширение кольца A, конечнопорожденное, как A-алгебра. Тогда B — конечнопорожденный A-модуль.*

Доказательство. Докажем по индукции. Пусть

$$A \subset A[\alpha_1] \subset A[\alpha_1, \alpha_2] \subset \cdots \subset A[\alpha_1, \alpha_2, \ldots, \alpha_n] = B,$$

где каждый α_i — целый элемент над A, а следовательно и над $A[\alpha_1, \alpha_2, \ldots, \alpha_{i-1}]$. Исходя из определения, $A[\alpha_1, \alpha_2, \ldots, \alpha_{i-1}][\alpha_i]$ —

конечно порожденный $A[\alpha_1, \alpha_2, \ldots, \alpha_{i-1}]$-модуль. Отсюда, B — конечнопорожденный A-модуль. $\square$

Теорема 3.56. *Пусть B — целое расширение кольца A, C — целое расширение кольца B. Тогда C — целое расширение кольца A. Обратно, если C — целое расширение кольца A, то B — целое расширение кольца A, и C — целое расширение кольца B.*

Доказательство. Если C — целое кольцо над A, то ясно, что B — целое кольцо над A, и C — целое кольцо над B. Предположим, что B — целое расширение кольца A, C — целое расширение кольца B. Пусть $\alpha \in C$. Тогда

$$\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0,$$

где $b_i \in B$. Положим $B_1 = A[b_0, b_1, \cdots, b_{n-1}]$. Тогда, согласно утверждению 3.55, B_1 — конечнопорожденный A-модуль. Следовательно, $B_1[\alpha]$ — конечнопорожденный A-модуль. С другой стороны, поскольку $A[\alpha] \subset B_1[\alpha]$, то $B_1[\alpha]$ — точный $A[\alpha]$-модуль. Отсюда, C — целое расширение кольца A. $\square$

Теорема 3.57. *Пусть A — подкольцо кольца B. Тогда элементы B, целые над A, образуют подкольцо в B.*

Доказательство. Если $\alpha \in B$ — целый над A, то $A[\alpha]$ — целое расширение кольца A. Действительно, для любого $\alpha' \in A[\alpha]$, $A[\alpha]$ является точным $A[\alpha']$-модулем. С другой стороны, $A[\alpha]$ — конечно порожденный A-модуль. Пусть $\alpha, \beta \in B$ — целые элементы над A. Рассмотрим башню $A \subset A[\alpha] \subset A[\alpha, \beta]$. Каждый этаж этой башни является целым расширением. Тогда, по теореме 3.56, $A[\alpha, \beta]$ — целое расширение A. Таким образом, $\alpha \pm \beta$, $\alpha\beta$ — целые элементы над A. $\square$

Теорема 3.58. *Пусть A — целостное кольцо, k — его поле частных, E — конечное расширение над k и $\alpha \in E$ — целый элемент над A. Тогда коэффициенты минимального многочлена α являются целыми над A. В частности целыми будут норма и след.*

Доказательство. Для всякого вложения σ поля E над k. $\square$

Пусть $A \subset B$. Множество элементов из B, целых над A, называется *целым замыканием* кольца A в B. Будем говорить, что целостное кольцо A *целозамкнуто*, если целое замыкание A в своем поле частных совпадает с A.

Литература

[1] Ван-дер-Варден Б.Л. *Современная алгебра.*

[2] Зарисский О., Самюэль П. *Комутативная алгебра.*

[3] Каргополов М.И., Мерзляков Ю.И. *Основы теории групп.*

[4] Кострикин А.И. *Основы алгебры.*

[5] Курош А.Г., *Курс высшей алгебры.*

[6] Ленг С. *Алгебра.*

[7] Постников М. М. *Теория Галуа.*