Глава VIII. Поля.

§ 1. Общие сведения о расширениях полей

При рассмотрении очередной алгебраической структуры, как обычно, начнем с уточнения определения изоморфизма: изоморфизм колец $\varphi : K_1 \to K_2$ называется *изоморфизмом полей,* если K_1 и K_2 — поля. Легко понять (убедитесь в этом!), что если φ — изоморфизм полей, то $\varphi(1) = 1$ и $\varphi(\alpha^{-1}) = \varphi(\alpha)^{-1}$ при любом ненулевом $\alpha \in K_1$. Если для двух полей K_1 и K_2 какой-нибудь изоморфизм $\varphi : K_1 \to K_2$ существует, то эти два поля мы, разумеется, будем называть изоморфными. Отметим попутно,что если K_1 — поле, а K_2 — кольцо и $\varphi : K_1 \to K_2$ — кольцевой изоморфизм, то K_2 — тоже поле, а φ изоморфизм полей (объясните, почему).

Основным объектом изучения в этом параграфе будет пара, состоящая из некоторого поля K и его подполя k; часто в такой ситуации мы будем говорить также, что K является *расширением* поля k. Расширением мы будем также называть саму пару, состоящую из поля и его подполя, записывая ее в виде K/k. Поле L назовем *промежуточным полем расширения* K/k, если L одновременно является расширением k и подполем K.

Если у данного поля K нет подполей, отличных от него самого, то такое поле K называется *простым.* Опишем все простые поля с точностью до изоморфности:

Предложение. *Пусть K — простое поле.*

1) Если характеристика K равна нулю, то K изоморфно полю рациональных чисел $\mathbb{Q}$.

2) Если $\mathrm{char}(K) = p \neq 0$ *(p — простое число), то K изоморфно полю $\mathbb{Z}/\langle p\rangle$ вычетов по модулю p.*

Proof. 1) При $\mathrm{char}(K) = 0$ рассмотрим отображение $\varphi : \mathbb{Q} \to K$, положив $\varphi(\frac{m}{n}) = (m1_K)(n1_K)^{-1}$ при любых $n \in \mathbb{N}$ и $m \in \mathbb{Z}$ (отметим, что элемент $n1_K$ отличен от нулевого из-за условия на характеристику). Легко понять, что наше отображение φ определено корректно: если $\frac{m}{n} = \frac{m_1}{n_1}$ в $\mathbb{Q}$, то $mn_1 = nm_1$ в $\mathbb{Z}$ и потому $(mn_1)1_K = (nm_1)1_K$. Нетрудно проверить (проверьте!), что φ является мономорфизмом аддитивных групп и $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ при любых $\alpha, \beta \in \mathbb{Q}$. Обозначим через K_1 образ $\mathbb{Q}$ при отображении φ. Тогда, как показывает несложная выкладка (проведите ее!), K_1 является подполем поля K, изоморфным $\mathbb{Q}$. Остается заметить, что из-за простоты K имеем $K = K_1$.

2) При $\mathrm{char}(K) = p \neq 0$ рассмотрим отображение $\varphi : \mathbb{Z}/\langle p\rangle \to K$, положив $\varphi(\bar{m}) = m1_K$ для произвольного целого m. Убедимся в корректности определения такого отображения: если целые числа m и n принадлежат одному классу вычетов ($\bar{m} = \bar{n}$ в поле $\mathbb{Z}/\langle p\rangle$), то $m = n + pq$ при некотором целом q и потому справедливо равенство $m1_K = n1_K + q(p1_K) = n1_K$. Далее, как и в предыдущем пункте доказательства, легко проверяется, что отображение φ — изоморфизм поля вычетов на подполе поля K, из-за простоты совпадающее с K.

□

Различных подполей у данного поля K может быть много. Легко понять, что пересечение любого непустого множества подполей само является подполем данного поля. Нетрудно заметить также, что пересечение всех подполей K является простым полем (его называют *простым подполем* данного поля). Только что доказанное предложение позволяет считать, что простое подполе произвольного поля — это либо поле рациональных чисел, либо поле вычетов по простому модулю.

Пусть K/k — расширение и M — непустое подмножество поля K. Пересечение всех промежуточных полей рассматриваемого расширения, содержащих подмножество M, принято обозначать $k(M)$ и называть *расширением поля k, получающимся присоединением к k элементов множества M* (для конечного $M = \{\theta_1, \ldots, \theta_n\}$ мы будем обозначать такое поле $k(\theta_1, \ldots, \theta_n)$). Если множество M состоит всего из одного элемента θ, то поле $k(M) = k(\theta)$ называют *простым расширением* k, а элемент θ называют *порождающим элементом* такого расширения.

Примеры. *1) Поле комплексных чисел является простым расширением поля вещественных чисел:*

$$\mathbb{C} = \mathbb{R}(i).$$

2) Любое поле k является простым расширением себя самого: $k(\theta) = k$ при произвольном $\theta \in k$.

Вновь фиксируем расширение K/k. Элемент $\theta \in K$ называют *алгебраическим над* k, если $f(\theta) = 0$ для некоторого ненулевого многочлена f из $k[x]$; в противном случае (если такого ненулевого многочлена нет) элемент θ называют *трансцендентным* над k. Если каждый элемент K алгебраичен над k, то K называют *алгебраическим расширением* k.

Пример. *Поле комплексных чисел является алгебраическим расширением поля вещественных чисел:* $f = x - \theta$ *при* $\theta \in \mathbb{R}$ *и* $f = (x - \theta)(x - \overline{\theta})$ *при* $\theta \notin \mathbb{R}$. *Однако поле* $\mathbb{C}$ *как расширение* $\mathbb{Q}$ *неалгебраично: число* π *не является корнем никакого ненулевого многочлена с рациональными коэффициентами.*

Для расширения K/k каждому $\theta \in K$ сопоставим множество $\mathfrak{A}_\theta$ всех многочленов из $k[x]$, имеющих данный элемент θ корнем (произвольный многочлен f из $\mathfrak{A}_\theta$ принято называть *аннулятором* элемента θ над полем k). Непосредственная проверка показывает, что для каждого $\theta \in K$ множество $\mathfrak{A}_\theta$ — идеал кольца $k[x]$ (убедитесь в этом!). Трансцендентность θ эквивалентна, очевидно, равенству $\mathfrak{A}_\theta = \{0\}$. Если же θ алгебраичен над k, то $\mathfrak{A}_\theta \neq 0$ и из-за евклидовости кольца $k[x]$ однозначно определен унитальный многочлен $g \in k[x]$, порождающий указанный идеал: $\mathfrak{A}_\theta = \langle g \rangle$; этот многочлен g далее мы будем называть *минимальным аннулятором* элемента θ. Из определения понятно, что минимальный аннулятор θ — это его ненулевой аннулятор наименьшей степени, а произвольный многочлен из $k[x]$ является аннулятором θ тогда и только тогда, когда он делится на минимальный аннулятор θ. Еще одно свойство минимального аннулятора сформулируем в виде отдельного утверждения.

Предложение. *Если* K/k *— расширение и* $\theta \in K$ *алгебраичен над* k, *то минимальный аннулятор* θ *неприводим в* $k[x]$.

Proof. Предположим, что минимальный аннулятор g нашего θ представим в виде произведения двух многочленов из $k[x]$: $g = g_1 g_2$. Из равенства $0 = g(\theta) = g_1(\theta) g_2(\theta)$ следует, что хотя бы один из двух сомножителей $g_1(\theta)$ или $g_2(\theta)$ равен 0, а это означает, что хотя бы один из многочленов g_1 или g_2 — также аннулятор θ. Осталось сравнить степени рассматриваемых многочленов. □

Если K — расширение поля k, то, как уже говорилось в главе IV, на K естественным образом определена структура линейного пространства над k; если это пространство конечномерно, то поле K называется *конечным расширением* k, а размерность K как пространства над k называется *степенью рассматриваемого расширения* и обозначается $(K : k)$. Для полей свойство "быть конечным расширением"транзитивно, точнее:

Теорема (о последовательных конечных расширениях). *Если* K/k *и* F/K *— конечные расширения, то* F/k *– конечное расширение, причем* $(F : k) = (F : K) \cdot (K : k)$.

Proof. Пусть $(\alpha_1, \ldots, \alpha_n)$ — базис поля K как пространства над k и $(\beta_1, \ldots, \beta_m)$ — базис поля F как пространства над K. Достаточно показать, что семейство произведений

$$(\alpha_i \beta_j)_{1 \leq i \leq n, 1 \leq j \leq m}$$

служит базисом F как пространства над k.

Любой элемент $\eta \in F$ представим в виде $\eta = \sum\limits_{j=1}^{m} \gamma_j \beta_j$ при некоторых $\gamma_j \in K$. Далее заметим, что каждый γ_j можно записать в виде $\gamma_j = \sum\limits_{i=1}^{n} \delta_{ij} \alpha_i$ при каких-то $\delta_{ij} \in k$. Поэтому мы имеем равенство $\eta = \sum \delta_{ij} \alpha_i \beta_j$, а это значит, что наше семейство произведений служит системой образующих поля F как прострнаства над полем k. В том же духе проверяется (проверьте!) линейная независимость над k рассматриваемого семейства произведений. □

Замечание. *Если* K *— промежуточное поле конечного расширения* F/k, *то расширения* K/k *и* F/K *— также конечные (объясните, почему).*

Следующее утверждение мы будем в дальнейшем часто использовать при рассмотрении конечных расширений:

Теорема (об алгебраичности конечного расширения). *Если* K/k *— конечное расширение, то* K/k *– алгебраическое расширение. При этом степень минимального аннулятора каждого элемента* $\theta \in K$ *не превосходит степени рассматриваемого роасширения.*

Proof. Если $(K : k) = n$, то для каждого $\theta \in K$ семейство его степеней $(1, \theta, \theta^2, \ldots, \theta^n)$ линейно зависимо в пространстве K. Это означает, что для некоторого нетривиального семейства $(\alpha_0, \ldots, \alpha_n)$ в k имеем равенство $\alpha_0 + \alpha_1\theta + \cdots + \alpha_n\theta^n = 0$. Поэтому принадлежащий кольцу $k[x]$ многочлен $f = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$ является ненулевым аннулятором θ, откуда следует алгебраичность θ. Для доказательства второй части утверждения достаточно вспомнить, что каждый аннулятор делится на минимальный. □

Следующая теорема посвящена простым расширениям поля, получающимся присоединением алгебраического элемента.

Теорема (о строении простого алгебраического расширения). *Пусть K — какое-нибудь расширение поля k, $\theta \in K$ — алгебраический над k элемент, g — минимальный аннулятор θ и $\deg g = n$. Тогда*

1) *поле $k(\theta)$ изоморфно полю $k[x]/\langle g\rangle$;*

2) *поле $k(\theta)$ — конечное расширение поля k, причем $(k(\theta) : k) = n$, а $(1, \theta, \theta^2, \ldots, \theta^{n-1})$ — базис $k(\theta)$ над k;*

3) *для каждого $\alpha \in k(\theta)$ поле $k(\alpha)$ является конечным расширением поля k, а число $(k(\alpha) : k)$ является делителем числа n.*

Proof. 1) Рассмотрим отображение

$$\varphi : k[x] \to K,$$

положив $\varphi(f) = f(\theta)$ при $f \in k[x]$. Легко проверить(проверьте!), что φ — гомоморфизм аддитивных групп колец, причем $\operatorname{Ker}\varphi = \mathfrak{A}_\theta$. Положим $L = \operatorname{Im}\varphi$. Как установлено в процессе доказательства первой теоремы о гомоморфизме, отображение $\bar\varphi : k[x]/\operatorname{Ker}\varphi \to L$, определяемое равенством $\bar\varphi(f + \operatorname{Ker}\varphi) = \varphi(f)$, является изоморфизмом аддитивных групп. Из определения умножения в факторкольце $k[x]/\operatorname{Ker}\varphi$ следует, что

$$\bar\varphi((f + \operatorname{Ker}\varphi)\cdot(h + \operatorname{Ker}\varphi)) = \bar\varphi(fh + \operatorname{Ker}\varphi) = (fh)(\theta) = f(\theta)h(\theta) = \bar\varphi(\bar f)\bar\varphi(\bar h),$$

поэтому L — подкольцо K, изоморфное $k[x]/\operatorname{Ker}\varphi$. Вспомним теперь, что идеал $\operatorname{Ker}\varphi$ порожден неприводимым многочленом g, а это, как показано в § 1 главы II, означает, что факторкольцо $k[x]/\operatorname{Ker}\varphi$ является полем; значит L — тоже поле, и оно изоморфно $k[x]/\operatorname{Ker}\varphi$. Далее, легко понять, что k — подполе L, причем наш элемент θ принадлежит L (объясните, почему). Следовательно, $k(\theta) \subseteq L$. Пусть теперь F — промежуточное поле расширения K/k и $\theta \in F$. Для любого $\beta \in L$ имеем $\beta = f(\theta)$ при некотором $f = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m \in k[x]$, а потому в представлении $\beta = \alpha_0 + \alpha_1\theta + \cdots + \alpha_m\theta^m$ все слагаемые правой части принадлежат полю F; таким образом, β содержится полю F, что доказывает включение $L \subseteq k(\theta)$. Тем самым мы установили равенство $L = k(\theta)$, завершив доказательство первой части нашей теоремы.

2) Если мы имеем $\beta_0 + \beta_1\theta + \ldots + \beta_{n-1}\theta^{n-1} = 0$ для некоторых $\beta_i \in k$, то многочлен $f = \beta_0 + \beta_1 x + \ldots + \beta_{n-1}x^{n-1}$ — аннулятор элемента θ. Поскольку $\deg f < n$ и f делится на минимальный аннулятор g, имеющий степень n, то f — нулевой многочлен, а семейство $(1, \theta, \theta^2, \ldots, \theta^{n-1})$ линейно независимо. С другой стороны, в предыдущем пункте мы доказали, что произвольный $\alpha \in k(\theta)$ представим в виде $\alpha = f(\theta)$ для некоторого многочлена f из $k[x]$. Применяя деление с остатком, найдем в $k[x]$ такие многочлены q и r, что $f = gq + r$ и $r = \beta_0 + \beta_1 x + \ldots + \beta_{n-1}x^{n-1}$ при некоторых $\beta_i \in k$. Ясно, что тогда мы имеем равенство $\alpha = r(\theta) = \beta_0 + \beta_1\theta + \ldots + \beta_{n-1}\theta^{n-1}$. Следовательно, наше семейство — базис $k(\theta)$ над k и $(k(\theta) : k) = n$.

3) Если $\alpha \in k(\theta)$, то $k(\alpha)$ — промежуточное поле расширения $k(\theta)/k$, откуда следует, что расширение $k(\alpha)/k$ конечно и $(k(\theta) : k) = (k(\theta) : k(\alpha))\cdot(k(\alpha) : k)$.

□

До сих пор, говоря о присоединении элемента к полю k, мы предполагали, что этот элемент и k содержатся в некотором "большом"поле K. Используя идею из первой части только что доказанной теоремы, можно строить простые алгебраические расширения поля k, не имея такого "объемлющего"поля.

Теорема (Кронекер). *Для произвольного поля k и любого неприводимого многочлена f из $k[x]$ существует простое алгебраическое расширение поля k, образующим элементом которого является некоторый корень многочлена f.*

Proof. Наше рассуждение почти дословно повторяет аргументы, использованные в главе III для определения поля комплексных чисел, поэтому мы не будем вдаваться в подробные пояснения (разберитесь в деталях самостоятельно!).

Из неприводимости f следует, что факторкольцо $k[x]/\langle f\rangle$ является полем; обозначим это поле через L. Рассмотрим отображение $j : k[x] \to L$, при котором произвольному многочлену h в факторкольце сопоставляется класс $j(h) = h + \langle f\rangle$. Поскольку j согласовано с алгебраическими операциями в обоих кольцах, а разные элементы исходного поля имеют разные образы, можно отождествить каждый элемент α поля k с его образом $j(\alpha)$ в L и считать k подполем поля L. Дальше остается заметить, что если θ определить как $\theta = j(x)$ (образ многочлена первой степени), то окажется, что $f(\theta) = 0$ и $L = k(\theta)$. □

Пример. *Пусть $k = \mathbb{Z}/\langle 2\rangle$ — поле вычетов по модулю 2. Многочлен $f = x^2 + x + 1$, очевидно, неприводим в кольце $k[x]$. В этой ситуации поле $L = k[x]/\langle f\rangle$ — простое алгебраическое расширение степени 2 поля k и $\theta = x + \langle f\rangle$ — порождающий элемент этого расширения. Пара $(1, \theta)$ является базисом L над k, а само поле L состоит из 4 элементов: $L = \{0, 1, \theta, \theta + 1\}$. Выпишем таблицы алгебраических операций в поле L :*

$+$	0	1	θ	$\theta+1$
0	0	1	θ	$\theta+1$
1	1	0	$\theta+1$	θ
θ	θ	$\theta+1$	0	1
$\theta+1$	$\theta+1$	θ	1	0

$\times$	0	1	θ	$\theta+1$
0	0	0	0	0
1	0	1	θ	$\theta+1$
θ	0	θ	$\theta+1$	1
$\theta+1$	0	$\theta+1$	1	θ

В различных расширениях K_1 и K_2 поля k один и тот же неприводимый многочлен $f \in k[x]$ может иметь разные корни, однако простые расширения, получающиеся присоединением к полю k различных корней многочлена f, оказываются с алгебраической точки зрения одинаковыми:

Предложение. *Пусть k — поле, f — неприводимый многочлен из $k[x]$. Если $k(\theta_1)$ и $k(\theta_2)$ — два простых расширения k, порождающие элементы θ_1 и θ_2 которых являются корнями многочлена f, то существует изоморфизм полей $\varphi : k(\theta_1) \to k(\theta_2)$, для которого $\varphi(\theta_1) = \theta_2$ и $\varphi(\alpha) = \alpha$ при всех α из поля k.*

Proof. Если f — многочлен степени n, то по теореме о строении простого алгебраического расширения $(1, \theta_1, \theta_1^2, \ldots, \theta_1^{n-1})$ — базис $k(\theta_1)$, а $(1, \theta_2, \theta_2^2, \ldots, \theta_2^{n-1})$ — базис $k(\theta_2)$. Положив $\varphi(\alpha_0 + \alpha_1\theta_1 + \cdots + \alpha_{n-1}\theta_1^{n-1}) = \alpha_0 + \alpha_1\theta_2 + \cdots + \alpha_{n-1}\theta_2^{n-1}$ при любых $\alpha_i \in k$, получаем отображение $\varphi : k(\theta_1) \to k(\theta_2)$, которое является изоморфизмом полей и удовлетворяет условиям нашего предложения (объясните, почему). □

Мы показали выше, что любой неприводимый над данным полем многочлен становится приводимым в некотором "достаточно малом"расширении этого поля, то есть в расширении, которое порождается одним из корней взятого многочлена. Наша следующая цель — обобщить этот результат.

Пусть k — поле и f — многочлен положительной степени над этим полем. Расширение K поля k назовем *полем разложения* многочлена f, если этот многочлен раскладывается на линейные множители в кольце $K[x]$ и поле K получается присоединением к k всех корней многочлена f.

Примеры. *1) Произвольное поле k является полем разложения любого линейного многочлена из $k[x]$.*

2) Для $k = \mathbb{R}$ поле $\mathbb{C}$ является полем разложения и многочлена $x^2 + 1$, и любого вещественного многочлена, имеющего хотя бы один мнимый корень (объясните, почему).

3) Над полем $\mathbb{Q}$ многочлен $x^4 - 2$ неприводим в силу критерия Эйзенштейна. Вещественное поле $\mathbb{Q}(\sqrt[4]{2})$ не является для этого многочлена полем разложения: в таком поле каноническое разложение нашего многочлена — это $(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x^2+\sqrt{2})$. В качестве поля разложения x^4-2 можно взять комплексное поле $\mathbb{Q}(\sqrt[4]{2}, i)$ (попробуйте это объяснить).

Предложение. *Для любого поля k и любого многочлена положительной степени из $k[x]$ поле разложения существует.*

Proof. Проведем индукцию по степени многочлена f. При $\deg f = 1$ наше утверждение тривиально. Предположим далее, что $\deg f = n > 1$ и поле разложения существует для любого многочлена, степень которого меньше n.

Возьмем какой-нибудь неприводимый делитель g многочлена f в $k[x]$ и, воспользовавшись теоремой Кронекера, построим простое расширение $K_1 = k(\alpha)$ поля k, в котором $g(\alpha) = 0 = f(\alpha)$. В кольце $K_1[x]$ многочлен f можно представить в виде $f = (x - \alpha)f_1$. Ясно, что $\deg f_1 < n$, поэтому в силу индукционного предположения для f_1 существует поле разложения K_2 — это некоторое конечное расширение K_1. Понятно, что в кольце $K_2[x]$ многочлен f раскладывается на линейные множители. Если $\alpha_1, \ldots, \alpha_m$ — все (различные) корни f в K_2, то порожденное ими промежуточное поле $k(\alpha_1, \ldots, \alpha_m)$ расширения K_2/k является полем разложения f. □

Замечания. *1) Разные расширения K_1 и K_2 поля k могут оказаться полями разложения одного и того же многочлена из $k[x]$. С алгебраической точки зрения, однако, эти поля можно не различать: существует такой изоморфизм полей $\varphi : K_1 \to K_2$, что $\varphi(\alpha) = \alpha$ для всех α из поля k. Доказывать существование изоморфизма с указанным свойством мы не будем.*

2) Можно определить понятие поля разложения для нескольких многочленов положительных степеней из $k[x]$ — в этом поле все такие многочлены должны раскладываться на линейные множители, а само поле должно порождаться всеми их корнями; легко понять, что такое поле совпадает с полем разложения произведения всех рассматриваемых многочленов и потому оно существует в силу только что доказанной теоремы. Аналогичным образом можно определять и поле разложения для бесконечного множества многочленов из $k[x]$ (доказывать существование такого поля мы не будем). В частности, можно говорить о поле разложения всех многочленов положительных степеней кольца $k[x]$ — это поле принято называть алгебраическим замыканием поля k *и обозначать $\bar{k}$. Замечательное свойство алгебраического замыкания состоит в том, что в кольце $\bar{k}[x]$ на линейные множители разложимы не только все многочлены положительных степеней из $k[x]$, но и все многочлены из $\bar{k}[x]$; говоря другими словами, алгебраическое замыкание произвольного поля — всегда алгебраически замкнутое поле. Для поля $\mathbb{R}$ алгебраическим замыканием служит поле $\mathbb{C}$, которое является конечным расширением $\mathbb{R}$. В большинстве других случаев алгебраическое замыкание не является конечным расширением основного поля — таковы, например, алгебраические замыкания поля рациональных чисел и поля вычетов по простому модулю.*

§ 2. Основные свойства конечных полей

Первый вопрос, который мы рассмотрим в этом параграфе — это вопрос о том, каким может быть число элементов конечного поля.

С примерами конечных полей мы впервые встретились в § 2 главы II, когда рассматривали поля вычетов по простому модулю. По понятным причинам (уточните!) характеристика произвольного конечного поля не может быть нулевой, а это в силу замечания к предложению из первого параграфа этой (восьмой) главы значит, что простое подполе конечного поля можно считать совпадающим с полем вычетов по некоторому простому модулю. Довольно понятно, что число элементов большего поля как-то связано с таким простым модулем. Эту связь мы уточним, доказав первое утверждение этого параграфа.

Предложение. *Если K — конечное поле и k — некоторое его подполе, состоящее из q элементов, то K/k — конечное расширение и $|K| = q^m$, где $m = (K : k)$.*

Proof. Конечность расширения K/k совершенно очевидна. Если $(\theta_1, \ldots, \theta_m)$ — базис K как пространства над k, то каждый элемент β из поля K однозначно представим в виде $\beta = \sum_{i=1}^{m} \alpha_i \theta_i$ при некоторых $\alpha_i \in k$. Для доказательства нашего утверждения достаточно заметить, что каждая координата α_i может принимать любое из q значений. □

Следствие. *Если K — конечное поле и $\operatorname{char} K = p$, то $|K| = p^n$, где n — степень K как расширения над его простым подполем (таким образом, число элементов любого конечного поля всегда является степенью некоторого простого числа).*

Доказанное утверждение оставляет открытыми два вопроса: существуют ли конечные поля, отличные от полей вычетов, и сколько таких полей? Конечно, используя теорему Кронекера из предыдущего параграфа, мы можем для полей вычетов строить их простые расширения, присоединяя корни неприводимых многочленов

степени > 1, но и на этом пути возникают некоторые проблемы — например, о существовании неприводимых многочленов с коэффициентами из поля вычетов и разнообразии их степеней. Ответы на эти и другие вопросы мы постараемся дать в этом параграфе.

Используя теоретико-групповые соображения, мы сейчас покажем, что каждое конечное поле тесно связано с введенным в предыдущем параграфе понятием поля разложения многочлена. Для этого мы установим следующий простой факт, являющийся обобщением малой теоремы Ферма.

Предложение. *Если K — поле из q элементов, то $\alpha^q = \alpha$ для каждого α из этого поля.*

Proof. При $\alpha = 0$ указанное равенство очевидно. Ненулевой α можно рассматривать как элемент мультипликативной группы K^* нашего поля, а она имеет порядок $q - 1$. В силу следствия из теоремы Лагранжа о группах мы имеем равенство $\alpha^{q-1} = 1$, из которого, очевидно, следует $\alpha^q = \alpha$. □

Доказанное утверждение позволит нам теперь охарактеризовать конечное поле как поле разложения некоторого многочлена.

Следствие. *Если K — конечное поле из q элементов, то в кольце $K[x]$ справедливо равенство*

$$x^q - x = \prod_{\alpha \in K} (x - \alpha)$$

(таким образом, K является полем разложения многочлена $x^q - x$ над любым своим подполем).

Proof. По доказанному предложению все элементы поля K являются корнями многочлена $x^q - x$, к тому же многочлены в левой и правой частях приведенного равенства имеют одинаковые степени и одинаковые старшие коэффициенты. □

Далее в этой главе нам потребуется один замечательный факт, касающийся арифметики полей ненулевой характеристики.

Лемма. *Если K — поле характеристики $p > 0$, то $(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$ для любого натурального числа m и произвольных элементов α и β из поля K.*

Proof. Из-за биномиального разложения

$$(\alpha + \beta)^{p^m} = \alpha^{p^m} + \sum_{i=1}^{p^m - 1} C^i_{p^m} \alpha^i \beta^{p^m - 1} + \beta^{p^m}$$

нам достаточно показать, что при всех индексах i, удовлетворяющих условию $1 \leq i \leq p^m - 1$, биномиальные коэффициенты $C^i_{p^m}$ делятся на число p. Для этого подсчитаем, с какими показателями наше p входит в канонические разложения числителя и знаменателя дроби $\frac{(p^m)!}{i!(p^m - i)!}$.

Как обычно, через $[y]$ будем обозначать *целую часть* рационального числа y, то есть наибольшее из целых чисел N, для которых $N \leq y$. Несложно подсчитать, что для всякого натурального n в каноническое разложение числа $n!$ простое число p входит с показателем

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$$

— понятно, что в этой сумме только конечное число слагаемых может быть отличным от нуля. В частности, для $n \leq p^m$ можно считать, что число слагаемых в этой сумме равно m. Далее, легко показать (покажите!), что при $1 \leq i < p^m$ имеют место неравенства

$$\left[\frac{i}{p^j}\right] + \left[\frac{p^m - i}{p^j}\right] \leq \left[\frac{p^m}{p^j}\right] \quad \text{для} \quad 1 \leq j < m \qquad \text{и} \qquad \left[\frac{i}{p^m}\right] + \left[\frac{p^m - i}{p^m}\right] < \left[\frac{p^m}{p^m}\right].$$

Поэтому при любом натуральном m показатель, с которым p входит в каноническое разложение числителя $C^i_{p^m}$, больше показателя p в каноническом разложении знаменателя $C^i_{p^m}$, а это значит, что наш биномиальный коэффициент делится на p. □

Теперь у нас все готово для доказательства одной из центральных теорем этого параграфа.

Теорема (о существовании конечного поля). *Для любого простого числа p и произвольного натурального n существует поле, содержащее ровно p^n элементов.*

Proof. Положим $q = p^n$ и для многочлена $f = x^q - x$ обозначим через K его поле разложения над полем вычетов по модулю p. Из определения поля разложения следует, что K — конечное поле (оно является расширением конечного поля и порождается над ним конечным множеством алгебраических элементов), а в кольце $K[x]$ многочлен f раскладывается на линейные множители: $f = \prod_{i=1}^{q}(x - \alpha_i)$. Заметим, что в семействе $(\alpha_1, \dots, \alpha_q)$ все члены принадлежат полю K и попарно различны: наш многочлен не имеет кратных корней, поскольку его производная f' равна -1. Следовательно, построенное нами поле K содержит не менее q элементов.

Рассмотрим теперь q-элементное подмножество

$$L = \{\alpha_1, \dots, \alpha_q\}.$$

Совершенно очевидно, что L содержит 0, а все его ненулевые элементы образуют группу относительно умножения. По лемме мы имеем

$$(\alpha_i + \alpha_j)^q = \alpha_i^q + \alpha_j^q = \alpha_i + \alpha_j,$$

откуда следует замкнутость множества L относительно сложения. Добавим, что вместе с каждым своим элементом L содержит и противоположный ему элемент: при нечетном p это является следствием равенства $(-\alpha_i)^q = (-1)^q \alpha_i^q$, а при $p = 2$ имеем $\alpha_i = -\alpha_i$. Все сказанное вместе означает, что L — поле (отметим, что оно, разумеется, совпадает с полем K, так как является полем разложения f). □

Чуть позже мы докажем, что любое поле из p^n элементов изоморфно только что построенному, но сначала установим важное свойство мультипликативной группы конечного поля.

Теорема (о строении мультипликативной группы конечного поля). *Мультипликативная группа любого конечного поля — циклическая.*

Proof. Пусть K — поле из p^n элементов и $m = p^n - 1$ — порядок его мультипликативной группы. Будем считать, что $m \geq 4$ — иначе наше утверждение тривиально.

Предположим, что каноническое разложение m имеет вид

$$m = p_1^{k_1} \dots p_r^{k_r}.$$

Как известно, для каждого натурального числа i, удовлетворяющего неравенствам $1 \leq i \leq r$, уравнение $x^{\frac{m}{p_i}} - 1 = 0$ имеет в поле K не более $\frac{m}{p_i}$ решений, поэтому можно найти такой элемент $\alpha_i \in K^*$, что $\alpha_i^{\frac{m}{p_i}} \neq 1$. Для каждого i зафиксируем α_i, положим $\beta_i = \alpha_i^{\frac{m}{{p_i}^{k_i}}}$ и рассмотрим $\operatorname{ord}\beta_i$ — порядок элемента β_i в группе K^*. Из теоремы Лагранжа следует, что $\alpha_i^m = 1 = \beta^{{p_i}^{k_i}}$, поэтому $\operatorname{ord}\beta_i$ является делителем числа ${p_i}^{k_i}$, то есть $\operatorname{ord}\beta_i = {p_i}^{l_i}$ для некоторого l_i при $0 \leq l_i \leq k_i$. Заметим, что при этом число l_i не может быть меньше k_i : в противном случае оказалось бы, что $\beta^{{p_i}^{k_i - 1}} = 1$, хотя $\beta^{{p_i}^{k_i - 1}} = \alpha_i^{\frac{m}{p_i}} \neq 1$. Таким образом, мы имеем $\operatorname{ord}\beta_i = {p_i}^{k_i}$ для каждого индекса i.

Рассмотрим далее произведение $\beta = \beta_1 \dots \beta_r$. Из-за соотношения $\beta^m = 1$ число m делится на $\operatorname{ord}\beta$, а потому

$$\operatorname{ord}\beta = {p_1}^{t_1} \dots {p_r}^{t_r}$$

при некоторых $t_i \leq k_i$. Предположим на минуту, что для некоторого индекса i имеется неравенство $t_i < k_i$; переставляя при необходимости сомножители в каноническом разложении m, можно, конечно, считать, что $t_1 < k_1$. Тогда для числа $s = p_1^{k_1 - 1} \dots p_r^{k_r}$ выполняется равенство $\beta^s = 1 = \beta_1^s \dots \beta_r^s$. Заметим, что при этом $\beta_j^s = 1$ при $j > 1$, поскольку s делится на $\operatorname{ord}\beta_j$. Но тогда оказывается, что $\beta_1^s = 1$ и потому число s делится на $\operatorname{ord}\beta_1 = p_1^{k_1}$, что противоречит выбору s. Таким образом, в описанной ситуации мы имеем $t_i = k_i$ для всех индексов i и $\operatorname{ord}\beta = m$, а это значит, что циклическая подгруппа, порожденная β, совпадает с K^*. □

Следствие. *Если K — конечное поле, а k — его подполе, то расширение K/k — простое.*

Proof. Если циклическая группа K^* порождена элементом θ, то $K = k(\theta)$. □

Следующая теорема служит естественным дополнением к теореме о существовании конечного поля.

Теорема (о единственности конечного поля). *Для любого простого числа p и произвольного натурального n все поля, состоящие из p^n элементов, изоморфны между собой.*

Proof. Пусть K_1 и K_2 — два поля, каждое из которых содержит ровно p^n элементов, и k — поле вычетов по модулю p. По следствию из предыдущей теоремы оба расширения K_1/k и K_2/k являются простыми; в частности, $K_1 = k(\theta_1)$ для некоторого θ_1 из K_1. Если g — минимальный аннулятор элемента θ_1 над k, то его степень равна n, а сам g является делителем в кольце $k[x]$ многочлена $f = x^{p^n} - x$ как аннулятора всех элементов поля K_1.

С другой стороны, в кольце $K_2[x]$ многочлен f также раскладывается на линейные множители; следовательно, в поле K_2 у многочлена g имеется некоторый корень θ_2. В этой ситуации g является минимальным аннулятором θ_2 над k, степень расширения $k(\theta_2)/k$ совпадает со степенью расширения K_2/k и поэтому $K_2 = k(\theta_2)$. Дальше остается сослаться на доказанное в предыдущем параграфе предложение об изоморфности простых расширений, порожденных корнем одного и того же неприводимого многочлена g. □

Замечание. *Доказанные теоремы о существовании и единственности позволяют в дальнейшем говорить просто о поле из p^n элементов. Это поле традиционно обозначают* $\mathrm{GF}(p^n)$ *и называют* полем Галуа *из p^n элементов (обозначение связано, конечно, с английским названием Galois field — поле Галуа, как иначе называют конечное поле); в последние годы, впрочем, более употребительным является обозначение $\mathbb{F}_{p^n}$ (по аналогии с $\mathbb{Q}$, $\mathbb{R}$ и т.д.) — этим обозначением мы и будем пользоваться далее. В частности, $\mathbb{F}_p$ — это поле вычетов по простому модулю p.*

Для произвольных простого p и натурального n поле $\mathbb{F}_{p^n}$ имеет, разумеется, конечное число подполей. Опишем их все.

Теорема (о подполях конечного поля). *1) Каждое подполе поля $\mathbb{F}_{p^n}$ состоит из p^m элементов, где m — некоторый делитель числа n.*

2) Для любого делителя m числа n существует единственное подполе поля $\mathbb{F}_{p^n}$, состоящее из p^m элементов.

Proof. Первое утверждение теоремы очевидно: в самом начале этого параграфа мы доказали, что если K — конечное поле, а k — его подполе, то $|K| = |k|^{(K:k)}$. Докажем второе утверждение.

Если n делится на m и $n = mr$, то

$$p^n - 1 = p^{mr} - 1 = (p^m - 1)\left(p^{m(r-1)} + p^{m(r-2)} + \ldots + p^m + 1\right)$$

и поэтому $p^n - 1$ делится на $p^m - 1$. Это значит, что в кольце $\mathbb{F}_{p^n}[x]$ многочлен $f = x^{p^n-1} - 1$ делится на многочлен $g = x^{p^m-1} - 1$: действительно, многочлен f раскладывается в этом кольце на линейные множители и не имеет кратных корней (объясните, почему), а каждый корень многочлена g является корнем f, причем простым корнем (его производная равна $(p^m - 1)x^{p^m-2} = -x^{p^m-2}$ и имеет только нулевой корень). В этой ситуации многочлен $F = x^{p^n} - x$ делится на многочлен $G = x^{p^m} - x$. Поскольку наше поле $\mathbb{F}_{p^n}$ является полем разложения над $\mathbb{F}_p$ многочлена F, поле $\mathbb{F}_{p^n}$ содержит и некоторое поле разложения многочлена G — именно, подполе L, получающееся присоединением к $\mathbb{F}_p$ всех корней многочлена G. Нетрудно проверить, что поле L содержит в точности p^m элементов (покажите это, вспомнив доказательство теоремы о существовании конечного поля).

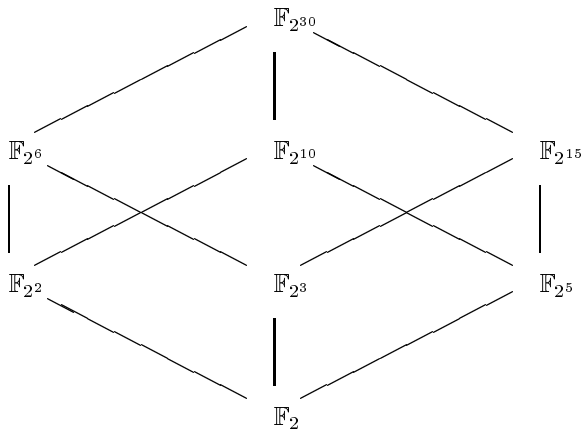
Предположим теперь, что L_1 — другое подполе поля $\mathbb{F}_{p^n}$, состоящее из p^m элементов: $L_1 \neq L$. В этом случае все элементы L_1 являются корнями уравнения $x^{p^m} - x = 0$ и поэтому корнями того же уравнения являются все элементы множества $L \cup L_1$. Таким образом, число корней многочлена G в поле $\mathbb{F}_{p^n}$ оказалось больше, чем степень этого многочлена. Полученное противоречие доказывает единственность искомого подполя. □

Следствие. *Над любым конечным полем существуют неприводимые многочлены произвольной степени.*

Proof. Пусть k — какое-нибудь поле из p^m элементов и n — произвольное натуральное число. Фиксируем некоторое поле K из p^{mn} элементов и обозначим через k_1 его единственное подполе, состоящее из p^m элементов. Из результатов этого параграфа следует, что K/k_1 — простое расширение степени n. Пусть $K = k_1(\theta)$ и $g = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ — минимальный аннулятор элемента θ из $k_1[x]$. Если $\varphi : k_1 \to k$ — изоморфизм полей, то многочлен $x^n + \varphi(\alpha_1)x^{n-1} + \ldots + \varphi(\alpha_n)$ неприводим в $k[x]$ (объясните, почему). □

Мы закончим этот параграф маленьким примером описания взаимного расположения подполей конечного поля.

Пример. *Опишем все подполя поля* $\mathbb{F}_{2^{30}}$ *— отрезками соединены пары "поле–подполе":*



§ 3. Элементы теории Галуа

Первый круг вопросов, который мы обсудим в этом параграфе, связан с особенностями минимальных аннуляторов алгебраических элементов, а потому — и с особенностями неприводимых многочленов.

Пусть k — некоторое поле, f — неприводимый в $k[x]$ многочлен и K — какое-нибудь его поле разложения: $f = \beta(x-\alpha_1)\dots(x-\alpha_n)$ в $K[x]$. Если все элементы α_i попарно различны, то есть если f не имеет кратных корней в своем поле разложения, то многочлен f называют *сепарабельным*. Таким образом, *несепарабельный многочлен* — это неприводимый многочлен из $k[x]$, имеющий кратные корни в своем поле разложения. Следующее утверждение можно рассматривать как описание несепарабельных многочленов, не зависящее от поля разложения.

Предложение. *Пусть k — произвольное поле и f — неприводимый многочлен из $k[x]$. Этот многочлен является несепарабельным тогда и только тогда, когда его производная f' — нулевой многочлен.*

Proof. Обозначим через K какое-нибудь поле разложения нашего многочлена f и будем считать, что $f = \beta(x-\alpha_1)\dots(x-\alpha_n)$ при некоторых $\beta \neq 0, \alpha_1, \dots, \alpha_n$ из K.

Если f' — нулевой многочлен, то по теореме из § 1 главы VI каждый α_i является кратным корнем f, откуда следует несепарабельность f.

Предположим теперь, что многочлен f несепарабелен и $\alpha_1 = \alpha_2$ для нашего разложения. Тогда по уже упоминавшейся теореме о кратных корнях имеем $f'(\alpha_1) = 0$. Рассмотрим наибольший общий делитель d многочлена f и его производной f' в кольце $k[x]$. Из существования линейного представления d следует, что $d(\alpha_1) = 0$, а потому d является аннулятором элемента α_1 в кольце $k[x]$. Но принадлежащий этому же кольцу многочлен f является неприводимым аннулятором α_1, поэтому он ассоциирован с минимальным аннулятором α_1 и потому многочлен d делится на f. В таком случае многочлены d и f ассоциированы и f' делится на f. Из сравнения степеней f и f' понятно, что это возможно только при $f' = 0$. □

Примеры. *1) Если k — поле нулевой характеристики, то каждый неприводимый над k многочлен сепарабелен (докажите это!).*

2) Над конечным полем $\mathbb{F}_{p^n}$ каждый неприводимый многочлен сепарабелен. Действительно, если $f = x^m + \alpha_1 x^{m-1} + \dots + \alpha_m$ — неприводимый несепарабельный многочлен, то $f' = 0$, а это значит, что m делится на p и $f = x^{pr} + \beta_1 x^{p(r-1)} + \dots + \beta_r$ при некотором r. Если какой-то коэффициент β_i такого многочлена

отличен от нуля, то $\beta_i^{p^n} = \beta_i$ *(объясните, почему) и, следовательно,* $\beta_i = \gamma_i^p$ *для некоторого* $\gamma_i \in \mathbb{F}_{p^n}^*$. *Но тогда мы имеем равенство*

$$f = x^{pr} + \gamma_1^p x^{p(r-1)} + \ldots + \gamma_r^p = \left(x^r + \gamma_1 x^{r-1} + \ldots + \gamma_r\right)^p,$$

противоречащее неприводимости многочлена f.

3) *Пусть* $k = \mathbb{F}_p[t]$ *— поле рациональных функций от переменной* t *над полем вычетов по простому модулю* p. *Многочлен* $f = x^p - t$ *в кольце* $k[x]$ *неприводим (подробное доказательство этого факта, использующее технику последнего параграфа главы VI для факториальных колец, мы приводить не будем) и, очевидно, несепарабелен.*

Алгебраический элемент θ расширения K/k назовем *сепарабельным* или *несепарабельным элементом этого расширения* в зависимости от того, сепарабельным или несепарабельным является его минимальный аннулятор (таким образом, оба эти термина осмыслены только для алгебраических элементов). Отметим, что если θ — сепарабельный элемент расширения K/k и L — промежуточное поле этого расширения, то θ сепарабелен и над L (объясните, почему); обратное верно, вообще говоря, не всегда.

Если K/k — алгебраическое расширение и все элементы этого расширения сепарабельны, то K/k мы будем называть *сепарабельным расширением;* в противном случае (то есть если K содержит хотя бы один несепарабельный над k элемент) мы будем говорить, что K/k — *несепарабельное расширение.* В частности, любое алгебраическое расширение поля нулевой характеристики является его сепарабельным расширением; произвольное конечное поле — это сепарабельное расширение всякого своего подполя.

Следующее утверждение описывает важное свойство сепарабельных расширений.

Теорема (о простоте сепарабельных расширений). *Любое конечное сепарабельное расширение является простым.*

Proof. Пусть K/k — конечное сепарабельное расширение и $(K : k) = n$; оба поля мы можем считать бесконечными — иначе наше утверждение уже доказано в § 2. Для $n = 1$ наше утверждение тривиально, поэтому будем считать $n > 1$.

Возьмем в K произвольный элемент α_1, не принадлежащий k, и, присоединив его к полю k, рассмотрим промежуточное поле $K_1 = k(\alpha_1)$ нашего расширения. Мы уже отмечали, что каждый элемент поля K сепарабелен над K_1. Если $K_1 = K$, то наше утверждение установлено. В противном случае мы имеем $1 < (K : K_1) < n$ и можно, взяв в K какой-нибудь элемент α_2, не принадлежащий K_1, рассмотреть промежуточное поле $K_2 = K_1(\alpha_2)$ расширения K/K_1. Расширение K/K_2 сепарабельно и $(K : K_2) < (K : K_1)$. Продолжая описанный процесс, мы за конечное число шагов построим цепочку последовательных простых расширений, связывающих k и K :

$$k \subset K_1 \subset K_2 \subset \ldots \subset K_r = K.$$

Поскольку каждое звено в этой цепочке является конечным простым сепарабельным расширением, для доказательства нашей теоремы достаточно показать, что любые два звена из простых расширений в этой цепочке можно заменить одним, то есть доказать, что если $k(\alpha)/k$ и $k(\alpha, \beta)/k$ — два простых конечных сепарабельных расширения, то $k(\alpha, \beta) = k(\gamma)$ для некоторого элемента γ из поля $k(\alpha, \beta)$.

Рассмотрим над полем k минимальный аннулятор f элемента α и минимальный аннулятор g элемента β. Пусть $\deg f = r$ и $\deg g = s$, а L — какое-нибудь поле разложение произведения $f \cdot g$ над полем $k(\alpha, \beta)$. Заметив, что в поле L наши многочлены f и g не имеют кратных корней (объясните, почему), будем полагать, что $\alpha_1 = \alpha, \ldots, \alpha_r$ — все корни f, принадлежащие L, а $\beta_1 = \beta, \ldots, \beta_s$ — все содержащиеся в L корни g. В нашем бесконечном поле k можно выбрать такой ненулевой μ, что равенство

$$\alpha_i + \mu\beta_m = \alpha_j + \mu\beta_l$$

имеет место в том и только том случае, когда $i = j$ и $m = l$: действительно, для этого достаточно взять любой ненулевой μ так, чтобы выполнялись неравенства

$$\mu \neq \frac{\alpha_j - \alpha_i}{\beta_m - \beta_l}$$

при всех $i \neq j$ и $r \neq t$, то есть сделать для μ запретными только конечное число значений.

Зафиксировав μ с описанными свойствами, положим далее

$$\gamma = \alpha + \mu\beta$$

и заметим, что этот элемент принадлежит полю $k(\alpha, \beta)$. Следовательно, $k(\gamma)$ — подполе $k(\alpha, \beta)$. Остается показать, что α и β содержаться в $k(\gamma)$.

Рассмотрим многочлен $h(x) = f(\gamma - \mu x)$ — его коэффициенты принадлежат, как легко понять, полю $k(\gamma)$. Из равенств

$$h(\beta) = f(\gamma - \mu\beta) = f(\alpha) = 0$$

следует, что h — аннулятор β над $k(\gamma)$. С другой стороны, g — также аннулятор β над $k(\gamma)$, поэтому принадлежащий кольцу $k(\gamma)[x]$ унитальный наибольший общий делитель d многочленов h и g также является аннулятором β. Будучи делителем g, многочлен d раскладывается в кольце $L[x]$ на линейные множители и не имеет кратных корней. Более того, в поле L он вообще не имеет корней, отличных от β. Действительно, его другим корнем может быть только какой-то β_m при $m > 1$, но тогда β_m оказался бы корнем многочлена h и мы имели бы $h(\beta_m) = f(\gamma - \mu\beta_m) = 0$, хотя $\gamma - \mu\beta_m \neq \alpha_i$ для произвольного i по выбору μ. Это значит, что $d = x - \beta$ и $\beta \in k(\gamma)$. Понятно, что тогда $\alpha = \gamma - \mu\beta$ также принадлежит $k(\gamma)$. □

Теперь мы введем еще один важный термин: произвольный изоморфизм поля на себя мы будем называть *автоморфизмом* этого поля.

Пример. *Для конечного поля $\mathbb{F}_{p^n}$ рассмотрим отображение $\varphi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, при котором каждому $\alpha \in \mathbb{F}_{p^n}$ сопоставляется $\varphi(\alpha) = \alpha^p$. Это отображение согласовано, очевидно, с умножением и является автоморфизмом аддитивной группы нашего поля (докажите это, использовав лемму из § 2). Следовательно, φ — автоморфизм поля $\mathbb{F}_{p^n}$; он называется* автоморфизмом Фробениуса.

Легко проверить, что множество всех автоморфизмов поля K образует группу относительно композиции — эту группу естественно обозначать $\mathrm{Aut}(K)$. Если k — какое-нибудь подполе поля K и $\sigma \in \mathrm{Aut}(K)$ не меняет элементов этого подполя, то есть $\sigma(\alpha) = \alpha$ при любом α из k, то σ называется *автоморфизмом расширения K/k.*

Примеры. *1) Для любого подполя k поля K тождественный автоморфизм ε_K является автоморфизмом расширения K/k.*

2) Любой автоморфизм $\sigma \in \mathrm{Aut}(K)$ переводит 1_K в 1_K; из этого следует (объясните, почему), что если k — простое подполе поля K, то каждый автоморфизм K является автоморфизмом расширения K/k.

3) Комплексное сопряжение — единственный нетождественный автоморфизм расширения $\mathbb{C}/\mathbb{R}$ (докажите это!).

Множество всех автоморфизмов расширения K/k мы будем обозначать $\mathrm{Aut}(K/k)$. Легко понять, что $\mathrm{Aut}(K/k)$ — подгруппа группы $\mathrm{Aut}(K)$.

Далее в этом параграфе мы часто будем рассматривать группы автоморфизмов алгебраических и, в частности, простых алгебраических расширений. Сформулируем в этой связи несколько свойств автоморфизмов расширения.

Предложение. *Предположим, что в расширении K/k элемент θ алгебраичен и g — его минимальный аннулятор степени n. Тогда*

1) для любого $\sigma \in \mathrm{Aut}(K/k)$ элемент $\sigma(\theta)$ является корнем g;

2) если $K = k(\theta)$ и η — произвольный корень многочлена g, принадлежащий полю K, то отображение $\sigma : K \to K$, определяемое равенством

$$\sigma(\alpha_0 + \alpha_1\theta + \ldots + \alpha_{n-1}\theta^{n-1}) = \alpha_0 + \alpha_1\eta + \ldots + \alpha_{n-1}\eta^{n-1}$$

при любых $\alpha_i \in k$, является автоморфизмом расширения K/k;

3) если $K = k(\theta)$, то автоморфизмами, описанными в предыдущем пункте, исчерпывается вся группа $\mathrm{Aut}(K/k)$;

4) если $K = k(\theta)$, то группа $\mathrm{Aut}(K/k)$ конечна и ее порядок не превосходит степени расширения.

Proof. 1) Если $g = x^n + \beta_1 x^{n-1} + \ldots + \beta_n$, то

$$g(\sigma(\theta)) = \sigma(\theta)^n + \sigma(\beta_1)\sigma(\theta)^{n-1} + \sigma(\beta_n) = \sigma(\theta^n + \beta_1\theta^{n-1} + \ldots + \beta_n) = \sigma(0) = 0.$$

2) Напомним (мы говорили об этом в § 1), что в ситуации этого пункта $(1, \theta, \ldots, \theta^{n-1})$ — базис K как пространства над k, поэтому отображение σ определено корректно; понятно также, что $\sigma(\alpha) = \alpha$ при всяком $\alpha \in k$. Для любого корня $\eta \in K$ многочлена g сам g является его минимальным аннулятором над k и поэтому $(1, \eta, \ldots, \eta^{n-1})$ — также базис расширения K/k. Из этого следует, что σ — автоморфизм аддитивной группы поля K. Чуть сложнее доказывается согласованность σ с умножением.

Заметим, что наше определение σ можно сформулировать несколько иначе: $\sigma(r(\theta)) = r(\eta)$ для любого многочлена r из $k[x]$, если $\deg r < n$. Произвольные элементы μ и ν из поля K можно записать в виде $\mu = f(\theta)$ и $\nu = h(\theta)$, где f и h — многочлены из $k[x]$, степени которых меньше n. Пусть $fh = gq + r$ для многочленов q и r, причем $\deg r < n$. Тогда

$$\sigma(\mu\nu) = \sigma(f(\theta)h(\theta)) = \sigma(r(\theta)) = r(\eta) = f(\eta)h(\eta) = \sigma(\mu)\sigma(\nu)$$

и $\sigma \in \mathrm{Aut}(K/k)$.

3) Достаточно применить первую часть утверждения.

4) В силу пункта 3) число различных автоморфизмов расширения K/k определяется числом корней многочлена g, а это число не превосходит n.

□

Теперь мы вычислим группу автоморфизмов конечного поля, совпадающую, как уже говорилось, с группой автоморфизмов этого поля над его простым подполем.

Теорема (об автоморфизмах конечного поля). *Группа $\mathrm{Aut}(\mathbb{F}_{p^n})$ является циклической группой порядка n. В качестве образующей этой группы можно взять автоморфизм Фробениуса.*

Proof. В § 2 мы уже говорили, что $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$, где θ — образующий элемент циклической группы $\mathbb{F}^*_{p^n}$ порядка $p^n - 1$. Каждый автоморфизм расширения $\mathbb{F}_{p^n}/\mathbb{F}_p$ определяется, как установлено последним предложением, некоторым корнем минимального аннулятора g элемента θ. Используя лемму из § 2, несложно проверить, что элементы $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$ являются корнями многочлена g; легко заметить также, что все эти корни попарно различны: если $\theta^{p^i} = \theta^{p^j}$ при $0 \le i < j \le n-1$, то $\theta^{p^{j-i}} = 1$ и $p^{j-i} \le p^{n-1} < p^n - 1$, а это противоречит тому, что θ — образующий элемент циклической группы порядка $p^n - 1$. Значит, $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$ — это все корни g и $|\mathrm{Aut}(\mathbb{F}_{p^n})| = n$. Остается заметить, что если автоморфизм σ_i поля $\mathbb{F}_{p^n}$ определяется равенством $\sigma_i(\theta) = \theta^{p^i}$, то $\sigma_1 = \varphi$ — автоморфизм Фробениуса и $\sigma_i = \varphi^i$ (разберитесь в деталях этого рассуждения). □

Фиксируем теперь произвольное расширение K/k и положим $G = \mathrm{Aut}(K/k)$. С каждым промежуточным полем L нашего расширения и с каждой подгруппой H группы G свяжем множества

$$G_L = \{\sigma \in G \mid \sigma(\alpha) = \alpha \text{ при всех } \alpha \in L\} \qquad \text{и} \qquad K^H = \{\alpha \in K \mid \sigma(\alpha) = \alpha \text{ при всех } \sigma \in H\}.$$

Нетрудно проверить (проверьте!), что G_L — подгруппа группы G, а K^H — промежуточное поле расширения K/k. Таким образом, если через $\mathfrak{K}$ обозначено множество всех промежуточных полей расширения K/k, а через $\mathfrak{G}$ — множество всех подгрупп группы автоморфизмов этого расширения, то мы определили два отображения: $\mathfrak{K} \to \mathfrak{G}$, при котором $L \mapsto G_L$, и $\mathfrak{G} \to \mathfrak{K}$, при котором $H \mapsto K^H$; эту пару отображений принято называть *соответствием Галуа*. Нетрудно проверить (сделайте это!), что соответствие Галуа обладает следующими замечательными свойствами:

Предложение. *Для произвольного расширения K/k с группой автоморфизмов G*

1) если L_1 и L_2 — два промежуточных поля и $L_1 \subseteq L_2$, то $G_{L_2} \subseteq G_{L_1}$;

2) если H_1 и H_2 — две подгруппы группы G и $H_1 \subseteq H_2$, то $K^{H_2} \subseteq K^{H_1}$;

3) если L — любое промежуточное поле, то $L \subseteq K^{G_L}$;

4) если H — любая подгруппа группы G, то $H \subseteq G_{K^H}$.

Далее мы покажем, что при определенных условиях для конечного расширения пара отображений из соответствия Галуа является парой взаимно обратных биекций, а сейчас установим один важный факт, связанный с конечными группами автоморфизмов.

Лемма (Артин). *Пусть K — произвольное поле, G — какая-нибудь конечная группа его автоморфизмов (необязательно совпадающая с $\mathrm{Aut}(K)$) и $k = K^G$ — подполе K, состоящее из всех элементов, которые не меняются под действием любого автоморфизма группы G. Тогда K/k — конечное расширение и $(K : k) = |G|$.*

Proof. Рассуждаем индукцией по порядку группы G. Если G состоит только из тождественного автоморфизма, что наше утверждение тривиально: $k = K$. Пусть $|G| > 1$ и α — какой-нибудь элемент поля K, не принадлежащий k. Сопоставим этому элементу конечное множество

$$H = \{\tau \in G \mid \tau(\alpha) = \alpha\}.$$

Легко проверить, что H — подгруппа группы G; ясно, что она не совпадает с G. Заметим, что $\sigma_1(\alpha) = \sigma_2(\alpha)$ для двух автоморфизмов σ_1 и σ_2 группы G тогда и только тогда, когда $\sigma_1^{-1}\sigma_2 \in H$, то есть когда σ_1 и σ_2 определяют один и тот же правый смежный класс G по H. Обозначим через m индекс $(G : H)$ и рассмотрим правое разложение Лагранжа

$$G = \bigcup_{i=1}^{m} \sigma_i H,$$

считая $\sigma_1 = \varepsilon_K$. Из наших рассуждений легко следует, что множество $M_\alpha = \{\sigma(\alpha) \mid \sigma \in G\}$ совпадает с множеством $\{\sigma_1(\alpha), \ldots, \sigma_m(\alpha)\}$. Отметим также, что

$$M_\alpha = \{\sigma\sigma_1(\alpha), \ldots, \sigma\sigma_m(\alpha)\}$$

при любом $\sigma \in G$ (объясните, почему).

Теперь нам потребуется многочлен $f = (x-\sigma_1(\alpha)) \ldots (x-\sigma_m(\alpha))$ из кольца $K[x]$. Все корни этого многочлена различны, а один из таких корней совпадает с α. Если $f = x^m + \gamma_1 x^{m-1} + \ldots + \gamma_m$, то каждый коэффициент γ_i с точностью до знака равен значению основного симметрического многочлена $s_i(t_1, \ldots, t_m)$ на корнях f (вспомните формулы Виета). Нетрудно понять (разберитесь в деталях!), что поэтому $\sigma(\gamma_i) = \gamma_i$ при каждом i. Следовательно, все коэффициенты многочлена f принадлежат полю k. Таким образом, α — алгебраический над k элемент, а f — его аннулятор. Нетрудно понять также, что он — минимальный аннулятор данного элемента: f делится на минимальный аннулятор g нашего α, а все $\sigma_1(\alpha), \ldots, \sigma_m(\alpha)$ являются корнями g в силу одного из ранее доказанных предложений этого параграфа. Тем самым мы доказали справедливость равенства

$$(G : H) = (k(\alpha) : k).$$

Далее для расширения K/k мы рассмотрим промежуточное поле K^H. Легко проверить (проверьте!), что K^H содержит $k(\alpha)$ в качестве подполя. Покажем, что на самом деле K^H и $k(\alpha)$ совпадают.

Пусть β — произвольный элемент поля K^H, то есть $\tau(\beta) = \beta$ при всех $\tau \in H$. Используя ранее введенные обозначения для σ_i, рассмотрим над полем K интерполяционную таблицу с m узлами

$\sigma_1(\alpha) = \alpha$	$\sigma_2(\alpha)$	$\ldots$	$\sigma_m(\alpha)$
$\sigma_1(\beta) = \beta$	$\sigma_2(\beta)$	$\ldots$	$\sigma_m(\beta)$

По формуле Лагранжа интерполяционный многочлен наименьшей степени для этой таблицы равен

$$h = \sum_{i=1}^{m} \frac{\sigma_i(\beta) \cdot f}{f'(\sigma_i(\alpha))(x - \sigma_i(\alpha))}.$$

Нетрудно понять, что любой автоморфизм из группы G не меняет коэффициентов многочлена h: под действием σ слагаемые в формуле Лагранжа просто меняются местами. Это значит, что h — многочлен из $k[x]$ и, следовательно, элемент $\beta = h(\alpha)$ принадлежит полю $k(\alpha)$, что доказывает равенство $K^H = k(\alpha)$.

В заключение заметим, что к паре (K, H) применимо индукционное предположение, по которому $(K : k(\alpha)) = |H|$. Таким образом, расширение K/k конечно и

$$(K : k) = (K : k(\alpha)) \cdot (k(\alpha) : k) = |H|(G : H) = |G|.$$

□

Далее в этом параграфе мы будем рассматривать только конечные сепарабельные расширения. Все они являются, как мы знаем, простыми, а потому группы автоморфизмов таких расширений конечны. Особо нас будут интересовать расширения, для которых степень совпадает с порядком группы автоморфизмов. Если для расширения K/k справедливо равенство $(K : k) = |\operatorname{Aut}(K/k)|$, то такое расширение принято называть *расширением Галуа* (вместо обозначения $\operatorname{Aut}(K/k)$ для расширения Галуа обычно применяют обозначение $\operatorname{Gal}(K/k)$, называя эту группу *группой Галуа* указанного расширения).

Примеры. *1) Из теоремы об автоморфизмах конечного поля следует, что каждое конечное поле является расширением Галуа своего простого подполя (напомним, что группа Галуа этого расширения циклична).*

2) Пусть p — простое число. Легко понять, что многочлен

$$f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$$

неприводим в кольце $\mathbb{Q}[x]$: достаточно использовать равенство $f(x) = \frac{x^p-1}{x-1}$ и неприводимость над полем $\mathbb{Q}$ многочлена $f(x+1)$, следующую из критерия Эйзенштейна. Пусть $K = \mathbb{Q}(\varepsilon)$ — комплексное подполе, получающееся присоединением к $\mathbb{Q}$ какого-нибудь корня ε многочлена f. Поскольку каждый отличный от 1 корень p-ой степени из 1 первообразен, поле K является полем разложения многочлена f над $\mathbb{Q}$. Каждый автоморфизм простого расширения $K/\mathbb{Q}$ определяется, очевидно, сопоставлением $\varepsilon \mapsto \varepsilon^r$ при некотором натуральном $r \leq p-1$, поэтому группа $\operatorname{Aut}(K/\mathbb{Q})$ содержит ровно $p-1$ автоморфизмов. Значит, $K/\mathbb{Q}$ — расширение Галуа.

3) Вещественное поле $K = \mathbb{Q}(\sqrt[3]{2})$ является расширением третьей степени поля $\mathbb{Q}$, но не является его расширением Галуа: любой автоморфизм этого расширения определяется единственным вещественным корнем многочлена $x^3 - 2$ и, следовательно, группа $\operatorname{Aut}(K/\mathbb{Q})$ состоит только из тождественного автоморфизма.

Следующее утверждение позволяет понятие расширения Галуа определять несколько иначе.

Предложение. *Пусть K/k — конечное сепарабельное расширение. Тогда равенство $|\operatorname{Aut}(K/k)| = (K : k)$ справедливо в том и только в том случае, когда минимальный аннулятор произвольного элемента этого расширения раскладывается в $K[x]$ на линейные множители.*

Proof. Пусть $(K : k) = n$ и $n > 1$ (иначе наше утверждение тривиально).

Достаточность сформулированного условия легко следует из простоты расширения K/k : если $K = k(\theta)$ и минимальный аннулятор произвольного элемента раскладывается в $K[x]$ на линейные множители, то на линейные множители раскладывается и не имеющий кратных корней минимальный аннулятор g образующего элемента θ, причем в силу одного из предложений этого параграфа автоморфизмы нашего расширения находятся во взаимно однозначном соответствии с корнями g; поэтому $|\operatorname{Aut}(K/k)| = (K : k)$.

Пусть теперь K/k — расширение Галуа и $G = \operatorname{Gal}(K/k)$ — его группа Галуа. Возьмем произвольный α из поля K, обозначим через f его минимальный аннулятор над k и будем считать, что $\deg f = l > 1$. Используя идею доказательства леммы Артина, рассмотрим подгруппу $H = \{\tau \in G \mid \tau(\alpha) = \alpha\}$ и промежуточное поле $L = K^H$. Если $(G : H) = m$ и $G = \bigcup_{i=1}^{m} \sigma_i H$ — правое разложение Лагранжа, то из рассуждений в доказательстве леммы Артина следует, что $\sigma_1(\alpha), \ldots, \sigma_m(\alpha)$ — различные корни f, откуда получаем неравенство $m \leq l$. С другой стороны, по лемме Артина имеем равенство $(K : L) = |H| = \frac{n}{m}$, из чего следует

$$(L : k) = \frac{(K : k)}{(K : L)} = m \leq l = (k(\alpha) : k).$$

В силу очевидного включения $k(\alpha) \subseteq L$ это возможно только при $k(\alpha) = L$ и $m = l$, что означает разложение $f = (x - \sigma_1(\alpha)) \ldots (x - \sigma_m(\alpha))$ в кольце $K[x]$. □

Следствие. *Если K/k — расширение Галуа и L — промежуточное поле этого расширения, то K/L — расширение Галуа.*

Proof. Конечность и сепарабельность расширения K/L очевидны. Если α — элемент K, многочлен g — его минимальный аннулятор над k, а f — минимальный аннулятор над L, то g раскладывается в $K[x]$ на линейные множители и делится на f. Следовательно, и f раскладывается на линейные множители в $K[x]$. Таким образом, K/L является расширением Галуа по доказанному предложению. □

Замечания. *1) Условие на минимальные аннуляторы, описанное в доказанном предложении, можно сформулировать несколько иначе: любой неприводимый в $k[x]$ многочлен, имеющий в K хотя бы один корень, раскладывается в $K[x]$ на линейные множители. Алгебраическое расширение (необязательно конечное), удовлетворяющее этому условию, принято называть* нормальным расширением. *Отметим без пояснений, что расширение, являющееся полем разложения произвольного многочлена, всегда нормально.*

2) Во второй части доказательства мы не использовали сепарабельность расширения Галуа. Более того, из приведенных рассуждений следует, что если $|\operatorname{Aut}(K/k)| = (K : k)$, то наше расширение сепарабельно. Это позволяет определять расширение Галуа как конечное расширение, степень которого совпадает с порядком группы автоморфизмов. В таком случае наш критерий может быть сформулирован следующим образом: конечное расширение является расширением Галуа тогда и только тогда, когда оно сепарабельно и нормально.

Теперь у нас все готово для доказательства основного результата этого параграфа.

Теорема (основная теорема теории Галуа). *Для произвольного расширения Галуа пара отображений, составляющих соответствие Галуа, является парой взаимно обратных биекций.*

Proof. Пусть K/k — расширение Галуа с группой Галуа G. Нам следует показать, что $G_{K^H} = H$ для всех $H \in \mathfrak{G}$ и $K^{G_L} = L$ для всех $L \in \mathfrak{K}$.

Если H — произвольная подгруппа группы G, то, как уже отмечалось, выполняется включение $H \subseteq G_{K^H}$. С другой стороны, подгруппа G_{K^H}, очевидно, является группой Галуа расширения K/K^H, имеющего в силу леммы Артина степень $|H|$. Таким образом, равенство $G_{K^H} = H$ является следствием совпадения порядков этих групп.

Если L — промежуточное поле расширения K/k, то G_L является группой Галуа расширения K/L — в этом случае $(K : L) = |G_L|$. Чтобы получить равенство $K^{G_L} = L$, остается дальше сослаться на включение $L \subseteq K^{G_L}$ и на равенство $(K : K^{G_L}) = |G_L|$, следующее из леммы Артина. □

Следствие. *Множество промежуточных полей расширения Галуа конечно.*

Замечание. *Мы уже говорили, что если K/k — расширение Галуа и L — его промежуточное поле, то K/L — также расширение Галуа. Естественно задать вопрос: является ли в этой ситуации L/k расширением Галуа? Ответ таков: L/k — расширение Галуа тогда и только тогда, когда группа* $\operatorname{Gal}(K/L)$ *является нормальной подгруппой группы* $\operatorname{Gal}(K/k)$; *при выполнении указанного условия группа Галуа расширения L/k изоморфна факторгруппе* $\operatorname{Gal}(K/k)\big/\operatorname{Gal}(K/L)$. *Доказывать эти факты мы не будем.*

В заключение этого параграфа вернемся к упоминавшейся в третьей главе задаче о разрешимости алгебраического уравнения в радикалах. Для простоты ограничимся случаем поля нулевой характеристики.

Сначала уточним постановку задачи. Имеется алгебраическое уравнение $f(x) = 0$, где в качестве f взят многочлен степени n над некоторым полем k (в числовом случае в качестве k обычно берется расширение поля рациональных чисел, полученное присоединением коэффициентов данного многочлена, или просто поле $\mathbb{Q}$ — если все коэффициенты рациональны). С точки зрения рассмотренных в этой главе понятий разрешимость уравнения $f(x) = 0$ в радикалах означает, что существует такая конечная цепочка последовательных расширений

$$k = K_0 \subsetneqq K_1 \subsetneqq \ldots \subsetneqq K_m,$$

что каждый ее член K_{i+1} является полем разложения некоторого многочлена $x^{n_i} - \beta_i$ из $K_i[x]$, а последнее поле K_m содержит поле разложения многочлена f (поле K_{i+1} должно быть именно полем разложения указанного многочлена, а не просто получаться присоединением одного из его корней, как можно было бы подумать, — вспомните решение в радикалах кубического уравнения).

Обозначим поле разложения многочлена f через L. При нулевой характеристике поле L, разумеется, является сепарабельным расширением поля k и, как всякое поле разложения, конечно и нормально над k; таким образом, L/k — расширение Галуа. Группу Галуа G расширения L/k называют также *группой Галуа данного уравнения.* Теория Галуа сводит задачу о существовании описанной цепочки бесконечных полей к проблеме существования в определенном смысле аналогичной цепочки подгрупп конечной группы G. Сформулируем (рапзумеется, без доказательства) на языке теории групп критерий разрешимости в радикалах нашего уравнения: для этого необходимо и достаточно, чтобы для группы G существовала такая цепочка подгрупп

$$\{\varepsilon\} = H_0 \lneqq H_1 \lneqq \ldots \lneqq H_r = G,$$

что каждый ее член H_i является нормальной подгруппой H_{i+1}, а факторгруппа $H_{i+1}\Big/H_i$ — циклическая (конечную группу G, удовлетворяющую поставленному условию, по понятным причинам принято называть *разрешимой).*

Мы не будем здесь подробно останавливаться на вычислении группы Галуа рассматриваемого уравнения — это достаточно сложная задача. Напомним только (об этом говорилось ранее), что автоморфизмы группы Галуа переводят одни корни нашего уравнения в другие, поэтому группу Галуа можно интерпретировать как подгруппу симметрической группы S_n — подгруппу, сохраняющую зависимости между корнями. Некоторые из этих зависимостей очевидны — это формулы Виета, другие могут быть более хитрыми и для их обнаружения требуются весьма изощренные методы. Мы приведем только один (на общем фоне — простенький) пример использования такого рода средств для установления свойств группы Галуа.

Пусть f — унитальный целочисленный многочлен и он неприводим над полем $\mathbb{Q}$ (из шестой главы известно, как это узнать). Выясним, когда группа Галуа уравнения $f(x) = 0$ содержит только четные подстановки. Занумеруем как-нибудь его корни $\alpha_1, \ldots, \alpha_n$ в поле разложения L и рассмотрим произведение

$$\delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)$$

— оно отлично от 0 из-за сепарабельности f. Поскольку произвольный автоморфизм σ из группы Галуа переставляет корни, $\sigma\left(\delta(f)\right)$ может отличаться от $\delta(f)$ только знаком. Точнее, если $\sigma(\alpha_1) = \alpha_{l_1}, \ldots, \sigma(\alpha_n) = \alpha_{l_n}$, то

$$\sigma\left(\delta(f)\right) = (-1)^t\delta(f),$$

где t — число инверсий в перестановке $(l_1, \ldots, l_n)$. Поэтому все автоморфизмы группы G действуют на $\delta(f)$ тождественно тогда и только тогда, когда группа Галуа G нашего уравнения содержится в знакопеременной группе A_n; в этом случае $\delta(f)$ принадлежит полю $L^G = \mathbb{Q}$. Самого произведения $\delta(f)$ мы, конечно, не знаем, зато нам известен его квадрат

$$\delta^2(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = \Delta(f)$$

— он, очевидно, является симметрическим многочленом от корней, с помощью формул Виета может быть вычислен по коэффициентам многочлена f и принадлежит кольцу целых чисел $\mathbb{Z}$. Из наших рассуждений следует, что $\Delta(f)$ является полным квадратом тогда и только тогда, когда группа Галуа G содержится в группе A_n.

Если корни связаны только формулами Виета,то группа Галуа совпадает со всей симметрической группой — это так, например, если рассматривается "общее"уравнение n-ой степени

$$x^n + a_1x^{n-1} + \ldots + a_n = 0$$

(поле k в этом случае можно считать полем рациональных функций от переменных $a_1, \ldots, a_n$ над $\mathbb{Q}$). При $n \geq 5$ единственной нетривиальной нормальной подгруппой симметрической группы S_n является знакопеременная группа A_n, которая, в свою очередь, не имеет нетривиальных нормальных подгрупп (в седьмой главе такие группы мы назвали простыми) и не является циклической. Поэтому при $n \geq 5$ группа S_n неразрешима. С симметрическими группами S_2, S_3 и S_4 ситуация иная. Группа S_2 имеет порядок 2 и, следовательно, для нее есть нужная нам цепочка, состоящая всего из одного звена

$$\{\varepsilon\} \lneqq \mathrm{S}_2.$$

Почти по столь же простой причине разрешима группа шестого порядка S_3 — знакопеременная группа A_3 является циклической подгруппой третьего порядка, поэтому в S_3 можно взять цепочку

$$\{\varepsilon\} \lneqq A_3 \lneqq S_3.$$

Группа же S_4, имеющая порядок 24, оказывается разрешимой из-за того, что ее нормальная подгруппа A_4, имеющая порядок 12, не является простой: в ней содержится абелева нормальная подгруппа четвертого порядка $K_4 = \{\varepsilon, (12)(34), (13)(24), (14)(23)\}$ *(четверная группа Клейна);* поэтому нашим условиям удовлетворяет цепочка

$$\{\varepsilon\} \lneqq \{\varepsilon, (12)(34)\} \lneqq K_4 \lneqq A_4 \lneqq S_4.$$

Таким образом, группа S_4 тоже разрешима.