Конспект по теории Галуа

Максим Васильев

Содержание

1 Общие сведения про поля

1.1 Небольшое введение про поля

Тут я позволю себе опустить определения поля, подполя, характеристики поля, гомоморфизмов полей, поскольку они были пройдены уже на самом курсе алгебры в последнем модуле.

Отдельно позволю себе отметить, что гомоморфизм полей сохраняет единицу (и как следствие является инъективным), а так же, любой гомоморфизм полей $\varphi : K \to L$ порождает гомоморфизм колец многочленов $f \mapsto {}^{\varphi}f$ из $K[x]$ в $L[x]$.

Если $f(x) = a_n x^n + \ldots + a_0 \in K[x]$, тогда ${}^{\varphi}f(x) = \varphi(a_n)x^n + \ldots \varphi(a_0)$.

То что это гомоморфизм колец проверяется непосредственно руками, используя свойства многочленов и гомоморфизмов.

Так же, если мы рассматриваем некоторое кольцо многочленов $K[(x_i)_{i\in I}]$ от произвольного множества переменных, тогда можно сделать гомоморфизм из $K[(x_i)_{i\in I}]$ в некоторое кольцо S, содержащее все $(s_i)_{i\in I}$ и K, тогда можно рассмотреть гомоморфизм-подстановку из $K[(x_i)_{i\in I}]$, переводящий элементы K в себя, а $x_j \mapsto s_j$, где s_j соответствующий для переменной x_j элемент S.

Иначе говоря: $\sum_{k=1}^{n} a_k \left(\prod_{i=1}^{n_k} x_i^{l_i}\right) \mapsto \sum_{k=1}^{n} a_k \left(\prod_{i=1}^{n_k} s_i^{l_i}\right)$. То что это гомоморфизм колец так же проверяется по опрделению, просто все расписать по определению, пользуясь свойствами многочленов и колец.

1.2 Подполя.

Перечислю некоторые свойства подполей и одно определение, оно нам понадобится в будущем (далеко в будущем).

Утверждение 1.1. *Пересечение любого семейства подполей некоторого поля F, является подполем в F.*

Доказательство основано на проверке для ненулевых α, β из пересечения, что $\alpha\beta^{-1}$ и $\alpha - \beta$ лежат в пересечении, это достаточно очевидно, так что я откажусь от более формального доказательства и перейду дальше.

Определение 1.1. *Направленное множество – это некоторое непустое множество A с заданным на нем рефлексивным и транзитивным отношением, в котором у любой пары элементов есть верхняя грань.*

Утверждение 1.2. *Если семейство полей при введении на нем отношения включения (как подполей) оказывается направленным множеством, то объединение этих полей является полем. Если же все поля в семействе были подполями поля F, то получившиеся подполе является подполем поля F.*

Доказательство. Рассмотрим семейство полей $\{K_i\}_{i\in I}$, где I – это некоторое индексное множество, тогда покажем, что множество $K = \bigcup_{i\in I} K_i$ является полем относительно операций, заданных следующем образом. Если $\alpha, \beta \in K_j$ для некоторого $j \in I$, то операции сложения и умножения такие же, как в поле F_j.

Это в силу направленности семейства полей по включения создает сложение и умножение для двух произвольных элементов поля, действительно $\alpha, \beta \in K$, тогда $\alpha \in K_i$, $\beta \in K_j$, тогда существует $l \in I$, что $K_i \subset K_l, K_j \subset K_l$, тогда $\alpha\beta, \alpha + \beta \in K_l \subset K$ и если $\beta \neq 0$, то $\beta^{-1}, -\beta \in K_k \subset K$. Так же из этого же свойства направленности следует, что единица и ноль любого K_i являются единицей и нулем K. Таким образом, действительно K является полем.

Для того, чтобы обосновать часть про подполе, то необходимо просто обратить внимание, что $K_i \subset F$, и дальше все сложится само собой. □

Определение 1.2. *Пусть S – некоторое подмножество поля F, тогда кольцом (полем) сгенерированным S называется наименьшее по включению кольцо (поле), содержащее S.*

Данное кольцо (поле) существует, так как пересечение колец (полей), является подкольцом (подполем) F, и тогда можно просто взять пересечение всех колец (полей), содержащих S.

Утверждение 1.3. *Пусть K – подполе поля F, и S – некоторое подмножество F.*

Тогда подкольцо сгенерированное $K \cup S$ обозначается, как $K[S]$ и равно множеству всех конечных линейных комбинаций произвольных конечных произведений степеней элементов из S с коэффициентами из K.

Подполе сгененированное $K \cup S$ обозначается, как $K(S)$ и есть множество произведений $ab^{-1} \in F$, $a, b \in K[S], b \neq 0$, и это изоморфно полю рациональных дробей, порожденному $K[S]$.

Доказательство. Если честно, я не совсем хочу совсем формально расписывать данное утверждение, поскольку оно достаточно техническое и немного муторное, поэтому просто напишу дорогу, к которой надо добавить немного формализма.

Тут есть 2 пути, насчет минимального подкольца, просто отожденствить с каждым элементом $s \in S$ свою формальную переменную x_s, рассмотреть кольцо многочленов $K[(x_s)_{s\in S}]$ от всех возможных переменных отождественных с элементами, и затем использовать гомоморфизм колец из $K[(x_s)_{s\in S}]$ в F, который на место формальнной переменной поставит соответствующий ей элемент. Тогда образ гомоморфизма в F равен множеству всех линейных комбинаций произвольных конечных произведений степеней элементов из S с коэффициентами из K. (тут надо помучаться с формальщиной, например, почему подстановка является гомоморфизмом и почему мы покроем все возможные линейные комбинации, это несложно, но больно).

Другой путь это просто взять и показать руками, что все аксиомы кольца (ассоциативного, коммутативного с единицей) выполняются, что тоже не очень приятно.

Теперь если мы покажем, что множество всех конечных линейных комбинаций конечных произведений степеней элементов из S с коэффициентами из K есть подкольцо F, то остается только сказать, что оно содержится в любом подкольце содержащем $K \subset S$ в силу свойств кольца, и это нам и даст равенство $K[S]$.

С $K(S)$ чуть проще, оно в том числе является кольцом, а следовательно содержит $K[S]$, но тогда в силу того, что поле. и содержит все элементы типа $ab^{-1} \in F, a, b \in K[S], b \neq 0$, это поле, изоморфное $\mathrm{Quot}(K[S])$, при помощи изоморфизма $ab^{-1} \mapsto \frac{a}{b}$. Минимальность опять же очевидна, из того, что если множество содержит $K \subset S$ и является полем, следовательно содержит $K[S]$, а в силу того, что поле содержит $K(S)$, хорошо. □

Теперь в частности, если у нас K минимальное подполе F, то есть поле содержащееся в любом подполе F (оно изморфно $\mathbb{Q}$ при $\mathrm{char}\ F = 0$, и $\mathbb{Z}_p$ при $\mathrm{char}\ F = p$), то можно просто считать, что наше подполе сгененированое $K \subset S$, может быть сгенерировано просто S, а K там появится автоматически.

Следствие 1.3.1. *Пусть F это поле, K – подполе F и $S \subset F$ некоторое подмножество, $\alpha_1, \ldots, \alpha_n \in F$, тогда*

1. $x \in K[\alpha_1, \ldots, \alpha_n] \Leftrightarrow x = f(\alpha_1, \ldots \alpha_n)$, *для некоторого многочлена* $f(x) \in K[x_1, \ldots, x_n]$
2. $x \in K(\alpha_1, \ldots, \alpha_n) \Leftrightarrow x = r(\alpha_1, \ldots \alpha_n)$, *где* $r(x_1, \ldots, x_n)$ *некоторая рациональная функция с коэффициентами из* K
3. $x \in K[S] \Leftrightarrow x \in K[\alpha_1, \ldots, \alpha_n]$ *для некоторых* $\alpha_i \in S$.
4. $x \in K(S) \Leftrightarrow x \in K(\alpha_1, \ldots, \alpha_n)$ *для некоторых* $\alpha_i \in S$.

Если первые 2, то это просто напросто уже доказанное утверждение выше, то последние 2 следуют из того, что все объекты в наших утверждениях были конечны.

1.3 Композиция полей

Определение 1.3. *Композицией непустого семейства подполей $(K_i)_{i\in I}$ поля F есть подполе $\prod_{i\in I} K_i$ (обозначается как умножение подполей), сгененированное множеством $\bigcup_{i\in I} K_i$.*

Вообще говоря, идеологически композиция полей очень сильно похожа на сумму векторных пространств, так как это некоторый способ объединить поля минимальным образом, создать из них новое поле.

Теперь достаточно техническое утверждение о композиции подполей.

Утверждение 1.4. *Пусть $(K_i)_{i\in I}$ некоторое непустое семейство подполей поля F, тогда $x \in \prod_{i\in I} K_i \Leftrightarrow x = ab^{-1}, a, b \in R, b \neq 0$, где R множество всех конечных сумм конечных произведений элементов из $\bigcup_{i\in I} K_i$.*

Доказательство. Для начала мы знаем, что в $\prod_{i\in I} K_i$ содержится минимальное подполе F, назовем его K_0, тогда можно сказать, что $\prod_{i\in I} K_i$ сгенерировано $K_0 \cup \left(\bigcup_{i\in I} K_i\right)$, а следовательно, $\prod_{i\in I} K_i = K_0(\bigcup_{i\in I} K_i)$, тогда мы знаем из предыдущей теоремы и ее следствия, что $x \in \prod_{i\in I} K_i \Leftrightarrow x = ab^{-1}, b \neq 0$, где a, b это конечные линейные комбинации конечных произведений степеней элементов из $\bigcup_{i\in I} K_i$ с коэффициентами из K_0, но K_0 принадлежит любому K_i чисто по определению минимального подполя, тогда и коэффициент из K_0 тоже принадлежит $\bigcup_{i\in I} K_i$. В свою очередь любая степень любого элемента из подполя K_i принадлежит ему же по определению, следовательно, степени элементов из $\bigcup_{i\in I} K_i$ принадлежат этому же объединению множеств.

Итого, складывая эти 2 факта, получаем, что действительно конечные линейные комбинации конечных произведений степеней элементов из $\bigcup_{i\in I} K_i$ с коэффициентами из K_0 есть конечная сумма элементов из $\bigcup_{i\in I} K_i$ (любая конечная сумма очевидно является линейной комбинацией с коэффициентом 1), тогда следующее верно $x \in \prod_{i\in I} K_i \Leftrightarrow x = ab^{-1}, a, b \in R, b \neq 0$, где R - множество конечных сумм произведений элементов из $\bigcup_{i\in I} K_i$ □

В случае, если семейство подполей конечно, то композицию можно обозначить как $F_1 \cdot \ldots \cdot F_n$, точки можно опустить.

Теперь из очевидного, из определения автоматически следует, что для двух полей K, F, если существует композиция KF, то она равна FK.

Теперь покажем ассоциативность операции взятия композиции.

Предложение 1.5. *Если K, F, E подполя некоторого поля, то $K(FE) = (KF)E = KFE$*

Доказательство. При доказательстве этого предложения, мы будем сильно опираться на предыдущее утверждение, описывающее композиции подполей.

Покажем, что $K(FE) = KFE$, из этого будет следовать все остальное. Если $x \in KFE$, тогда и только тогда $x = ab^{-1}$, где a, b являются конечной суммой конечных произведений элементов из $K \cup F \cup E$.

Если $x \in K(FE)$, тогда и только тогда $x = ab^{-1}$, где a, b являются конечной суммой конечных произведений элементов из $K \cup FE$.

Теперь если a это произвольная конечная сумма конечных произведений элементов из $K \cup F \cup E$, то в силу того, что $F \subset FE, E \subset FE$, то это конечная сумма конечных произведений элементов из $K \cup FE$.

Теперь в другую сторону, если a это произвольная конечная сумма конечных произведений элементов из $K \cup FE$, то вспомним, что любой элемент FE это конечная сумма произведений элементов из $F \cup E$, тогда расписывая в произведении элемент из FE как сумму и раскрывая скобки по дистрибутивности, мы представим a как конечную сумму конечных произведений элементов из $K \cup F \cup E$. Свойство конечности сохранится, так как у нас конечное количество элементов из FE, и каждый из них расписывается в конечную сумму.

Таким образом, любой элемент из $K(FE)$ может быть представлен в виде элемента KFE и наоборот. Тогда равенство доказано. □

2 Расширения полей

2.1 Пространные размышления о том, что такое расширение поля

Определение 2.1. *Расширение E поля K есть некоторое поле E, такое, что K является в нем подполем.*

Будем обозначать это так же как теоретико-множественное включение, то есть $K \subseteq E$.

Вообще говоря есть и другой, во многих случаях более удобный случай вводить определение расширения поля, а именно E есть расширения поля K, если существует гомоморфизм из K в E. Это определение во многом удобнее, поскольку может связать объекты разной природы, например при присоединении корня неприводимого многочлена, мы столкнемся с расширением поля, объекты которого будут смежные классы в факторкольце многочленов по некоторому неприводимому многочлену f. Строго говоря, числа не являются элементами факторкольца кольца многочленов по идеалу, порожденному f, но тут понятно, что число k можно отождествить с $k + (f)$, таким вот простым гомоморфизмом.

Так вот, эти 2 определения эквивалентны с точностью до изоморфизмов, если у нас есть некоторое теоретико-множественное расширение $K \subset E$ и $E \simeq F$, то существует гомоморфизм (сужение изморфизма E и F на K) из K в F.

Теперь, если $\varphi : K \to F$, то $K \simeq \operatorname{Im}\varphi$, а $\operatorname{Im}\varphi \subseteq F$.

Итого, мы будем пользоваться эквивалентностью этих определений с точностью до изоморфизмов, и в случае чего будем включение, как гомоморфизм и теоретико-множественное включение.

Определение 2.2. *Пусть E, F – расширения поля K, то:*

- *K-гомоморфизм, это такой гомоморфизм $\varphi : E \to F$, что $\forall k \in K \varphi(k) = k$.*
- *K-изоморфизм, это K-гомоморфизм E и F, который при этом является изоморфизмом.*

Аналогично определяются K-эндоморфизмы, K-автоморфизмы, K-(подставить слово)морфизмы.

В частности, если 2 расширения K-изоморфны с изоморфизмом $\psi : E \to F$, то можно рассматривать их как 2 одинаковых расширения K, с полностью одинаковой структурой над K, например, если для $\alpha \in E, f(\alpha) = 0, f(x) \in K[x]$, то $f(\psi(\alpha)) = 0$, тоже.

2.2 Степень расширения

Давайте вот прям с этого момента текста и далее договоримся, что мы верим в аксиому выбора, тогда в любом векторном пространстве есть базис. (Это упоминалось в курсе линейной алгебры, да и доказательства этого много где есть).

Определение 2.3. *Для расширения E поля K степень расширения E над K $[E : K]$ есть размерность векторного пространства E над K, если эта размерность конечна, то E – конечное расширение K, иначе бесконечное.*

Утверждение 2.1. *Если $K \subseteq F \subseteq E$ и $[E : K] < \infty$, то $[E : K] = [E : F][F : K]$.*

Это было уже доказано в курсе алгебры на четвертом модуле.

2.3 Простые расширения

Хочу ввести несколько достаточно полезных определений, некоторые из них нам уже знакомы.

Определение 2.4. *Расширение поля $K \subseteq E$ называется конечно сгененрированным, если существует набор $\alpha_1, \dots \alpha_n \in E$, что $E = K(\alpha_1, \dots, \alpha_n)$.*

Расширение E поля K называется простым, если $E = K(\alpha), \alpha \in E$.

Определение 2.5. *Пусть E – расширение поля K, тогда элемент $\alpha \in E$ называется алгебраическим над F, если существует $f(x) \in K[x]$, что $f(\alpha) = 0$, иначе, элемент α – трансцендентный элемент над F.*

Определение 2.6. *Пусть E – расширение поля K и $\alpha \in E$ – алгебарический над K элемент.*

Тогда $\mathrm{Irr}(\alpha : K) = q(x) \in K[x]$ есть неконстнантный приведенный многочлен с минимальной возможной степенью и такой, что $q(\alpha) = 0$.

Некоторые уже известные свойства минимального многочлена, которые не хочется передоказывать.

- $\mathrm{Irr}(\alpha : K)$ – неприводимый многочлен.
- $\mathrm{Irr}(\alpha : K)$ – определен единственным образом.
- $f(x) \in K[x]$, тогда $f(\alpha) = 0 \Leftrightarrow f(x) = \mathrm{Irr}(\alpha : K)(x)g(x), g(x) \in K[x]$

Теперь перейдем к небольшой теореме, которая была уже доказана на курсе алгебры.

Теорема 2.2. *Пусть E – расширение поля K и $\alpha \in E$.*

Если α – трансцендентный элемент над K, то существует K-изоморфизм $K(\alpha) \simeq K(x)$, где $K(x)$ – поле рациональных дробей над $K[x]$.

Если же α – алгебраический элемент, то пусть $q(x) = \mathrm{Irr}(\alpha : K)$, и тогда $K[\alpha] = K(\alpha) \simeq K[x]/(q(x))$ и $[K(\alpha) : K] = \deg q(x)$ и $1, \alpha, \dots, \alpha^{n-1}$ – базис $K(\alpha)$ над K.

Доказательство. Вторую часть теоремы мы уже доказали на алгебре.

Для первой надо рассмотреть изоморфизм $\psi : K(x) \to K(\alpha)$ где $\psi\left(\frac{f(x)}{g(x)}\right) = f(\alpha)(g(\alpha))^{-1}, g(x) \neq 0 \Rightarrow g(\alpha) \neq 0$, так как трансцендентный элемент над K.

Меня тут укусила формалистская гадина, так как надо хотя бы одно утверждение в этой секции нормально доказать.

Покажем, что это корректный гомоморфизм.

Для начала корректность, если $\frac{f_1(x)}{g_1(x)} = \frac{f_2(x)}{g_2(x)}$, то $f_1(x)g_2(x) = f_2(x)g_1(x)$

Тогда мы знаем, что $f_1(\alpha)g_2(\alpha) = f_2(\alpha)g_1(\alpha)$, в силу трансцендентности это эквивалентно тому, что: $f_1(\alpha)g_1(\alpha)^{-1} = f_2(\alpha)g_2(\alpha)^{-1}$

Теперь из этого следует, что $\psi\left(\frac{f_1(x)}{g_1(x)}\right) = \psi\left(\frac{f_2(x)}{g_2(x)}\right)$

То, что $1 \mapsto 1$ достаточно очевидно, тогда покажем что гомоморфизм сохраняет сумму и произведение.

$$\psi\left(\frac{f_1(x)}{g_1(x)}\cdot\frac{f_2(x)}{g_2(x)}\right)=\psi\left(\frac{f_1(x)f_2(x)}{g_1(x)g_2(x)}\right)=f_1(\alpha)f_2(\alpha)(g_1(\alpha)g_2(\alpha))^{-1}=f_1(\alpha)g_1(\alpha)^{-1}f_2(\alpha)g_2(\alpha)^{-1}=\psi\left(\frac{f_1(x)}{g_1(x)}\right)\psi\left(\frac{f_2(x)}{g_2(x)}\right)$$

$$\psi\left(\frac{f_1(x)}{g_1(x)}+\frac{f_2(x)}{g_2(x)}\right)=\psi\left(\frac{f_1(x)g_2(x)+f_2(x)g_1(x)}{g_1(x)g_2(x)}\right)=(f_1(\alpha)g_2(\alpha)+f_2(\alpha)g_1(\alpha))(g_1(\alpha)g_2(\alpha))^{-1}=$$
$$=f_1(\alpha)g_1(\alpha)^{-1}+f_2(\alpha)g_2(\alpha)^{-1}=\psi\left(\frac{f_1(x)}{g_1(x)}\right)+\psi\left(\frac{f_2(x)}{g_2(x)}\right)$$

Теперь следующий шаг, покажем, что этот гомоморфизм сюръективен (гомоморфизм полей инъективен автоматически), если $b\in K(\alpha)$, то $b=f(\alpha)(g(\alpha)^{-1}), g(\alpha)\neq 0$, и тогда $\psi\left(\frac{f(x)}{g(x)}\right)=f(\alpha)g(\alpha)^{-1}$. Итого, да, у нас сюръективный гомоморфизм, $K(x)\simeq K(\alpha)$. □

А теперь будет блок про конечные простые расширения.

Теорема 2.3. *Если K – это поле, а $q(x)\in K[x]$ это неприводимый многочлен.*

Тогда $E=K[x]/(q(x))$ есть конечное расширение поля K, и $E=K(\alpha), \alpha=x+(q(x))$. Более того, $[E:K]=\deg q(x)$ и $q(x)=\mathrm{Irr}(\alpha:K)$.

Доказательство этой теоремы было уже на курсе алгебры в четвертом модуле. Из этого утверждения следует, что любое поле можно расширить так, чтобы произвольный неприводимый многочлен имел в нем корень.

А теперь у нас первый раз будет в меню что-то интересное, чего не было в меню на курсе алгебры в четвертом модуле.

Теорема 2.4. *Пусть $K\subseteq E, \alpha\in E$ и α – алгебраический над K элемент, $q(x)=\mathrm{Irr}(\alpha:K)$. Тогда произвольный гомоморфизм полей $\psi: K\to L$ можно продолжить до гомоморфизма полей $\varphi: K(\alpha)\to L$ ровно столько раз, сколько различных корней у ${}^{\psi}q(x)$ в L, причем каждый такой гомоморфизм переправляет α в корень ${}^{\psi}q(x)$.*

Доказательство. Заранее отметим, что в силу алгебраичности $\alpha\in E$ над K, верно, что $K[\alpha]=K(\alpha)$

Пусть $\psi: K\to L$ произвольный гомоморфизм полей, а $\varphi: K(\alpha)\to L$ его продолжение. Покажем, что $\varphi(a)$ есть корень ${}^{\psi}q(x)$.

$${}^{\psi}q(\varphi(\alpha))=\sum_{k=0}^{n}\psi(a_k)\varphi(\alpha)^k=\sum_{k=0}^{n}\varphi(a_k)\varphi(\alpha)^k=\varphi\left(\sum_{k=0}^{n}a_k\alpha^k\right)=\varphi(q(\alpha))=0$$

Таким образом, любое продолжение ψ на $K(\alpha)$ переводит α в корень ${}^{\psi}q(x)$.

Теперь покажем, что для любого корня $\beta\in L$, ${}^{\psi}q()$ существует единственный гомоморфизм продолжающий ψ на $K(\alpha)$, такой что $\alpha\mapsto\beta$.

Для начала покажем существование, а затем объясним единственность.

Пусть $f(\alpha)\in K(\alpha)=K[\alpha]$ произвольный элемент $K[\alpha]$, тогда пусть потенциальный гомоморфизм φ переводит:

$$\varphi_\beta(f(\alpha))=\sum_{k=0}^{n}\psi(a_k)\beta^k={}^{\psi}f(\beta)$$

Для начала, покажем что такое определение корректно.

Если $f(\alpha)=g(\alpha)$, то $f(\alpha)-g(\alpha)=0$, а, следовательно, $f(x)-g(x)=q(x)l(x)$, тогда посмотрим, на ${}^{\psi}f(x)-{}^{\psi}g(x)={}^{\psi}\left(f(x)-g(x)\right)={}^{\psi}\left(q(x)l(x)\right)={}^{\psi}q(x)^{\psi}l(x)$

Тогда $\varphi_\beta(f(\alpha))-\varphi_\beta(g(\alpha))={}^{\psi}f(\beta)-{}^{\psi}g(\beta)={}^{\psi}q(\beta)^{\psi}l(\beta)=0$.

Наше отображение корректно, переводит одинаковые элементы в один и тот же элемент.

То что само отображение является гомоморфизмом следует из того, что:

${}^{\psi}1=1, {}^{\psi}(f(x)+g(x))={}^{\psi}f(x)+{}^{\psi}g(x), {}^{\psi}(f(x)g(x))={}^{\psi}f(x)^{\psi}g(x)$, подставляя β наши равенства не испортятся.

Таким образом, наше отображение φ_β, действительно является гомоморфизмом.

Единственность в свою очередь следует и того, что любое продолжение ψ переводящее α в β будет действовать ровно так, как действует φ_β в силу свойств гомоморфизма.

Итого, способов продлить $\psi: K\to L$ до $\varphi: K(\alpha)\to L$ существует ровно столько, сколько корней у ${}^{\psi}q(x)$ в L, причем каждый гомоморфизм продляющий ψ переводит α в корень ${}^{\psi}q(x)$, а для каждого корня существует свой единственный гомоморфизм. □

2.4 Алгебраические расширения полей

Определение 2.7. *Если E – расширение поля K, то оно называется алгебраическим расширением, если любой элемент E алгебраичен над K, иначе, наше расширение является трансцендентным.*

Поскольку этот класс расширений полей, достаточно часто встречается в нашей теории и обладает достаточно приятными свойствами, то изучим эти свойства.

Утверждение 2.5. *Любое конечное расширение $K \subseteq E$ является алгебраическим расширением.*

Доказательство. Если $[E : K] = n$, то для любого $\alpha \in E$ верно, что $1, \alpha, \ldots, \alpha^n$ линейно зависимы над K, тогда из соответствующих коэффициентов из нетрививальной и зануляющей линейной комбинации можно составить зануляющий многочлен. □

Утверждение 2.6. *Если $E = K(\alpha_1, \ldots, \alpha_n)$ и любой $\alpha_i \in E$ алгебраичен над K, то $K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$, E – конечное расширение K, а, следовательно, и алгебраическое.*

Доказательство. Проведем доказательство по индукции по n.

Случай $n = 1$ следует из теоремы 2.2.

Теперь переход, пускай для $k < n$ верно условие теоремы, покажем для n.

Для начала заметим, что $K(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$. Это связано с тем, что любую конечную линейную комбинацию степеней $\alpha_1, \ldots, \alpha_n$ с коэффициентами из K простой перегруппировкой слагаемых представить как линейную комбинацию степеней α_n с коэффициентами из $K[\alpha_1, \ldots, \alpha_{n-1}]$ и тогда принадлежит $K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$.

Теперь в другую сторону, отметим, что любой элемент $K(\alpha_1, \ldots, \alpha_{n-1})$ представим как линейная комбинация степеней $\alpha_1, \ldots, \alpha_{n-1}$ с коэффициентами из K в силу предположения индукции, тогда любая линейная комбинация степеней α_n с коэффициентами из $K(\alpha_1, \ldots, \alpha_{n-1})$ при помощи перегруппировки слагаемых, представима в виде линейной комбинации степеней $\alpha_1, \ldots, \alpha_n$ с коэффициентами из K, а следовательно эта линейная комбинация принадлежит $K(\alpha_1, \ldots, \alpha_n)$

Таким образом, верно равенство, сформулированное выше.

Также отдельно отметим, что из этого так же следует, что $K[a_1, \ldots, \alpha_n] = K[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n]$, и еще данные равенства верны и без алгебраичности, просто надо немного повозиться со знаменателями коэффициентов из $K(\alpha_1, \ldots, \alpha_{n-1})$ и все получится.

Теперь мы знаем, что элемент $\alpha_n \in E$, алгебраичен над K, а следовательно алгебраичен и над $K[\alpha_1, \ldots, \alpha_{n-1}]$, и тогда, во-первых, $K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_{n-1}](\alpha_n) = K[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n] = K[\alpha_1, \ldots, \alpha_{n-1}, \alpha_n]$,
во-вторых, $[K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})] = \deg \operatorname{Irr}(\alpha_n, K(\alpha_1, \ldots, \alpha_{n-1})) < \infty$.

Тогда так же верно, что $[K(\alpha_1, \ldots, \alpha_{n-1}) : K] < \infty$ по предположению индукции.

Тогда $[K(\alpha_1, \ldots, \alpha_n) : K] = [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})] \cdot [K(\alpha_1, \ldots, \alpha_{n-1}) : K] < \infty$, что и хотелось доказать.

□

Утверждение 2.7. *Если E некоторое расширение поля K, и S некоторое подмножество E, состоящее из алгебраических над K элементов, то $K(S)$ это алгебраическое расширение поля K.*

Доказательство. По следствию 1.3.1 верно, что $\alpha \in K(S) \Leftrightarrow \alpha \in K(\alpha_1, \ldots, \alpha_n), \alpha_i \in S$, но тогда по 2.6 $K(\alpha_1, \ldots, \alpha_n)$ – алгебраическое расширение K, а следовательно α алгебраично над K.

□

Утверждение 2.8. *Если $K \subseteq F \subseteq E$ поля и E – алгебраично над K, то F алгебраично над K и E алгебраично над F.*

Доказательство. Предлагаю внимательно приглядеться в утверждение. □

Утверждение 2.9. *Если $K \subseteq F \subseteq E$ поля, F алгебраично над K, и E алгебраично над F, то E алгебраично над K.*

Доказательство. Пусть $\alpha \in E$, тогда в силу, того, что E алгебраично над F, то существует $f(x) \in F[x]$, что $f(\alpha) = 0$, тогда $f(x) = \sum_{k=0}^{n} a_k x^k, a_i \in F$, тогда посмотрим на $F' = K(a_0, \ldots, a_n)$, так как F алгебраично над K, то F' – это конечное расширение K по утверждению 2.6.

Теперь α алгебраично над F', так как $f(x) \in F'[x]$, тогда известно $[F'(\alpha) : F'] = \deg \operatorname{Irr}(\alpha, F') < \infty$, Тогда $[F'(\alpha) : K] = [F'(\alpha) : F'] \cdot [F' : K] < \infty$, тогда $F'(\alpha)$ алгебраическое расширение K и α алгебраично над K. □

Утверждение 2.10. *Если E – алгебраическое расширение K и существует композиция EF, то EF это алгебраическое расширение KF.*

Доказательство. Для начала отметим, что KF существует и является подполем EF, так как K и F являются подполями EF.

Теперь $\alpha \in EF$, тогда из утверждения 1.4, $\alpha = ab^{-1}$, где a и b имеют вид: $\sum_{k=1}^{n} \left(\prod_{i=1}^{n_k} \alpha_i\right), \alpha_i \in E \cup F$, тогда $\alpha \in KF(\alpha_1, \ldots, \alpha_m) = H$, где α_i это элементы из произведений в разложении, принадлежащие E, в силу, того, что $\alpha_i \in E$ алгебраично над K, то оно алгебраично и над KF, а, следовательно, H это конечное и алгебраическое расширение KF, тогда $\alpha \in H$, алгебраично над KF.

□

Утверждение 2.11. *Любая композиция алгебраических расширений K является алгебраическим расширением K.*

Доказательство. Это следует из того, что по 1.4 любой член α композиции будет конечной суммой, конечных произведений алгебраических над K элементов, и тогда он принадлежит некоторому алгебраическому над K расширению $K(\alpha_1, \ldots, \alpha_n)$, для некоторых α_i, принадлежащих разложению элементу и алгебраичных над K, тогда и α алгебраично над K. □

Теперь некоторые предложения, небольшие, но приятные свойства, вытекающие из этого.

Предложение 2.12. *Если E - конечное расширение K и композиция EF существует, то EF – конечно над KF. Следовательно, композиция конечного числа конечных расширений K есть конечное расширение K.*

Доказательство. Начнем с доказательства первой части.

Пусть $e_1, \ldots, e_n$ – базис E над K, тогда покажем, что $EF = KF(e_1, \ldots, e_n)$.

Вложенность $\supset$ следует из того, что $KF \subset EF$ и $e_i \in E \subset EF$.

Вложенность в другую сторону, из того, что $x \in EF$, следует, что: $x = \sum_{k=1}^{m} \left(\prod_{i=1}^{m_k} \alpha_i\right), \alpha_i \in E \cup F$, тогда сгруппировав в каждом слагаемом элементы из F в единый коэффициент и элементы из E в единый коэффициент, можно представить x в виде $x = \sum_{k=1}^{m} a_k \beta_j = \sum_{k=1}^{m} a_k \left(\sum_{i=1}^{n} \gamma_{ki} e_i\right) = \sum_{i=1}^{n} b_i e_i, a_i \in F, \beta_j \in E, \gamma_i \in K, b_i \in KF$, тут я расписал β_j по базису E над K, а затем раскрыл скобки по дистрибутивности и перегруппировал слагаемые, итого получил линейную комбинацию e_i, с коэффициентами из KF, а следовательно $x \in KF(e_1, \ldots, e_n)$, а следовательно, доказано равенство $EF = KF(e_1, \ldots, e_n)$.

Теперь все $e_i \in E$ алгебраичны над K, а следовательно и над KF, а следовательно, $EF = KF(e_1, \ldots, e_n)$ это конечное расширение KF.

Теперь вторая часть утверждения доказывается по индукции по n, с использованием первой.

Собственно при $n = 1$ нечего доказывать.

Теперь пусть утверждение верно при $n-1$, покажем при n, из 1.5 мы знаем, что $F_1 \ldots F_n = (F_1 \ldots F_{n-1})F_n$, F_i – конечные расширения K, тогда по предположению индукции, $(F_1 \ldots F_{n-1})$ это конечное расширение K, тогда по первому пункту нашего предложения, верно, что $(F_1 \ldots F_{n-1})F_n$ это конечное расширение KF_n, а оно в свою очередь опять же по первому пункту, конечное раширение $KK = K$, тогда по формуле о размерности расширения и размерности промежуточного подполя, верно, что $(F_1 \ldots F_{n-1})F_n$ это конечное расширение K, что мы и хотели доказать.

□

Предложение 2.13. *Если $E \supseteq K$ поля, то тогда множество всех алгебраических над K элементов E образует алгебраическое над K подполе E.*

Доказательство. $F = \{\alpha \in E | \exists f(x) \in K[x], f(\alpha) = 0\}$, множество всех алгебраических над K элементов

Для начала $1, 0 \in K$, и поэтому они алгебраичны над K, а, следовательно, принадлежат F, теперь, пусть $\alpha, \beta \in F, \beta \neq 0$, тогда $K(\alpha, \beta) \subset E$, есть конечное расширение K по 2.6, но тогда $K(\alpha, \beta) \subset F$, а, следовательно, $\alpha - \beta,\ \alpha\beta^{-1} \in K(\alpha, \beta) \subset F$. □

3 Алгебраическое замыкание

Я напомню, что во всем в этом тексте верим в аксиому выбора, а следовательно и в эквивалентную ей лемму Цорна.

Лемма 3.1 (Лемма Цорна)**.** *Непустое частично упорядоченное множество, в котором любая непустое цепь имеет верхнюю грань, содержит максимальный элемент.*

3.1 Максимальный идеал

Определение 3.1. *Максимальный левосторонний (правосторонний, двусторонний) идеал в кольце R, это такой идеал M, что не существует левостороннего (правостороннего, двустороннего) идеала I, что $M \subsetneq I \subsetneq R$.*

Утверждение 3.2. *В любом ненулевом (возможно некоммутативном) кольце с единицей R существует левосторонний (правосторонний, двусторонний) идеал.*

Доказательство. Докажем для левостороннего идеала, для остальных аналогично.

Для начала известно для левостороннего идеала I, что $1 \in I \Leftrightarrow I = R$.

Введем на множестве U всех идеалов не равных R частичный порядок по включению идеалов. Так как $1 \neq 0$ в нашем случае, $\{0\} \in U \Rightarrow U \neq \emptyset$.

Напомню, что цепью называется линейно-упорядоченное подмножество исходного частичного порядка. Пусть $(I_i)_{i\in J} \subset U$ это некоторая непустая цепь из идеалов, не равных R. Тогда покажем, что $I = \bigcup_{i\in J} I_i$ это идеал в R, причем не равный R.

Начнем с того, что это идеал. $u, v \in I \Rightarrow u \in I_i, v \in I_j, i, j \in J$, тогда будем считать без потери общности, что $I_j \subset I_i$, тогда $u - v \in I_i \subset I$, и тогда I – абелева группа по сложению.

Так же если $r \in R, u \in I$, то $u \in I_j, ru \in I_j \subset I$, так как I_j – идеал.

Теперь I – идеал, причем так как $\forall i \in J : 1 \notin I_i$, тогда $1 \notin I$ и $I \neq R$, а следовательно $I \in U$, и по понятным причинам является верхней гранью $(I_i)_{i\in J}$.

Тогда по лемме Цорна имеется максимальный элемент $M \in U$, то есть чисто по определению, такой идеал, что не существует идеала $I \subset R$, что $M \subsetneq I \subsetneq R$. □

Утверждение 3.3. *Для любого коммутативного, ассоциативного кольца с единицей идеал $I \subset R$ является максимальным тогда и только тогда R/I – поле.*

Доказательство. $\Rightarrow$

Пусть $a \notin I$, тогда идеал $(a, I) = \{ra + v \mid r \in R, v \in I\} \supsetneq I$, и тогда в силу максимальности $1 \in (a, I), 1 = r'a + v'$, тогда $(a + I)(r' + I) = r'a + I = 1 - v' + I = 1 + I$. Хорошо, все ненулевые элементы обратимы, а так как $1 \notin I$, то $1 + I \neq 0 + I$, и тогда у нас действительно факторкольцо является полем.

$\Leftarrow$

Пусть R/I это поле, тогда пусть $J \supsetneq I$, некоторый идеал, содержащий в себе I, и $a \in J\backslash I$, тогда существует $(r+I)$ что $(a+I)(r+I) = 1+I$, тогда $ra+u = 1, u \in I$, следовательно $1 \in (a, I) \subset J$, а следовательно, $(a, I) = R$, и тогда $J = R$, так как любой идеал не равный I и содержащий I равен R, то I – максимальный идеал.

□

Утверждение 3.4. *Любой собственный идеал $I \subseteq R$ содержится в некотором максимальном идеале M.*

Доказательство. Доказательство практически аналогично тому, что было в 3.2, только надо рассмотреть множество собственных идеалов, содержащих I.

В конце из леммы Цорна мы получим некоторый идеал M, если он не является макисмальным идеалом в R, то существует идеал J, что $I \subset M \subsetneq J \subsetneq R$, но тогда J больше, чем M в упорядоченном множестве собственных идеалов содержащих I, что дает противоречие.

□

3.2 Определение эквивалентного замыкания

Утверждение 3.5. *Для поля K следующие утверждения эквивалентны:*

1. *Единственное алгебраическое расширение K это само K.*
2. *В $K[x]$ любой неприводимый многочлен имеет степень 1.*
3. *У любого неконстантного полинома в $K[x]$ есть корень в K.*

Доказательство. $1 \Rightarrow 2$

Если $q(x)$ – неприводимый многочлен, что $K[x]/(q(x)) = E$ это расширение K, тогда в силу условия 1 и 2.3: $1 = [E : K] = \deg q(x)$.

$2 \Rightarrow 3$

Из курса алгебры мы знаем, что любой многочлен единственным образом раскладывается на неприводимые множители с точностью до умножения на какое-то ненулевое число. (Вообще говоря в любом кольце главных идеалов без делителей нуля раскладывается на простые элементы с точностью до умножения на обратимый элемент кольца, но об этом надо говорить отдельно).

Тогда $f(x) = ag_1(x)\dots g_m(x)$, где $f(x) \in K[x]$ – неконстантный многочлен, $a \in K$, $g_i(x) \in K[x]$ неприводимый многочлен. Теперь из неприводимости $g_1(x)$ и условия 2, следует, что $g_1(x) = x - b \in K[x]$, и тогда $f(b) = 0$ и тогда у $f(x)$ есть корень в K.

$3 \Rightarrow 2$

Банально следует из того, что если $f(a) = 0$, то $f(x) = (x-a)g(x), \deg g(x) < \deg f(x)$

$2 \Rightarrow 1$

Пусть E какое-то алгебраическое расширение K, тогда $\alpha \in E$, $\mathrm{Irr}(\alpha : K) = q(x)$ неприводим, а следовательно имеет степень 1, тогда $q(x) = x - b, \alpha - b = 0 \Rightarrow \alpha = b$. □

Определение 3.2. *Поле K является алгебраически замкнутым, если выполнено одно из эквивалентных условий из 3.5.*

3.3 Существование алгебраически замкнутого поля

Теорема 3.6 (Теорема о продолжении гомоморфизма.)**.** *Любой гомоморфизм из поля K в алгебраически замкнутое поле L, может быть продолжен до гомоморфизма из E в L для произвольного алгебраического расширения $E \supset K$.*

Доказательство. Пусть $\varphi : K \to L$ какой-то гомоморфизм.

Для начала отметим, что если у нас простое расширение $K(\alpha)$, где α алгебраический над K элемент, то тогда по конструкции из 2.4 существует продолжение φ на $K(\alpha)$, так как $^{\varphi}(\mathrm{Irr}(\alpha : K))$ точно имеет корень в силу алгебраической замкнутости L.

Теперь перейдем к случаю с произвольным расширением $E \supset K$.

Пусть $\mathcal{S}$ это совокупность всех пар (F, ψ), где F это промежуточное поле между $K \subset F \subset E$, а $\psi : F \to L$ это продолжение φ на F.

Введем частичный порядок на этом множестве.

$$(F, \psi) \leq (P, \chi) \Leftrightarrow F \subseteq P \text{ и } \chi\text{– продолжение } \psi \text{ на } P$$

Нетрудно убедиться, что это отношение рефлексивно, симметрично и транзитивно.

Поэтому, чтобы перейти к лемме Цорна, заметим, что $(K, \varphi) \in \mathcal{S} \Rightarrow \mathcal{S} \neq \emptyset$, тогда пусть $(F_i, \psi_i)_{i\in I}$, это некоторая непустая цепь из $\mathcal{S}$.

Следовательно, $F = \bigcup_{i\in I} F_i \subset E$, это поле по 1.2, причем оно является алгебраическим расширением K, так как каждый элемент принадлежит какому-то K_i, алгебраическому над K полю.

Теперь построим ψ так, если $v \in F \Rightarrow v \in F_i$, тогда $\psi(v) = \psi_i(v)$, заметим, что это корректное построение отображения, так как если $v \in F_i$ и $v \in F_j$, то без потери общности, можно считать, что $(F_j, \psi_j) \leq (F_i, \psi_i)$, и тогда ψ_i это продолжение ψ_j, а следовательно $\psi_i(v) = \psi_j(v)$.

Это гомоморфизм, так как $1 \in F_i$, тогда $\psi(1) = \psi_i(1) = 1$,

Если $v, u \in F$, то будем считать, что $v \in F_j \subset F_i, u \in F_i$, тогда $\psi(v+u) = \psi_i(v+u) = \psi_i(v) + \psi_i(u) = \psi(v) + \psi(u)$, и аналогично с умножением.

Также ψ продолжает φ, так как любой ψ_i продолжает φ.

Итого, $(F, \psi) \in \mathcal{S}$ и является верхней гранью для цепи $(F_i, \psi_i)_{i\in I}$, по построению.

Таким образом, по лемме Цорна в $\mathcal{S}$ существует максимальный элемент (M, χ). Покажем, что $M = E$, предположим противное, тогда $\alpha \in E\backslash M$, и тогда $M(\alpha)$ является алгебраическим расширением M, так как E – алгебраическое расширение K, тогда гомоморфизм χ имеет продолжение $\chi_\alpha : M(\alpha) \to L$ по примеру с простым алгебраическим расширением в начале, тогда χ_α является продолжением φ, так как таковым является φ. В свою очередь, $K \subset M \subsetneq M(\alpha) \subset E$, тогда $M(\alpha)$ – алгебраическое расширение K, и $(M(\alpha), \chi_\alpha) \in \mathcal{S}$ и $(M(\alpha), \chi_\alpha) > (M, \chi)$ по введенному нами порядку, что противоречит тому, что (M, χ)– максимальный элемент $\mathcal{S}$.

Итого, $M = E$, а χ является продолжением φ на E. □

Теперь опишем с одной стороны, неприятный, но с другой стороны, по-своему инженерный способ алгебраически расширить поле так, чтобы в расширении любой неконстантный многочлен из исходного поля имел корень.

Лемма 3.7. *Для любого поля K существует алгебраическое расширение, такое, что в нем любой неконстантный многочлен из $K[x]$ имеет корень.*

Доказательство. Пусть U – множество всех неконстантных многочленов из $K[x]$. Отождествим с каждым элементом $f \in U$ свою формальную переменную x_f и рассмотрим кольцо многочленов $K[(x_f)_{f\in U}]$.

Докажем от противного, что идеал I порожденный всеми многочленами вида $f(x_f)$ является собственным.

Действительно, пусть идеал совпадает со всем кольцом, тогда $1 \in I$, тогда $1 = \sum_{k=1}^{n} f_k(x_{f_k})q_k(x_{k1}, \ldots, x_{kn_k})$, такое разложение гарантировано существует из определения порожденного идеала.

Пусть E это такое конечное алгебраическое расширение K, что многочлены $f_1(x), \ldots, f_n(x)$ имеют корни в E, и пусть α_i – корень $f_i(x)$.

Теперь рассмотрим K-гомоморфизм-подставновку $\varphi : K[(x_f)_{f\in U}] \to E$, такой, оно переводит x_{f_k} в α_k, если f_k участвует в разложении 1, иначе $x_g \mapsto 0$, тогда $1 = \varphi(1) = \varphi\left(\sum_{k=1}^{n} f_k(x_{f_k})q_k(x_{k1}, \ldots, x_{kn_k})\right) = 0$, тогда в поле $E, 1 = 0$, что невозможно из аксиом поля, противоречие.

Тогда идеал I является собственным, а, следовательно, по 3.4 содержится в некотором максимальном идеале M.

Теперь рассмотрим факторкольцо $E = K[(x_f)_{f\in U}]/M$ по утверждению 3.3 оно является полем.

Тогда существует гомоморфизм полей $\psi : K \to K[(x_f)_{f\in U}]/M, \quad k \mapsto k + M$, а следовательно, можно считать , что E является расширением K, а для еще большего удобства, можно отождествить, $k \in K$ и $k + M$ и сказать, что $\alpha_f = x_f + M$, тогда с этим переименованием (фактически, теперь мы в новом поле называем полем K множество смежных классов элементов из K по M) можно сказать, что $E = K[(\alpha_f)_{f\in U}]$.

Теперь если $f(x) \in K[x]$ неконстантный многочлен, то в поле E $f(\alpha_f) \in I \subset M \Rightarrow f(\alpha_f) = 0$.

Также верно, что любой α_f зануляется соответствующим ему многочленом, тогда, все элементы $\alpha_f \in E$ алгебраичны над K, а следовательно по утверждению 2.7 E является алгебраическим расширением K.

□

Теорема 3.8. *У любого поля K существует алгебраическое расширение $\overline{K}$, которое является алгебраически замкнутым. Более того, $\overline{K}$ единственно с точностью до K-изоморфизма.*

Доказательство. Рассмотрим такую башню расширений:

$$K = E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots \subseteq E_n \subseteq \ldots$$

Такую, что по лемме выше в E_{k+1} есть корни для всех неконстантных многочленов из $E_k[x]$.

Заметим, что по индукции, используя 2.9 можно запросто доказать, что любой E_k это алгебраическое расширение K.

Теперь рассмотрим $E = \bigcup_{i=0}^{\infty} E_i$ по 1.2 это является полем, причем оно является, во-первых, расширением K, причем алгебраическим, любой $\alpha \in E$, принадлежит какому-то E_n, а это поле уже является алгебраическим расширением K, тогда и $\alpha \in E_n$ алгебраический над K элемент.

Так же любой неконстантный многочлен в E имеет корень, действительно, если $f(x) \in E[x]$, то все коэффициенты лежат в каком-то E_n (так как всего коэффициентов конечное количество), и тогда у $f(x)$ есть корень $\beta \in E_{n+1} \subset E$, а следовательно поле E является алгебраически замкнутым алгебраическим расширением K, отныне назовем его $\overline{K}$.

Теперь покажем вторую часть утверждения про K-изоморфность.

Пусть L это некоторое алгебраическое расширение K, которое является алгебраически замкнутым. Тогда существует гомоморфизм включение $\mathrm{id} : K \to L$, и по 3.6 в силу алгебраичности $\overline{K}$, можно продолжить до гомоморфизма $\varphi : \overline{K} \to L$.

Теперь $\overline{K} \simeq \mathrm{Im}(\varphi)$, причем изоморфны над K. Причем, несложно заметить, что $\mathrm{Im}(\varphi)$ это алгебраически замкнутое поле, так как если $f(x) \in \mathrm{Im}(\varphi)[x]$, то можно посмотреть на ${}^{\varphi^{-1}}f(x) \in \overline{K}[x]$, у у этого многочлена есть корень $\alpha \in \overline{K}$, тогда несложно убедиться, что $\varphi(\alpha)$ это корень $f(x)$, $f(\varphi(\alpha)) = \varphi\left({}^{\varphi^{-1}}f(\alpha)\right) = 0$,

Тогда $K \subset \mathrm{Im}(\varphi) \subset L$, и тогда L это алгебраическое расширение $\mathrm{Im}(\varphi)$, но в силу 3.5, верно, что $\mathrm{Im}(\varphi) = L$, и тогда $\overline{K}$ K-изоморфно L. □

Теперь собственно введем определение алгебраического замыкания поля.

Определение 3.3. *Поле $\overline{K}$ является алгебраическим замыканием полем K, если оно является алгебраическим расширением поля K и является алгебраически замкнутым полем.*

Но из вышеописанных достаточно содержательных теорем можно вывести следующие эквивалентные определения $\overline{K}$ – алгебраического замыкания K.

Утверждение 3.9. *Для поля $K \subset \overline{K}$ следующее эквивалентно:*

1. *$\overline{K}$ это алгебраически замкнутое алгебраическое расширение K.*
2. *$\overline{K}$ это максимальное алгебраическое расширение K, то есть, если $\overline{K} \subset E$ и E алгебраическое расширение K, то $E = \overline{K}$.*
3. *$\overline{K}$ это, с точностью до K-изоморфизма, наибольшее алгебраическое расширение K, то есть любое алгебраическое расширение K K-изоморфно какому-то подполю $\overline{K}$.*
4. *$\overline{K}$ это минимальное алгебраически замкнутое расширение K, то есть если $K \subset L \subset \overline{K}$ и L – алгебраически замкнуто, то $L = \overline{K}$.*
5. *$\overline{K}$, с точностью до K-изоморфизма, является наименьшим алгебраически замкнутым расширением K, то есть если L – алгебраически замкнутое расширение K, то $\overline{K}$ K-изоморфно подполю L.*

Доказательство. На всякий случай, покажем, что это все эквивалетно.

$1 \Leftrightarrow 2$ сразу следует из 3.5.

$1 \Rightarrow 3$ следует из продолжения гомоморфизма в алгебраически замкнутое поле.

$3 \Rightarrow 1$ Пусть F это некоторое произвольное алгебраически замкнутое алгебраическое расширение K (оно существует по теореме выше), тогда F – K-изоморфно подполю $H \subset \overline{K}$, которое является (как я показал в теореме выше), алгебраически замкнутым алгебраическим расширением K и $\overline{K}$ это алгебраическое расширение H, тогда в силу алгебраической замкнутости $\overline{K} = H$ и $\overline{K}$ алгебраически замкнуто.

$1 \Rightarrow 4$

Из того, что $\overline{K}$ это алгебраическое расширение K, следует, что любое алгебраически замкнутое промежуточное поле равно $\overline{K}$, это следует, из того, что $\overline{K}$ будет алгебраическим расширением промежуточного поля и из 3.5.

$4 \Rightarrow 1$

Покажем, что $\overline{K}$ это алгебраическое расширение K.

Пусть U это подполе (по 2.13) $\overline{K}$ содержащее в себе все алгебраические над K элементы (оно включает в себя K по понятным причинам).

Покажем, что U – алгебраически замкнутое поле. $f(x) = \sum_{k=1}^{n} a_k x^k \in U[x]$, у него есть корень $\alpha \in \overline{K}$ по условию 4.

Тогда $U' = K(a_0, \ldots, a_n)$ это конечное расширение K, а α это алгебраический над U' элемент, следовательно $U'(\alpha)$ это конечное расширение U', а следовательно и конечное расширение K, тогда α это алгебраический над K элемент, следовательно $\alpha \in U$, и тогда U это алгебраически замкнутое поле.

Опять же из 4 следует, что $U = \overline{K}$, а, следовательно, $\overline{K}$ это алгебраическое расширение K.

$1 \Rightarrow 5$

Следует из того, что $\overline{K}$ это алгебраическое расширение K и 3.6.

$5 \Rightarrow 1$

$\overline{K}$ уже алгебраически замкнуто.

Надо рассмотреть опять же $U \subset \overline{K}$ – подполе алгебраических над K элементов. Оно является алгебраически замкнутым, тогда по условию 5 $\overline{K}$ K-изоморфно подполю $H \subset U$ (пусть K-гомоморфизм это ψ), тогда в силу того, что у нас K-изоморфизм, то $K \subset H \subset U$, тогда H– алебраическое расширение U, тогда для любого $\alpha \in \overline{K}$, существует $f(x) \in K[x]$, что $f(\psi(\alpha)) = 0$, так как у нас инъективный K-гомоморфизм, то $f(\psi(\alpha)) = \psi(f(\alpha)) = 0 \Rightarrow f(\alpha) = 0$, и тогда $\alpha \in U$, тогда $\overline{K} = U$, следовательно $\overline{K}$ – алгебраическое расширение U.

□

Итого, благодаря утверждению 3 из эквивалентности выше, для изучения всех алгебраических расширений K, достаточно изучить все промежуточные поля $K \subset E \subset \overline{K}$.

Так же верно, что:

Следствие 3.9.1. *Для любого алгебраического расширения E поля K, верно, что $\overline{E}$ это алгебраическое замыкание K. Также для любого алгебраического замыкания $\overline{K}$ верно, что E K-изоморфно промежуточному полю $K \subseteq F \subseteq \overline{K}$.*

Первая часть следствия следует из 2.9 и 3.9.

Вторая часть из продолжения гомоморфизма или того, что все алгебраические замыкания K K-изоморфны.

Также добавим еще несколько интересных и достаточно очевидных, из того, что я расписал выше свойств.

Предложение 3.10. *Любой K-эндоморфизм $\overline{K}$ есть K-автоморфизм.*

Предложение 3.11. *Если $K \subset E \subset \overline{K}$ и $\varphi : E \to \overline{K}$ K-гомоморфизм, то φ продолжается до K-автоморфизма $\overline{K}$.*

4 Сепарабельные расширения

4.1 Сепарабельный многочлен

Пусть K это произвольное поле, а $f(x) \in K[x]$ это проивзольный неконстантный многочлен. Тогда в $\overline{K}[x]$ верно, что многочлен $f(x)$ раскладывается единственным образом на произведение многочленов степени 1, то есть

$$f(x) = a(x-\alpha_1)^{m_1} \dots (x-\alpha_n)^{m_n}$$

Где $a \in K$, это старший коэффициент $f(x)$, $\alpha_i \in \overline{K}, m_i \geq 1$. Заметим, что a и m_i не зависят от выбора алгебраического замыкания, так как все замыкания алгебраические замыкания K-изоморфны и существует гомоморфизм многочленов $f \mapsto {}^{\varphi}f$ описанный в самом начале конспекта. Вспомним, что корень многочлена называется кратным, если соответствующий ему $m_i > 1$.

Теперь введем понятие сепарабельного многочлена.

Определение 4.1. *Многочлен $f(x) \in K[x]$ является сепарабельным, если он неконстантный и у него нет кратных корней в $\overline{K}$.*

Для примера $f(x) = x^2+2x+1 = (x+1)^2 \in \mathbb{R}[x]$ не является сепарабельным, а $x^2-4 = (x+2)(x-2) \in \mathbb{R}[x]$ является таковым.

Давайте попробуем понять, как выглядят неприводимые многочлены в поле, с точки зрения сепарабельности.

Утверждение 4.1. *Пусть K это поле и $q(x) \in K[x]$ это некоторый неприводимый многочлен над K.*

1. *Если $\mathrm{char}K = 0$, то $q(x)$ это сепарабельный многочлен.*
2. *Если $\mathrm{char}K = p > 0$, то $q(x) = g(x^{p^m})$ для некоторого неприводимого и сепарабельного многочлена $g(x)$ и все корни $q(x)$ имеют одинаковую кратность p^m.*

Доказательство. Для начала сделаем ремарку, о том, что в поле характеристики p, верно, что $a \mapsto a^p$ является гомоморфизмом, так как любой $\binom{p}{k} = 1$, если $k = 0, p$, иначе $\binom{p}{k} = 0$.

Будем считать, что многочлен $q(x)$ приведенный, так мы всегда можем вынести старший коэффициент и представить $q(x) = a\widetilde{q}(x)$, где $\widetilde{q}(x)$ приведенный многочлен. Это никак не влияет на разложение $q(x)$ оно совпадает с разложением $\widetilde{q}(x)$ с точностью до начального коэффициента.

Теперь пусть $\alpha \in \overline{K}$ это кратный корень $q(x) = \sum_{k=0}^{n} a_k x^k, a_n = 1, n > 1$. Тогда мы знаем, что $q'(\alpha) = 0$, где $q'(x) = \sum_{k=1}^{n}(k \cdot a_k)x^{k-1}$ это формальная производная многочлена $q(x)$. Тогда в силу того, что $q(x)$ неприводим и приведен, то $q(x) = \mathrm{Irr}(\alpha : K)$, и тогда $q(x) | q'(x)$, но из того, что $\deg q'(x) < \deg q(x)$ следует, что $q'(x) = 0$.

Если $\mathrm{char}K = 0$, то $nx^{n-1} \neq 0$, тогда $q'(x) \neq 0$, противоречие, не может быть неприводимого и несепарабельного многочлена.

Теперь посмотрим на поле положительной характеристики.

$q'(x) = \sum_{k=1}^{n}(k \cdot a_k)x^{k-1} = 0$, тогда $k \cdot a_k = 0$ для любого $k > 0$, если $p \nmid k$, то $a_k = 0$, иначе a_k может быть любым, так как его занулит k. итого в $q(x)$ ненулевыми могут быть коэффициенты при степенях кратных p, тогда $q(x) = \sum_{k=0}^{l} a_{pk}x^{pk} = \sum_{k=0}^{l} a_{pk}(x^p)^k, a_{pl} = 1$, и тогда $s(x) = \sum_{k=0}^{l} a_{pk}x^k \in K[x]$ и $q(x) = s(x^p)$, где $s(x)$ это неприводимый и приведенный (за эти 2 термина на русском, надо придушить их создателей) многочлен. Действительно, приведенность напрямую наследуется от $q(x)$, а если $s(x)$ приводимый многочлен, то из условия $q(x) = s(x^p)$ следует, что и $q(x)$ приводимый, но он неприводим.

Если $s(x)$ несепарабельный многочлен, то можно повторить процедуру выше и получить, что $u(x^p) = s(x), u(x^{p^2}) = s(x^p) = q(x)$, тогда так как $p > 1$, то $\deg u(x) < \deg s(x) < \deg q(x)$, и эта цепочка не может быть бесконечной, следовательно, $q(x) = g(x^{p^m})$ для некоторого сепарабельного многочлена $g(x) \in K[x]$.

Тогда $g(x) = (x-\beta_1)\dots(x-\beta_n), \beta_i \in \overline{K}$, так как $\overline{K}$ это алгебраически замкнутое поле, то у каждого β_i есть корень α_i степени p^m, то есть $\alpha_i^{p^m} = \beta_i$ и $\alpha_i = \alpha_j \Leftrightarrow i = j$, тогда:

$$q(x) = g(x^{p^m}) = (x^{p^m} - \beta_1)\dots(x^{p^m} - \beta_n) = (x^{p^m} - \alpha_1^{p^m})\dots(x^{p^m} - \alpha_n^{p^m}) = (x - \alpha_1)^{p^m}\dots(x - \alpha_n)^{p^m}$$

Последнее равенство верно опять же из того, что в поле характеристики p, $a^p - b^p = (a - b)^p$.

Тогда из единственности разложения многочлена на неприводимые множители в кольце многочленов, следует, что в $q(x)$ все корни имеют одну и ту же кратность, а именно p^m. □

И еще добавим очевидную, но достаточно полезную лемму.

Лемма 4.2. *Если $f(x) \in K[x]$ это сепарабельный многочлен, то любой неконстнантный делитель $f(x)$ является сепарабельным многочленом.*

Доказательство. Если $f(x) = q(x)u(x), \deg q(x) > 0$, то тогда из единственности разложения на множители в $\overline{K}[x]$, следует, что в $q(x)$ тоже нет кратных корней (иначе был бы и в $f(x)$), тогда $q(x)$ – сепарабельный многочлен. □

4.2 Степень сепарабельности

Определение 4.2. *Степень сепарабельности $[E : K]_s$ алгебраического расширения $K \subset E$ есть количество K-гомоморфизмов из E в $\overline{K}$.*

Отдельно отметим, что степень сепарабельности не зависит от выбора алгебраического замыкания K, так как пусть L, U – алгебраические замыкания K, по 3.8 они K-изоморфны, и пусть $\sigma : L \to U$ это K-изоморфизм. Тогда умножение слева на σ переводит любой K-гомоморфизм из E в L, в K-гомоморфизм из E в U, а умножение на σ^{-1} слева является обратной функцией для умножения на σ, тогда умножение слева на σ является биекцией между множеством K-гомоморфизмов из E в L и K-гомоморфизмами из E в U.

Множество K-гомоморфизмов из E в $\overline{K}$ непусто по 3.6.

Теперь перейдем к описанию степени сепарабельности для простых алгебраических расширений.

Утверждение 4.3. *Если α это некоторый алгебраический элемент над K из какого-то расширения K, то тогда $[K(\alpha) : K]_s$ это количество различных корней $\mathrm{Irr}(\alpha : K)$ в $\overline{K}$. Тогда $[K(\alpha) : K]_s = [K(\alpha) : K]$, если характеристика K равна 0, если же она равна $p > 0$, то $[K(\alpha) : K] = p^m[K(\alpha) : K]_s, m \geq 0$ и $[K(\alpha) : K]_s \Leftrightarrow \mathrm{Irr}(\alpha : K)$ – сепарабельный многочлен.*

Это утверждение автоматически следует из 2.4 и 4.1.

Теперь покажем, что степень сепарабельности обладает тем же приятным свойством, что и алгебраические расширения и промежуточные подполя.

Утверждение 4.4. *Если F – алгебраическое расширение K и $[F : K]_s < \infty$, то для $K \subset E \subset F$ верно, что $[F : K]_s = [F : E]_s \cdot [E : K]_s$.*

Доказательство. Для начала скажем, что из конечности $[F : K]_s$ следует конечность $[F : E]_s$ и конечность $[E : K]_s$. Действительно, для начала выберем замыкания, такие, что $\overline{E} = \overline{K}$, так можно из 3.9.1.

Если $[F : E]_s = \infty$, то у нас уже бесконечно K-гомоморфизмов, из F в $\overline{K} = \overline{E}$.

Если $[E : K]_s = \infty$, то любой K-гомоморфизм из E, можно продлить до K-гомоморфизма из F, и вот уже бесконечность K-гомоморфизмов из F в $\overline{K}$.

Тогда мы доказали, что $[F : E]_s, [E : K]_s < \infty$.

Теперь перейдем к доказательству исходного утверждения.

Покажем, что существует ровно $[F : E]_s$ способов продлить продлить произвольный K-гомоморфизм $\varphi : E \to \overline{K} = \overline{E}$ до K-гомоморфизма из F в $\overline{K}$

Для начала по 3.6 можно продлить φ до $\sigma : \overline{K} \to \overline{K}$, K-автоморфизма $\overline{K}$ (по 3.10), продолжающего φ.

Теперь пусть $\mathfrak{K}$ – это множество E-гомоморфизмов из F в $\overline{K} = \overline{E}$, а $\mathfrak{U}$ это множество K-гомоморфизмов из F в $\overline{K}$, продолжающих φ, заметим, что $|\mathfrak{K}| = [F : E]_s$ по определению.

Теперь пусть $\psi \in \mathfrak{K}$, покажем, что $\sigma\psi$ продолжает φ (напомню, что композиция гомоморфизмов есть гомоморфизм), если $u \in E$, то $\sigma(\psi(v)) = \sigma(v) = \varphi(v)$, первое равенство верно, так как ψ это E-гомоморфизм, а второе верно, так как σ продолжает φ.

Теперь если $\tau \in \mathfrak{U}$, то покажем, что $\sigma^{-1}\tau$ это E-гомоморфизм, пусть $u \in E$, тогда $\sigma^{-1}(\tau(u)) = \sigma^{-1}(\varphi(u)) = \sigma^{-1}(\sigma(u)) = u$. Первые 2 равенства верны, так как ограничения σ, τ на E есть φ по определению.

Тогда функция $\Phi : \mathfrak{K} \to \mathfrak{U}, \Phi(\psi) = \sigma\psi$ есть биекция двух множеств, и тогда $|\mathfrak{U}| = |\mathfrak{K}| = [F : E]_s$.

Остался последний компонент, для того, чтобы завершить доказательство.

Разобьем множество всех возможных K-гомоморфизмов из F в $\overline{K}$, на классы эквивалентности, где 2 гомоморфизма лежат в одном классе тогда и только тогда, когда их ограничение на E одинаково.

Покажем, что множество всех классов эквивалентности равномощно с множеством всех K-гомоморфизмов из E в K-гомоморфизмов из E в $\overline{K}$. Рассмотрим функцию переводящую класс эквивалетности (они все непусты по определению) U в ограничение на E какого-то из его элементов. Это отображение задано корректно по определению нашего отношения эквивалентности, а так же инъективно по нему же. Сюрьективность же верна, так как любой φ – K-гомоморфизм из E в $\overline{K}$, можно продлить до ψ – K-гомоморфизма из F в $\overline{K}$, и тогда класс эквивалетности, образованный ψ, отображается в φ.

Тогда всего у нас будет $[E : K]_s$ классов эквивалетности. А как мы доказали чуть выше существует ровно $[F : E]_s$ способов продлить на F произвольных K-гомоморфизм из E в $\overline{K}$. Таким образом, множество всех возможных K-гомоморфизмов из F в $\overline{K}$ делится на ровно $[E : K]_s$ классов эквивалентности, в каждом из которых ровно $[F : E]_s$ элементов, тогда $[F : K]_s = [F : E]_s \cdot [E : K]_s$.

(Отдельно хочу отметить, что в основной части доказательства я вообще не использовал никаких особых свойств конечности, а по сути доказал, что множество всех K-гомоморфизмов из F в $\overline{K}$, равномощно декартовому произведению множества K-гомоморфизмов из E в $\overline{K}$ и множества всех E-гомоморфизмов из F в $\overline{E}$, но мне не хочется писать строгий аппендикс про кардинальные числа, поэтому утверждение сформулировано только для конечных степеней сепарабельности). □

Теперь утверждение про конечные расширения полей.

Утверждение 4.5. *Если $E \supset K$ и $[E : K] < \infty$, то если $\operatorname{char} K = 0$, то $[E : K]_s = [E : K]$, если же $\operatorname{char} K = p > 0$, то $[E : K] = p^m\,[E : K]_s, m \geq 0$.*

Доказательство. Для начала, в силу конечности E над K, то E – алгебраическое расширение K, теперь пусть $e_1, \ldots, e_n$ – базис E над K, тогда рассмотрим башню расширений $K = E_0 \subset E_1 \subset \ldots \subset E_n = E$, где $E_k = K(e_1, \ldots, e_k), k > 0$, и воспользуемся тем, что $K(e_1, \ldots, e_k) = K(e_1, \ldots, e_{k-1})(e_k)$ и утверждениями 4.3, 4.4. □

4.3 Сепарабельное расширение

Определение 4.3. *Пусть $E \supset K$, тогда $\alpha \in E$ – сепарабельный над K элемент, если α это алгебраический над K элемент и $\operatorname{Irr}(\alpha : K)$ – сепарабельный многочлен. E – сепарабельное расширение K, если любой элемент $\alpha \in E$ сепарабелен над K.*

Утверждение 4.6. *Любое алгебраическое расширение поля K характеристики 0, есть сепарабельное расширение K.*

Доказательство. Следует из 4.1. □

Теперь посмотрим как можно по-другому определить конечное сепарабельное расширение поля K.

Утверждение 4.7. *Если E – конечное расширение поля K, то тогда следующие утверждения эквивалентны:*

1. *E – сепарабельное расширение K.*
2. *$E = K(\alpha_1, \ldots, \alpha_n)$, где $n \in \mathbb{N}$ и $\alpha_i \in E$ – сепарабельный над E элемент.*
3. *$[E : K]_s = [E : K]$*

Доказательство. $1 \Rightarrow 2$

Пусть $e_1, \ldots e_n$ – базис E над K, тогда e_i – сепарабелен над K, так как E – сепарабельное расширение K по 1, тогда $E = K(e_1, \ldots, e_n)$.

$2 \Rightarrow 3$

Пусть $E = K(\alpha_1, \ldots, \alpha_n)$, где α_i – сепарабельный над K элемент.

Тогда рассмотрим башню расширений:

$$K = E_0 \subset E_1 \subset \ldots \subset E_k = K(\alpha_1, \ldots, \alpha_k) \subset \ldots \subset E_n = E$$

Покажем, что $[E_{k+1} : E_k] = [E_{k+1} : E_k]_s$.

Для начала договоримся выбрать такое замыкание $\overline{K}$, что $\overline{K} = \overline{E_k} = \overline{E}$, так можно по 3.9.1. Тогда $K(\alpha_1, \ldots, \alpha_{k+1}) = K(\alpha_1, \ldots, \alpha_k)(\alpha_{k+1})$, а в силу того, что $\mathrm{Irr}(\alpha_{k+1} : K) = q(x)$ – сепарабельный многочлен и $\mathrm{Irr}(\alpha_{k+1} : E_k) \mid q(x)$, из леммы 4.2 следует что, $\mathrm{Irr}(\alpha_{k+1} : E_k)$– сепарабельный многочлен, и тогда $[E_{k+1} : E_k] = [E_{k+1} : E_k]_s$ по 4.3.

Теперь $[E : K] = \prod_{k=0}^{n-1}[E_{k+1} : E_k] = \prod_{k=0}^{n-1}[E_{k+1} : E_k]_s = [E : K]_s$ по 4.4 и 2.1.

$3 \Rightarrow 1$

Пусть $\alpha \in E$, покажем, что α – сепарабельный над K элемент.

Рассмотрим $K(\alpha)$, $[K(\alpha) : K], [E : K(\alpha)] < \infty$, так как $[E : K] < \infty$.

Тогда мы знаем в силу утверждения 4.5, что $[K(\alpha) : K]_s \leq [K(\alpha) : K], [E : K(\alpha)]_s \leq [E : K(\alpha)]$, тогда

$$[E : K(\alpha)] \cdot [K(\alpha) : K] = [E : K] = [E : K]_s = [E : K(\alpha)]_s \cdot [K(\alpha) : K]_s$$

Это верно в силу ранее доказанных теорем о степенях и промежуточных полях, а так же по условию 3, но если одно из неравенств выше строгое, то у нас нет равенства $[E : K] = [E : K]_s$, поэтому $[K(\alpha) : K]_s = [K(\alpha) : K], [E : K(\alpha)]_s = [E : K(\alpha)]$. Тогда по 4.3 верно, что $\mathrm{Irr}(\alpha : K)$ является сепарабельным многочленом, а следовательно α – сепарабельный над K элемент E. □

Теперь покажем свойства сепарабельного расширения.

Утверждение 4.8. *Если K это некоторое поле, и каждый элемент $\alpha \in S$ является сепарабельным над K, то $K(S)$ это сепарабельное расширение K.*

Доказательство. $\beta \in K(S) \Leftrightarrow \beta \in K(\alpha_1, \ldots, \alpha_n)$, где α_i это некоторые элементы из S, но все α_i сепарабельные над K, а, следовательно, по утверждению 4.7 $K(\alpha_1, \ldots, \alpha_n)$ – сепарабельное расширение K, и тогда β – сепарабельный над K элемент, а следовательно, $K(S)$ – сепарабельное расширение K. □

Утверждение 4.9. *Если $K \subset E \subset F$ и F – сепарабельное расширение K, то E сепарабельно над K и F – сепарабельно над E.*

Доказательство. То что E сепарабельно над K банально следует из того, что любой $E \subset F$, а любой минимальный многочлен элемента F над K сепарабелен.

Теперь если мы знаем, что для любого элемента $\beta \in F$, верно, что $\mathrm{Irr}(\beta : E) \mid \mathrm{Irr}(\beta : K)$, а $\mathrm{Irr}(\beta : K)$ сепарабелен по условию, тогда из 4.2 следует, что $\mathrm{Irr}(\beta : E) \in E[x]$ – сепарабельный многочлен и β – сепарабельный над E элемент. □

Утверждение 4.10. *Пусть $K \subset E \subset F$ это некоторые расширения полей. Если F – сепарабельное расширение E, а E – сепарабельное расширение K, то F – сепарабельное расширение K.*

Доказательство. Если $\alpha \in F$, то $q(x) = \mathrm{Irr}(\alpha : E) = \sum_{k=0}^{n} a_k x^k \in E[x]$ это сепарабельный многочлен. Рассмотрим $E' = K(a_0, \ldots, a_n)$ это конечное сепарабельное расширение K, по утверждению 4.7.

В силу того, что $E' \subset E$, то $q(x) = \mathrm{Irr}(\alpha : E')$ (из того, что $\mathrm{Irr}(\alpha : E) \mid \mathrm{Irr}(\alpha : E')$ и единственности мин. многочлена), тогда $E'(\alpha)$ это конечное сепарабельное расширение E' и тогда $[E'(\alpha) : K]_s = [E'(\alpha) : E']_s \cdot [E' : K]_s = [E'(\alpha) : E'] \cdot [E' : K] = [E'(\alpha) : K]$ и тогда по утверждению 4.7 верно, что $E'(\alpha)$ – сепарабельное расширение K, и тогда α – сепарабельный над K элемент. □

Утверждение 4.11. *Если E сепарабельное расширение K и композиция EF существует, то EF это сепарабельное расширение KF.*

Доказательство. Пусть $\alpha \in EF$, тогда по 1.4 верно, что $\alpha = ab^{-1}$, где a, b имеют вид $\sum_{k=1}^{n} \left(\prod_{i=1}^{n_k} \alpha_i\right), \alpha_i \in E \cup F$, И тогда $\alpha \in KF(\alpha_1, \ldots, \alpha_m), \alpha_i \in E$, где α_i это участвовавшие в разложении α элементы E, каждый элемент $\alpha_i \in E$ сепарабелен над K, тогда по лемме 4.2 верно, что α_i сепарабелен над KF, и тогда по утверждению 4.7 верно, что $KF(\alpha_1, \ldots, \alpha_m)$ это сепарабельное расширение KF и α это сепарабельный над KF элемент □

Утверждение 4.12. *Любая композиция сепарабельных расширений K есть сепарабельное расширение K.*

Доказательство. Пусть $F = \prod_{i \in I} F_i$, где F_i – сепарабельное расширение K, тогда для $\alpha \in F$, верно, что $\alpha = ab^{-1}$, где a, b имеют вид $\sum_{k=1}^{n} \left(\prod_{i=1}^{n_k} \alpha_i\right), \alpha_i \in \bigcup_{i \in I} F_i$, тогда $\alpha \in K(\alpha_1, \ldots, \alpha_m)$ для некоторых α_i – сепарабельных над K элементов, а следовательно по 4.7 $K(\alpha_1, \ldots, \alpha_m)$ – это сепарабельное расширение K и α – сепарабельный над K элемент. □

Теперь выведем из этого некоторые приятные следствия.

Утверждение 4.13. *Если E – конечное сепарабельное расширение K, то E – простое расширение K.*

Доказательство. Если $|K| < \infty$, то в силу конечности расширения $|E| < \infty$, то тогда мы уже доказали на курсе алгебры в 4 модуле, что мультипликативная группа E циклична и порождается неким $\alpha \in E$ и тогда $E = K(\alpha)$.

Теперь рассмотрим случай $|K| = \infty$, тогда пусть $[E : K] = [E : K]_s = n$, и $E = K(e_1, \dots, e_n)$, где $e_1, \dots, e_n$ – базис E над K.

Докажем, что если $E = K(\alpha, \beta)$, то $E = K(\gamma)$ для какого-то элемента. Далее, воспользовавшись индукцией и тем, что $K(\alpha_1, \dots, a_{k-1}, a_k) = K(\alpha_1, \dots, a_{k-2})(a_{k-1}, a_k)$ докажем утверждение для произвольного k.

Пусть $E = K(\alpha, \beta)$ и $\varphi_1, \dots, \varphi_n$ – различные K-гомоморфизмы из E в $\overline{K}$.

Теперь рассмотрим многочлен:

$$f(x) = \prod_{1 \le i < j \le n} ((\varphi_i(\alpha) + \varphi_i(\beta)x) - (\varphi_j(\alpha) + \varphi_j(\beta)x)) \in \overline{K}[x]$$

Поскольку если $\varphi_i(\alpha) = \varphi_j(\alpha), \varphi_i(\beta) = \varphi_j(\beta)$ означается для K-гомоморфизма, что $\varphi_i = \varphi_j \Leftrightarrow i = j$, то $f(x) \neq 0$, а у неконстантного многочлена в поле конечное число корней, тогда существует $t \in K$, что $f(t) \neq 0$.

Так же в силу того, что φ_i – K-гомоморфизм, то $\varphi_i(\alpha) + \varphi_i(\beta)t = \varphi(\alpha + \beta t)$.

Тогда из условия $f(t) \neq 0$, следует, что $i \neq j \Rightarrow \varphi_i(\alpha + \beta t) \neq \varphi_i(\alpha + \beta t)$.

Теперь $K \subseteq K(\alpha + \beta t) \subseteq K(\alpha, \beta)$, тогда $K(\alpha + \beta t)$ – сепарабельное расширение K, но ограничения φ_i на $K(\alpha + \beta t)$ уже дают n разных K-гомоморфизмов из $K(\alpha + \beta t)$ в $\overline{K}$, и $[K(\alpha + \beta) : K] = [K(\alpha + \beta) : K]_s = n = [E : K]$, следовательно $K(\alpha + \beta t) = K(\alpha, \beta) = E$, что мы и хотели доказать. □

Утверждение 4.14. *Если E – сепарабельное расширение поля K и $\deg \mathrm{Irr}(\alpha : K) \le n$ для любого $\alpha \in E$, то $[E : K] \le n < \infty$.*

Доказательство. Пусть $\alpha \in E$ это элемент с максимальной степенью минимального многочлена, то есть $\deg \mathrm{Irr}(\alpha, K) = m$ и степень мин. многочлена любого другого элемента не больше m.

Теперь $\beta \in E$ это проивзольный элемент E, тогда $K(\alpha, \beta) = K(\gamma)$ по утверждению 4.13 и $[K(\gamma) : K] \le m$, но $[K(\alpha) : K] = m$, тогда $[K(\gamma) : K] = m$ и $K(\gamma) = K(\alpha) \Rightarrow \beta \in K(\alpha)$, и тогда $K(\alpha) = E$ $[E : K] = m \le n$. □

4.4 Важный пример

Вообще говоря, вдумчивый читатель может задаться вопросом, а существуют ли вообще какие-либо неприводимые и несепарабельные многочлены. Вообще наше утверждение 4.1 говорит, что в теории в каком-то поле положительной характеристики может встретится неприводимый и несепарабельный многочлен.

Но вот незадача, любой приходящий в голову пример поля положительной характеристики это поле конечное поле, но в нем ВСЕ неприводимые многочлены сепарабельны (это будет доказано в конспекте чуть позже).

Поэтому тут надо думать хитрее, и найти поле положительной характеристики, которое является бесконечным.

Тут я позволю себе сослаться в первый раз на что-либо кроме курса алгебры в четветом модуле (Abstract Algebra (Graduate Texts in Mathematics), Pierre Antoine Grillet, 2007, p.141-146).

Мне нужно достать лемму Гаусса и критерий Эйзейнштейна для произвольных факториальных колец (определение есть в книге). Я уже успел разобрать самостоятельно эти утверждения для целых и рациональных чисел, они несложные и факториальные кольца ведут себя похоже на целые числа, так что разобрать те утверждения самостоятельно это дело 8 часов, максимум.

Так же я позволю себе не переписывать все определения сюда, в случае чего, их можно посмотреть в книге.

Определение 4.4. *Многочлен $f(x) \in R[x]$, где R это факториальное кольцо называется примитивным, если наибольший общий делитель коэффициентов $f(x)$ ассоциирован с единицей.*

Лемма 4.15. *Пусть Q – поле отношений факториального кольца R, тогда для любого $f(x) \in Q[x]$ существует единственное, с точностью до умножения на обратимые элементы R, представление $f(x) = tf^*(x)$, где $t \in Q, t \neq 0$ и $f^*(x) \in R[x]$ – примитивный многочлен.*

Лемма 4.16 (лемма Гаусса)**.** *Пусть R – факториальное кольцо.*

Если $f(x), g(x) \in R[x]$ это примитивные многочлены, то $f(x)g(x)$ тоже примитивный многочлен.

Следствие 4.16.1. *Пусть Q – поле частных факториального кольца R, тогда $f(x) \in Q[x]$ неприводим тогда и только тогда $f^*(x) \in R[x]$ неприводим в $R[x]$.*

Утверждение 4.17 (Критерий Эйзейнштейна)**.** *Пусть R это факториальное кольцо.*

$f(x) = \sum_{k=0}^{n} a_k x^k \in R[x]$.

Многочлен $f(x)$ неприводим, если существует простой элемент p из R, что:

1. $p \mid a_i, i < n$
2. $p \nmid a_n$
3. $p^2 \nmid a_0$

В книге есть дополнительно условие про примитивность многочлена, оно не нужно, так как p не делит наибольший общий множитель.

Так же есть более общая формулировка, где участвует простой идеал, но я не доказал даже ту что выше, поэтому не имеет особого смысла писать более сложную версию.

Теперь собственно перейдем к примеру.

Пусть $\mathbb{F}_q$ это некоторое конечное поле $q = p^n, \operatorname{char} K = p$, рассмотрим поле рациональных дробей над этим полем $\mathbb{F}_q(t)$ и многочлен $f(x) = x^p - t \in \mathbb{F}_q(t)[x]$.

Для заметим, что $f(x)$ это примитивный многочлен в $\mathbb{F}_q[t]$, а поэтому его неприводимость эквивалентна неприводимости в $\mathbb{F}_q(t)$ по 4.16.1,

$\mathbb{F}_q[t]$ является факториальным кольцом, в силу единственности разложения многочлена на неприводимые многочлены.

Теперь заметим, что в силу того, что $\deg(f \cdot g)(x) = \deg f(x) + \deg g(x)$, то элемент $t \in \mathbb{F}_q[t]$ является простым, нет такого нетривиального разложения $t = f(t) \cdot g(t)$.

Теперь заметим, что в $f(x) = x^p - t$ верно, что старший коэффициент не делится на t, все остальные делятся на t, а свободный не делится на t^2. Тогда наш многочлен удовлетворяет критерию Эйзейнштейна и является неприводимым над $\mathbb{F}_q[t]$, а следовательно и над $\mathbb{F}_q(t)$.

Теперь посмотрим на $f(x)$ в $\overline{\mathbb{F}_q(t)}$, в силу алгебраической замкнутости $\overline{\mathbb{F}_q(t)}$ есть $\alpha \in \overline{\mathbb{F}_q(t)}$ что $f(\alpha) = 0$, тогда $t = \alpha^p$, а так как у нас поле характеристики p, то $f(x) = x^p - t = x^p - \alpha^p = (x - \alpha)^p \in \overline{\mathbb{F}_q(t)}[x]$, но тогда из единственности разложения на множители в $\overline{\mathbb{F}_q(t)}[x]$ следует, что $f(x)$ не является сепарабельным многочленом.

Такой вот интересный пример, ради которого пришлось подтянуть много интересной теории.

5 Чисто несепарабельные расширения

На всякий случай рассмотрим антипода сепарабельного расширения, а именно чисто несепарабельное расширение.

Определение 5.1. *Алгербраическое расширение E поля K называется чисто несепарабельным, если любой элемент $E \backslash K$ не является сепарабельным над K.*

Утверждение 5.1. *Для любого алгебраического расширения $E \subset K$, верно что*

$F = \{\alpha \in E \mid \alpha$– сепарабельный над K элемент$\}$ – это сепарабельное над K подполе E и E это чисто несепарабельное расширение F.

Доказательство. Для начала любой элемент K – сепарабелен над K, и тогда $1, 0 \in F$.

Так же для произвольных $\alpha, \beta \in F, \beta \neq 0$, верно, что $K(\alpha, \beta)$ это сепарабельное расширение K по 4.7 и тогда $\alpha - \beta, \alpha\beta^{-1} \in F$, и тогда F – подполе E.

F – сепарабельно над K по определению.

Теперь покажем, что любой сепарабельный над F элемент F принадлежит F (тогда автоматически любой элемент $E \backslash F$ не сепарабелен над F, так как иначе он бы принадлежал F)

Если $\alpha \in E$ – сепарабелен над F, то по утверждению 4.7, верно, что $F(\alpha)$ – сепарабельное расширение F, но тогда по 4.10 верно, что $F(\alpha)$ – сепарабельное расширение K, и тогда α – сепарабельный над K элемент и $\alpha \in F$, что мы и хотели доказать. □

Также известно, что в поле характеристики ноль все чисто несепарабельные расширения K тривиальны, то есть равны K.

Если же мы находимся в поле K характеристики $p > 0$, то вспомним, что для любых $\alpha, \beta \in K$, верно, что $(\alpha - \beta)^p = \alpha^p - \beta^p$, а также для многочленов, верно, что $x^{p^m} - \alpha^{p^m} = (x - \alpha)^{p^m}$, все это следует из бинома Ньютона.

Тогда для любого элемента $a \in K$ существует α корень степени p^m в $\overline{K}$ в силу того, что $\overline{K}$ – алгебраически замкнутое поле. При этом этот корень единственный, так как у многочлена $f(x) = x^{p^m} - a = x^{p^m} - \alpha^{p^m} = (x-\alpha)^{p^m}$ ровно один корень в $\overline{K}$ (это следует из единственности разложения на простые в кольце многочленов над полем). Воспользуемся этим для рассмотрения такого примера:

Утверждение 5.2. *Если поле K имеет характеристику $p > 0$, то $K^{1/p^\infty} = \left\{\alpha \in \overline{K} \mid \exists\, m \geq 0 : \alpha^{p^m} \in K\right\}$ это чисто несепарабельное расширение K.*

Доказательство. Для начала покажем, что K^{1/p^∞} – подполе $\overline{K}$, содержащее K.

Для начала, любой элемент K принадлежит K^{1/p^∞}, так как $v^1 = v \in K$, тогда $1, 0 \in K^{1/p^\infty}$,

Теперь $\alpha, \beta \in K^{1/p^\infty}, \beta \neq 0$, тогда $\alpha^{p^n} \in K, \beta^{p^m} \in K$, пусть $l = \max(m, n)$. тогда:

$$(\alpha - \beta)^{p^l} = \alpha^{p^l} - \beta^{p^l} = (\alpha^{p^n})^{p^{l-n}} - (\beta^{p^m})^{p^{l-m}} \in K$$

$$(\alpha\beta^{-1})^{p^l} = (\alpha^{p^n})^{p^{l-n}} \left((\beta^{p^m})^{p^{l-m}}\right)^{-1} \in K$$

Тогда действительно подполе.

Теперь если $\alpha \in K^{1/p^\infty} \backslash K$ и $\alpha^{p^m} = a \in K$, тогда $\operatorname{Irr}(\alpha : K) \mid x^{p^m} - a = (x - \alpha)^{p^m}$, тогда у $\operatorname{Irr}(\alpha : K)$ только один корень $\alpha \in \overline{K}$, но при этом так как $\alpha \notin K$, то $\deg \operatorname{Irr}(\alpha : K) > 1$, и тогда α несепарабельный над K элемент и K^{1/p^∞} – чисто несепарабельное расширение K. □

И теперь еще одна достаточно полезная лемма для описания чисто несепарабельного расширения.

Лемма 5.3. *Если характеристика K равна $p > 0$ и α – алгебраический над K элемент, то $\alpha^{p^n} \in K$ для какого-то $n \geq 0 \Leftrightarrow \operatorname{Irr}(\alpha : K) = x^{p^m} - a, m \geq 0, a \in K$.*

Доказательство. $\Leftarrow$ очевидно, $\alpha^{p^m} = a$.

$\Rightarrow$.

Пусть $\alpha^{p^n} = b$, тогда $\operatorname{Irr}(\alpha : K) = q(x)$ и $q(x) \mid x^{p^n} - b = (x - \alpha)^{p^n}$ Тогда у $q(x)$ только один корень в $\overline{K}$ и это α. Так же из доказательства 4.1 видно, что $q(x) = s(x^{p^m})$ для какого-то сепарабельного многочлена $s(x) \in K[x]$, причем из доказательства следует, что у $q(x)$ ровно столько корней, сколько и у $s(x)$ (это так же следует из того, что только один корень степени p^m в $\overline{K}$). Тогда у $s(x)$ только один корень в $\overline{K}$, а в силу сепарабельности $s(x) = x - a \in K[x]$, тогда $q(x) = s(x^{p^m}) = x^{p^m} - a, a \in K$, что мы и хотели доказать.

□

Определение 5.2. *Если характеристика поля K равна $p > 0$, то тогда элемент $\alpha \in E \supset K$ чисто несепарабелен над K, если $\alpha^{p^m} \in K, m \geq 0$ или эквивалентно $\operatorname{Irr}(\alpha : K) = x^{p^n} - a, n \geq 0, a \in K$.*

Утверждение 5.4. *Если $E \subset K$ – алгебарическое расширение, $\operatorname{char} K = p > 0$, то следующее эквивалентно:*

1. *E – чисто несепарабельное расширение K.*
2. *Любой элемент E чисто несепарабелен над K.*
3. *Существует K-гомоморфизм из E в K^{1/p^∞}.*
4. *$[E : K]_s = 1$.*

Доказательство. $1 \Rightarrow 2$

Если $\alpha \in E$, то $q(x) = \operatorname{Irr}(\alpha : K)$ и из 4.1 $s(x)$ это некоторый неприводимый, сепарабельный и приведенный многочлен, такой, что $q(x) = s(x^{p^n})$, тогда $s(x) = \operatorname{Irr}(\alpha^{p^n} : K)$ в силу неприводимости $s(x)$, но многочлен $s(x)$ сепарабельный, следовательно α^{p^n} – сепарабельный над K элемент, в силу того, что E – чисто несепарабельное расширение поля K, то $\alpha^{p^n} \in K$ и тогда α – чисто несепарабельный над K элемент.

$2 \Rightarrow 3$.

Пусть $\varphi : E \to \overline{K}$ некоторый K-гомоморфизм, он существует из утверждения 3.6.

Теперь пусть $\alpha \in E$ и в силу 2, $\alpha^{p^n} = a \in K$, тогда покажем, что $\varphi(\alpha) \in K^{1/p^\infty}$.

$\varphi(\alpha)^{p^n} = \varphi\left(\alpha^{p^n}\right) = \varphi(a) = a \in K$, предпоследнее равенство верно, так как φ – K– гомоморфизм, тогда $\varphi(\alpha)^{p^n} \in K$, а следовательно $\varphi(E) \subset K^{1/p^\infty}$.

$3 \Rightarrow 4$

Пусть $\varphi : E \to K^{1/p^\infty} \subset \overline{K}$ это K-гомоморфизм из условия 3.

Теперь пусть $\psi : E \to \overline{K}$ произвольный K-гомоморфизм, покажем, что $\psi(\alpha) = \varphi(\alpha)$ для $\alpha \in E$

Для начала так как $\varphi(\alpha) \in K^{1/p^\infty}$, то $\varphi(\alpha)^{p^n} = a \in K$, тогда воспользуемся свойством гомоморфизма, а именно $a = \varphi(\alpha)^{p^n} = \varphi\left(\alpha^{p^n}\right) \in K$ а, так как φ – K-гомоморфизм и любой гомоморфизм полей инъективен, тогда $\varphi(a) = a = \varphi\left(\alpha^{p^n}\right) \Rightarrow a = \alpha^{p^n}$.

Теперь посмотрим на $\psi(\alpha)^{p^n} = \psi(\alpha^{p^n}) = a$, тогда $\psi(\alpha), \varphi(\alpha) \in \overline{K}$ – корни степени p^n из a, но тогда из единственности корня степени p^n, которая была описана выше, следует, что $\varphi(\alpha) = \psi(\alpha)$.

Следовательно любой K-гомоморфизм $\psi : E \to \overline{K}$ совпадает с φ, и тогда $[E : K]_s = 1$.

$4 \Rightarrow 1$

Пусть $\alpha \in E$ – сепарабельный над K, элемент, тогда $[K(\alpha) : K] = [K(\alpha) : K]_s = \deg \mathrm{Irr}(\alpha : K) = n$, теперь $1 = [E : K]_s = [E : K(\alpha)]_s \cdot [K(\alpha) : K]_s \geq n$ по 4.4 из того, что $1 \geq n$, следует, что $n = 1$, тогда $[K(\alpha) : K] = 1, K(\alpha) = K, \alpha \in K$, тогда любой сепарабельный элемент принадлежит K, а следовательно все элементы в $E \backslash K$ не являются сепарабельными. □

Так же из условия 3 автоматически следует, что K^{1/p^∞} это наибольшее, с точностью до изоморфизма, чисто несепарабельное расширение K (любое чисто несепарабельное расширение K изоморфно подполю K^{1/p^∞}).

Теперь перечислим свойства чисто несепарабельного расширения K, они доказываются похоже с тем, что мы доказывали выше для сепарабельных и алгебраических расширений, поэтому я позволю себе опустить доказательства этих свойств.

Утверждение 5.5. *Если для любого $\alpha \in S$ верно, что α – чисто несепарабельный над K элемент, то $K(S)$ – чисто несепарабельное расширение K.*

Утверждение 5.6. *Пусть $K \subset E \subset F$ – поля и если F – чисто несепарабельное расширение K, то E – чисто несепарабельное расширение K и F – чисто несепарабельное расширение E.*

Утверждение 5.7. *Пусть $K \subset E \subset F$ – поля и если F – чисто несепарабельное расширение E и E – чисто несепарабельное расширение K, то F – чисто несепарабельное расширение K.*

Утверждение 5.8. *Если E – алгебраическое и чисто несепарабельное расширение K, и EF существует, то EF – чисто несепарабельное расширение KF.*

Утверждение 5.9. *Любая композиция чисто несепарабельных и алгебраических расширений K есть чисто несепарабельное расширение K.*

6 Нормальные расширения

6.1 Поле разложение

Определение 6.1. *Говорят, что многочлен $f(x) \in K[x]$ разлагается на линейные множители (можно просто сократить до разлагается) в $E \supset K$, если существует факторизация $f(x) = a(x-\alpha_1)\dots(x-\alpha_n), \alpha_i \in E, a \in K$.*

Определение 6.2. *Пусть K – поле.*

Тогда поле разложения многочлена $f(x) \in K[x]$ над K это такое расширение $E \supseteq K$, что в нем $f(x)$ разлагается на линейные множители, и E сгененрировано над K корнями $f(x)$.

Если $\mathcal{S} \subseteq K[x]$ некоторое подмножество кольца многочленов над K, то поле разложения $\mathcal{S}$ над K – это расширение $E \supseteq K$, такое, что в нем разлагается любой многочлен из $\mathcal{S}$, и E сгененрировано над K корнями многочленов из $\mathcal{S}$.

Поле разложение сгененрировано алгебраическими элементами над K, а следовательно является алгебраическим расширением K.

У полей разложений есть прекрасное свойство, опишем его.

Лемма 6.1. *Если E и F поля разложения $\mathcal{S} \subseteq K[x]$ над K и $F \subseteq \overline{K}$, то для произвольного K-гомоморфизма $\varphi : E \to \overline{K}$, верно, что $\varphi E = F$.*

Доказательство. Для начала заметим, что множество $F = K(\mathcal{M})$, где $\mathcal{M} = \{\alpha \in F \,|\, g(\alpha) = 0, g(x) \in \mathcal{S}\} = \left\{\alpha \in \overline{K} \,|\, g(\alpha) = 0, g(x) \in \mathcal{S}\right\}$.

Второе равенство следует из того, что в $F \subseteq \overline{K}$ раскладываются все многочлены из $\mathcal{S}$, тогда в силу единственности разложения многочлена на неприводимые множители в $\overline{K}[x]$, любой корень многочлена из $\mathcal{S}$ в $\overline{K}$ лежит в F. В свою очередь все корни в F лежат и в $\overline{K}$.

Теперь покажем, что $\varphi(E) \subseteq F$, в силу того, что φ – K-гомоморфизм, верно, что если $\alpha \in E$ – корень $g(x) \in \mathcal{S}$, то и $\varphi(\alpha)$ – корень $g(x)$, а следовательно $\varphi(\alpha) \in \mathcal{M} \subseteq F$.

По утверждению 1.4, верно, что любой элемент E имеет вид $u = ab^{-1}$, где a, b имеют вид $\sum_{k=1}^{n} a_k \left(\prod_{i=1}^{n_k} \alpha_i^{l_i}\right), a_k \in K, \alpha_i$ – корень какого-то многочлена из $\mathcal{S}$

Тогда $\varphi\left(\sum_{k=1}^{n} a_k \left(\prod_{i=1}^{n_k} \alpha_i^{l_i}\right)\right) = \sum_{k=1}^{n} a_k \left(\prod_{i=1}^{n_k} \varphi(\alpha_i)^{l_i}\right) \in F$ (так как $K \subseteq F$), тогда
$\varphi(u) = \varphi(a)\varphi(b)^{-1} \in F$, таким образом, $\varphi(E) \subseteq F$.

Покажем, что $F \subseteq \varphi(E)$.

Для начала, если $f(x) \in \mathcal{S}$, то $f(x) = a(x - \alpha_1) \dots (x - \alpha_n)$, но вспоминая о гомоморфизме $f(x) \mapsto {}^{\varphi}f(x)$, и тогда $f(x) = {}^{\varphi}f(x) = {}^{\varphi}\left(a(x - \alpha_1) \dots (x - \alpha_n)\right) = a(x - \varphi(\alpha_1)) \dots (x - \varphi(\alpha_n))$.

Таким образом, любой $\alpha \in \mathcal{M} \subseteq \overline{K}, g(\alpha) = 0, g(x) \in \mathcal{S}$ также принадлежит и $\varphi(E)$, поскольку любой произвольный многочлен из $\mathcal{S}$ раскладывается в $\varphi(E) \subseteq \overline{K}$, тогда $\mathcal{M} \subseteq \varphi(E)$, еще верно, что в силу того, что φ – K-гомоморфизм, то $K \subseteq \varphi(E)$, тогда (по 1.3) $F = K(\mathcal{M}) \subseteq \varphi(E)$.

В итоге, $F = \varphi(E)$

□

Следствие 6.1.1. *Для любого $\mathcal{S} \subseteq K[x]$, существует поле разложение $E \subseteq \overline{K}$, более того, все поля разложения $\mathcal{S}$ K-изоморфны друг другу.*

6.2 Определение нормального расширения

Утверждение 6.2. *Для алгебраического расширения $K \subseteq E \subseteq \overline{K}$ следующие утверждения эквивалентны:*

1. *E – поле разложения над K для некоторого подмножества $\mathcal{S} \subseteq K[x]$.*
2. *$\varphi(E) = E$ для любого K-гомоморфизма $\varphi : E \to \overline{K}$.*
3. *$\varphi(E) \subseteq E$ для любого K-гомоморфизма $\varphi : E \to \overline{K}$.*
4. *$\sigma(E) = E$ для любого σ – K-автоморфизма $\overline{K}$.*
5. *$\sigma(E) \subseteq E$ для любого σ – K-автоморфизма $\overline{K}$.*
6. *Любой неприводимый многочлен $q(x) \in K[x]$ с корнем в E разлагается на линейные множители в E.*

Доказательство. $1 \Rightarrow 2$ это 6.1.

$2 \Rightarrow 3, 4 \Rightarrow 5$, это более слабое условие.

$2 \Rightarrow 4$ рассмотреть $\sigma|_E$ – K-гомоморфизм из E в $\overline{K}$, тогда $\sigma(E) = \sigma|_E(E) = E$.

$3 \Rightarrow 5$, аналогично $2 \Rightarrow 4$.

$5 \Rightarrow 6$ Пусть $q(x)$ это некоторый неприводимый полином из $K[x]$, и $q(\alpha) = 0, \alpha \in E$, тогда пусть в $\overline{K}$ $q(x) = a(x - \alpha_1) \dots (x - \alpha_n) = a(x - \beta_1)^{n_1} \dots (x - \beta_m)^{n_m}, \beta_i \neq \beta_j$.

Теперь по 2.4 в силу того, что $q(x)/a = \mathrm{Irr}(\alpha : K)$ (a – старший коэффициент, для минимального многочлена тут важна неприводимость), верно, что для любого β_i существует K-гомоморфизм $\varphi_{\beta_i} : K(\alpha) \to \overline{K}$, такой, что $\varphi(\alpha) = \beta_i$, тогда поскольку $K \subseteq K(\alpha) \subseteq E \subseteq \overline{K}$, то φ_{β_i} продляется до K-автоморфизма $\overline{K}$ σ_{β_i}, тогда мы знаем по условию 5, что $\sigma_{\beta_i}(\alpha) = \beta_i \in E$, следовательно все $\beta_i \in E$ и тогда $q(x)$ разлагается в E.

$6 \Rightarrow 1$.

Пусть $K \subseteq F \subseteq \overline{K}$ – это поле разложения $\mathcal{S} = \{q(x) \in K[x] \,|\, q(x)$ – неприводимый многочлен с корнем в $E\}$.

Покажем, что $F = E$.

Для начала пусть $\mathcal{M} = \{\alpha \in F \,|\, g(\alpha) = 0, g(x) \in \mathcal{S}\} = \{\alpha \in \overline{K} \,|\, g(\alpha) = 0, g(x) \in \mathcal{S}\}$, последнее равенство верно, в силу того, что в $F \subseteq \overline{K}$ раскладывается на линейные множители любой многочлен из $\mathcal{S}$ и если $\alpha \in \overline{K}$ – корень $g(x) \in \mathcal{S}$, то $\alpha \in F$ (иначе ни одна из скобок в разложении в $F \subseteq \overline{K}$ не занулится).

$F = K(\mathcal{M})$

Тогда, если $\alpha \in E \subseteq \overline{K}$, то α – корень $\mathrm{Irr}(\alpha : K)$ – неприводимого многочлена с корнем α в E, то есть многочлена из $\mathcal{S}$, тогда $\alpha \in \mathcal{M} \subseteq F$.

С другой стороны, $\mathcal{M} \subseteq E$, так как в $E \subseteq \overline{K}$ раскладывается любой многочлен из $\mathcal{S}$ по условию 6, а следовательно E содержит все его корни из $\overline{K}$ (любой корень из $\overline{K}$ лежит в E, иначе не будет занулена ни одна из скобок в разложении в E), так же E содержит K по определению, тогда $K(\mathcal{M}) \subset E \subset K(\mathcal{M}) \Rightarrow F = E$, но более того, $\mathcal{M} \subset E \subset \mathcal{M}$, тогда поле E есть поле разложения $\mathcal{S}$ и равно множеству всех корней многочленов из $\mathcal{S}$ в $\overline{K}$.

□

Определение 6.3. *Нормальное расширение поля K, это такое алгебраическое расширение поля K, которое удовлетворяет одному из эквивалентных свойств из 6.2 для какого-то алгебраического замыкания K, содержащим в себе наше расширение.*

6.3 Сопряжения.

Определение 6.4. *Если K это поле, то сопряженный с $\alpha \in \overline{K}$ элемент это образ α под действием некоторого K-автоморфизме $\overline{K}$.*

Сопряжение алгебраического расширения $K \subseteq E \subseteq \overline{K}$ это образ E под действием какого-то K-автоморфизме E.

Утверждение 6.3. *Все сопряжения $\alpha \in \overline{K}$ есть корни $\mathrm{Irr}(\alpha : K)$ в $\overline{K}$.*

Доказательство. Пусть $\mathrm{Irr}(\alpha : K) = q(x) = (x - \alpha_1) \dots (x - \alpha_n)$.

Если σ некоторый K-автоморфизм $\overline{K}$, то $q(\sigma(\alpha)) = \sigma(q(\alpha)) = 0$, так как σ – K-автоморфизм.

С другой стороны, если α_i – корень $q(x)$ то по 2.4 существует $\varphi : K(\alpha) \to \overline{K}$, что $\varphi(\alpha) = \alpha_i$, причем так как $K(\alpha) \subseteq \overline{K}$, то по 3.6 существует продолжение φ на $\overline{K}$, некоторый σ – K-автоморфизм $\overline{K}$, тогда $\sigma(\alpha) = \alpha_i$ и α_i сопряжен над K с α.

Таким образом, действительно, все сопряжения $\alpha \in \overline{K}$ над K есть в точности корни $q(x)$. □

Утверждение 6.4. *Для алгебраического расширения $K \subseteq E \subseteq \overline{K}$ следующие условия эквивалентны:*

1. *E – нормальное расширение K.*
2. *Все сопряжения над K произвольного элемента E лежат в E.*
3. *У E только одно сопряжение над K.*

Доказательство. $1 \Leftrightarrow 3$ следует из того, что любое расширение K сопряжено над K само с собой и 6.2.

$1 \Rightarrow 2$

Если E – нормальное расширение, то по 6.2 следует, что любой неприводимый многочлен с корнем в E, раскладывается в E, тогда если $\alpha \in E$, то $\mathrm{Irr}(\alpha : K)$ раскладывается в $E \subseteq \overline{K}$, и тогда E содержит все возможные корни $\mathrm{Irr}(\alpha : K)$ в $\overline{K}$, а следовательно по утверждению 6.3 содержит все сопряжения с α над K. Тогда E содержит все сопряжения для произвольного элемента E.

$2 \Rightarrow 1$.

Пусть σ – произвольный K-автоморфизм $\overline{K}$, тогда для любого $\alpha \in E$, верно, что $\sigma(\alpha) \in E$, в силу того, что $\sigma(\alpha)$ это сопряжение с α.

Тогда $\sigma(E) \subseteq E$, а следовательно по 6.2 верно, что E –нормальное расширение K. □

6.4 Свойства нормальных расширений.

Давайте обсудим некоторые свойства.

Утверждение 6.5. *Если F – нормальное расширение K и $K \subseteq E \subseteq F$, то F – нормальное раширение E.*

Доказательство. Следует из 6.2 и того, что любой E-гомоморфизм это K-гомоморфизм. □

Утверждение 6.6. *Если E – нормальное расширение K и композиция EF существует, то EF – нормальное расширение KF.*

Доказательство. В силу того, что по утверждению 2.10 EF это алгебраическое расширение KF, то по утверждению 3.9.1 можно выбрать такое алгебраическое замыкание $K \subseteq E \subseteq EF \subseteq \overline{KF}$. В силу того, что $\overline{KF}$ это алгебраически замкнутое расширение E, то по утверждению 3.9 существует подполе $\overline{KF}$ E-изоморфное $\overline{E}$, его и будем считать $\overline{E} = \overline{K}$ так можно по 3.9.1.

Таким образом получаем $K \subseteq E \subseteq \overline{K} \subseteq \overline{KF}$.

Теперь покажем, что под действием произвольного KF-автоморфизма $\overline{KF}$ элементы E принадлежат E.

Пусть σ – произвольный KF-автоморфизм $\overline{KF}$. Любой KF-автоморфизм является и K автоморфизмом, теперь $\alpha \in E$, тогда α – корень $\mathrm{Irr}(\alpha : K) = q(x)$, а этот многочлен разлагается в $\overline{K}$ на линейные множители по определению, тогда $q(\sigma(\alpha)) = \sigma(q(\alpha)) = 0$, тогда $\sigma(\alpha)$ это корень $q(x)$, а следовательно лежит в $\overline{K}$, так как $q(x)$ разлагается в $\overline{K}$ на линейные множители.

Таким образом $\sigma|_E$ – это K-гомоморфизм из E в $\overline{K}$, но тогда в силу нормальности E (по 6.2), верно, что $\sigma(E) = \sigma|_E(E) = E$.

Тогда любой элемент $E \cup F$ под действием σ – KF– автоморфизма $\overline{KF}$ лежит в $E \cup F$, но тогда $\sigma(EF) \subseteq EF$ (это следует из классификации композиции 1.4).

Таким образом по 6.2 у нас нормальное расширение. □

Утверждение 6.7. *Любая композиция нормальных расширений K есть нормальное расширение K.*

Доказательство. Пусть нам дано $\prod_{i \in I} F_i$, где F_i – нормальное расширение K.

Для начала, это алгебраическое расширение K (по 2.11), тогда по утверждению 3.9.1 верно, что существует такое $\overline{K}$, что $K \subseteq \prod_{i \in I} F_i \subseteq \overline{K}$, тогда любого $\alpha \in F_j, j \in I$, верно, что если σ – произвольный K-автоморфизм $\overline{K}$, то $\sigma(\alpha) \in F_j$ в силу нормальности, но тогда вспоминая, как выглядит элемент $\prod_{i \in I} F_i$ (из 1.4), получаем, что $\sigma(\prod_{i \in I} F_i) \subseteq \prod_{i \in I} F_i$. □

Утверждение 6.8. *Любое пересечение нормальных полей $E_i \subseteq \overline{K}$ есть нормальное поле.*

Доказательство. Теперь $E = \bigcap_{i \in I} E_i$ это, во-первых, поле, а во-вторых, для произвольного σ K-автоморфизма $\overline{K}$, верно, что $\sigma(E_i) = E_i$, тогда если элемент α принадлежал всем полям из семейства $(E_i)_{i \in I}$, то и его образ принадлежит всем полям семейства. □

Но некоторые ожидаемые свойства не верны.

Например, неверно, что если $K \subseteq E \subseteq F$, где F – нормально над E и E – нормально над K, то F – нормально над K.

Так же не верно, то что если $K \subseteq E \subseteq F$ и F – нормально над K, то E – нормально над K.

Для начала скажу, что подполе $\overline{\mathbb{Q}} \subset \mathbb{C}$ всех алгебраических над $\mathbb{Q}$ чисел является алгебраическим замыканием $\mathbb{Q}$ по причинам аналогичным тому, что было в доказательстве 3.9.

Например для второго случая, рассмотрим башню $\mathbb{Q} \subseteq \mathbb{Q}(t) \subseteq \mathbb{Q}(t, j)$, где $t = \sqrt[3]{2}, j = \cos\left(\frac{\pi}{3}\right) + i\sin(\frac{\pi}{3})$, тогда в нашем случае поле $\mathbb{Q}(t, j)$ является полем разложения неприводимого многочлена $f(x) = x^3 - 2$, так как его корнями являются t, tj, tj^2, следовательно, оно является нормальным над $\mathbb{Q}$, но при этом существует (по 3.6) $\mathbb{Q}$-гомоморфизм $\varphi : \mathbb{Q}(t) \to \mathbb{Q}(tj) \subset \overline{\mathbb{Q}} \subset \mathbb{C}, \varphi(t) = tj$, но $\mathbb{Q}(tj) \neq \mathbb{Q}(j)$, так как во втором поле вообще нет таких чисел, квадрат которых дает отрицательное число, а во втором есть. Тогда $\mathbb{Q}(t)$ не является нормальным над $\mathbb{Q}$ полем.

Для первого же случая, я бы предложил рассмотреть пример $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$, тут $\mathbb{Q}(\sqrt{2})$ нормально над $\mathbb{Q}$ т.к поле разложения $x^2 - 2$, $\mathbb{Q}(\sqrt[4]{2})$ нормально над $\mathbb{Q}(\sqrt{2})$, так как поле разложения $x^2 - \sqrt{2}$, но при этом $\mathbb{Q}(\sqrt[4]{2})$ не является нормальным над $\mathbb{Q}$, так как есть гомоморфизм $\varphi : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(i\sqrt[4]{2}) \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}, \varphi(\sqrt[4]{2}) = i\sqrt[4]{2}$, так как $x^4 - 2 = \mathrm{Irr}(\sqrt[4]{2} : \mathbb{Q})$, а $\mathbb{Q}(\sqrt[4]{2}) \neq \mathbb{Q}(i\sqrt[4]{2})$, так как во втором поле, есть число квадрат которого является отрицательным числом, а в первом нет.

Добавим еще несколько нетривиальных свойств

Определение 6.5. *Наименьшее по включению нормальное поле $K \subseteq E \subseteq \overline{K}$ это такое нормальное расширение K, содержащееся в любом нормальном расширении K, содержащем E, оно существует и является пересечением всех нормальных над K подполей $\overline{K}$ содержащих E (по 6.8 оно нормально и не пусто, так как $\overline{K}$ – нормально над K).*

Утверждение 6.9. *Наименьшее по включению нормальное поле $N \subseteq \overline{K}$, содержащее в себе алгебраическое расширение $K \subseteq E \subseteq \overline{K}$ является композицией всех сопряженний E над K.*

Доказательство. Для начала композиция является алгебраическим расширением, так как она по построению будет вложена в $\overline{K}$

Пусть $N \subseteq \overline{K}$ – наименьшее нормальное поле над K, включающее в себя E, тогда если поле E_i сопряжено с E, то существует σ – K-автоморфизм $\overline{K}$, что $\sigma(E) = E_i$, но так как N – нормальное поле и $E \subseteq N$, то $\sigma(E) = E_i \subseteq N$, следовательно N содержит в себе все сопряжения над K с E, но тогда по утверждению 1.4 N автоматически содержит и композицию всех сопряжений с E.

Теперь покажем, что композиция всех сопряжений с E это нормальное расширение K.

Пусть E_i это некоторое сопряжение с E, тогда существует некоторый τ – K-автоморфизм $\overline{K}$, что $\tau(E) = E_i$, тогда если σ это произвольный K-автоморфизм $\overline{K}$, то $\sigma(E_i) = (\sigma\tau)(E)$, но $\sigma\tau$ это тоже K-автоморфизм $\overline{K}$, тогда $\sigma(E_i)$ это тоже какое-то сопряжение с E, тогда если $\alpha \in \bigcup_{i\in I} E_i$, где мы проиндексировали все возможные сопряжения E и объединили их, то и $\sigma(\alpha) \in \bigcup_{i\in I} E_i$, для произвольного K-автоморфизма $\overline{K}$.

Тогда так как каждый элемент геннерирующего множества композиции остается принадлежать ему же после применения произвольного K-автоморфизма $\overline{K}$, то композиция является нормальной. (Вспомним как выглядят элементы композиции из 1.4).

Таким образом композиция всех сопряжений включена в любое нормальное над K расширение, содержащее в себе E, а так же сама является нормальным расширением K, а следовательно равна N по определению. □

Утверждение 6.10. *Любое конечное (сепарабельное, конечное и сепарабельное) расширение K содержится в конечном (сепарабельном, конечном и сепарабельном) нормальном расширении K.*

Доказательство. Пусть $K \subseteq E \subseteq \overline{K}$

Будем называть N наименьшее нормальное расширение K, содержащее E, которое по 6.9 есть композиция всех сопряжений E над K.

$K \subseteq E \subseteq N \subseteq \overline{K}$

Для начала покажем для конечного расширения.

Если $[E : K] = n < \infty$, то тогда и $[E : K]_s \leq [E : K] = n$, а следовательно у нас есть конечное число ограничений K-автоморфизмов $\overline{K}$ на E, а следовательно и конечное число сопряжений с E над K, каждый из которых конечно порожден над K, так как базис E над K под действием K-автоморфизма $\overline{K}$ переходит в базис сопряжения.

А так как конечная композиция конечных расширений K есть конечное расширение K по 2.12,
то $[N : K] < \infty$.

В то же время, если E – сепарабельное расширение, то если σ – K-автоморфизм $\overline{K}$, то для любого $\alpha \in E$ верно, что $\mathrm{Irr}(\alpha : K) = \mathrm{Irr}(\sigma(\alpha) : K)$ и тогда сопряжение E тоже является сепарабельным расширением K и тогда N это композиция всех сопряжений E, а композиция сепарабельных расширений является сепарабельным расширением по 4.12.

Для конечного и сепарабельного надо скомбинировать эти 2 факта. □

Утверждение 6.11. *Если $E \subseteq \overline{K}$ это нормальное расширение K, то*

$$F = \left\{ \alpha \in E \mid \sigma(\alpha) = \alpha \text{ для любого } K\text{-автоморфизма } \overline{K} \right\}$$

есть чисто несепарабельное расширение K, а E – сепарабельное расширение F.

Доказательство. Для начала покажем, что F это подполе E, содержащее K.

Так как для любого K–автоморфизма $\overline{K}$ по определению любой элемент K отображается в себя, то $K \subseteq F$ и в частности $0, 1 \in F$.

Теперь пусть $\alpha, \beta \in F, \beta \neq 0$, тогда пусть σ – произвольный K–автоморфизм $\overline{K}$.

$\sigma(\alpha - \beta) = \sigma(\alpha) - \sigma(\beta) = \alpha - \beta \in F$

$\sigma(\alpha\beta^{-1}) = \sigma(\alpha)\sigma(\beta)^{-1} = \alpha\beta^{-1} \in F$, тогда действительно подполе.

Теперь $K \subseteq F \subseteq E \subseteq \overline{K}$, покажем, что $[F : K]_s = 1$ по утверждению 5.4 это будет означать, что F – чисто несепарабельное расширение K.

Пусть $\varphi : F \to \overline{K}$ – произвольный K-гомоморфизм, тогда по 3.6 его можно продлить до $\sigma : \overline{K} \to \overline{K}$ – K-автоморфизма.

Но тогда по определению F верно, что $\varphi = \sigma|_F = \mathrm{id}$, следовательно любой K-гомоморфизм из F в $\overline{K}$ действует тождественно и тогда $[F : K]_s = 1$.

Теперь покажем, что произвольный элемент $\alpha \in E$ – сепарабелен над F, поскольку E – нормальное K, то согласно утверждениям 6.4, 6.3 верно, что E содержит все сопряженные с α элементы $\alpha_1, \ldots, \alpha_n$, которые

по совместительству являются корнями минимального многочлена $\mathrm{Irr}(\alpha : K)$ (и поэтому их конечное число). Условимся считать, что $\alpha_1 = \alpha$, в силу того, что $\mathrm{id} : \overline{K} \to \overline{K}$ это K-автоморфизм K. Рассмотрим многочлен $f(x) = (x - \alpha_1) \dots (x - \alpha_n) \in E[x]$. В силу того, что $\alpha_1 = \alpha$, то $f(\alpha) = 0$.

Теперь так же заметим, что для K-автоморфизма $\sigma : \overline{K} \to \overline{K}$ верно, что $\sigma(\alpha_i) = (\sigma\tau)(\alpha)$, где τ – K-автоморфизм $\overline{K}$ (так можно так как α сопряжено с α_i), тогда так как $\sigma\tau$ тоже K-автоморфизм, то $\sigma(\alpha_i)$ тоже сопряжено с α. Так же в силу того, что у нас σ это инъекция, то $\sigma(\alpha_i) = \sigma(\alpha_j) \Leftrightarrow i = j$.

Таким образом, $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ это n различных сопряженных с α элементов, а всего у нас n сопряжений, тогда $\{\sigma(\alpha_1), \dots, \sigma(\alpha_n)\} = \{\alpha_1, \dots, \alpha_n\}$, следовательно произвольный K-автоморфизм $\overline{K}$, просто переставляет местами сопряженные с α элементы.

Тогда ${}^{\sigma}f(x) = {}^{\sigma}((x - \alpha_1) \dots (x - \alpha_n)) = (x - \sigma(\alpha_1)) \dots (x - \sigma(\alpha_n)) = (x - \alpha_1) \dots (x - \alpha_n) = f(x)$, где σ – произвольный K-автоморфизм.

Тогда можно сделать вывод, что для коэффициента a_i из $f(x)$ верно, что $\sigma(a_i) = a_i$ для любого K-автоморфизма $\overline{K}$. Тогда $f(x) \in F[x]$ по определению F, тогда $\mathrm{Irr}(\alpha : F) \,|\, f(x)$. Но так как $f(x)$ является сепарабельным многочленом по построению, то и $\mathrm{Irr}(\alpha : F)$ тоже сепарабелен по 4.2. Следовательно, произвольный элемент $\alpha \in E$ является сепарабельным над F, а следовательно и все расширение E является сепарабельным над F. □

6.5 Совершенные поля

Посмотрим на этот приятный пример полей, при изучении которых используется теория нормальных и чисто несепарабельных полей.

Определение 6.6. *Поле K называется совершенным, если оно имеет характеристику ноль или же имеет характеристику $p > 0$ и у любого элемента K есть корень степени p.*

Утверждение 6.12. *Конечные и алгебраически замкнутые поля являются совершенными.*

Доказательство. Если поле алгебраически замкнуто, что там вообще любой многочлен вида $x^n - a$ имеет решение, а значит есть и корень любой степени, поэтому оно совершенно.

Если же поле K конечно, то его характеристика равна p и автоморфизм Фробениуса $x \mapsto x^p$ является сюръективным, а следовательно, для любого $x \in K$, существует $y \in K$, что $y^p = x$. □

Лемма 6.13. *У совершенного поля K нет нетривиального чисто несепарабельного расширения.*

Доказательство. Если поле характеристики 0, то тут нечего обсуждать. Поэтому $\mathrm{char}\, K = p > 0$. Тогда поймем, что если у u есть корень v степени p^m, то он единственный, так как $x^{p^m} - u = x^{p^m} - v^{p^m} = (x - v)^{p^m}$.

Теперь пусть E – чисто несепарабельное расширение K, тогда по 5.4 верно, что для любого $\alpha \in E$, верно, что $\alpha^{p^n} = a \in K, n \geq 0$, но тогда, нетрудно вывести по индукции из существования корня степени p в K для любого элемента K, существование корня степени p^n (это корень степени p от корня степени p^{n-1}), тогда для $a \in K$, существует $\beta \in K$, что $\beta^{p^n} = a$, но из единственности корня степени p^n следует, что $\alpha = \beta \in K$, тогда если E это чисто несепарабельное расширение K, то $E = K$. □

Утверждение 6.14. *Любое алгебраическое расширение совершенного поля K является сепарабельным.*

Доказательство. Пусть $E \subseteq \overline{K}$, тогда по 6.9 верно, что это расширение содержится в некотором нормальном расширении $N \subseteq \overline{K}$ и тогда, $K \subseteq F \subseteq N$, где F – чисто несепарабельное расширение K, а N – сепарабельное расширение F, но так как K – совершенное поле, то по лемме выше, $F = K$, следовательно N – сепарабельное расширение K, тогда $K \subseteq E \subseteq N$, и E – сепарабельное расширение K. □

Утверждение 6.15. *Любое алгебраическое расширение E совершенного поля K является совершенным.*

Доказательство. Если поле характеристики 0, то опять же нечего доказывать, поэтому пусть характеристика равна $p > 0$, Любой элемент $\alpha \in E$ лежит в некотором конечном расширении $K \subset K(\alpha) \subset E$. Поэтому покажем, что любое конечное расширение является совершенным, и тогда в $K(\alpha) \subset E$ есть корень степени p для α.

Поэтому пусть $[F : K] < \infty$, и поле K является совершенным.

$e_1, \dots, e_n$ – базис F над K, покажем, что $e_1^p, \dots, e_n^p$ это линейно независимая система, в силу равенства размерностей это будет достаточно, для того, чтобы показать, что это базис.

Пусть $\beta_1 e_1^p + \dots \beta_n e_n^p = 0, \beta_i \in K$, в силу того, что у нас совершенное поле, существует $\alpha_i \in K$, что $\alpha_i^p = \beta_i$, тогда $\beta_1 e_1^p + \dots \beta_n e_n^p = (\alpha_1 e_1 + \dots + \alpha_n e_n)^p = 0 \Leftrightarrow \alpha_1 e_1 + \dots + \alpha_n e_n = 0$, но $e_1, \dots e_n$ – линейно независимы, следовательно $\alpha_i = \beta_i = 0$, тогда и $e_1^p, \dots, e_n^p$ линейно независимы, а следовательно являются базисом.

Пусть $b \in F$ произвольный элемент равный $b = \beta_1 e_1^p + \ldots + \beta_n e_n^p$, в силу совершенности есть $\alpha_i \in K$, что $\alpha_i^p = \beta_i$ и тогда $a = \alpha_1 e_1 + \ldots + \alpha_n e_n$ и $a^p = (\alpha_1 e_1 + \ldots + \alpha_n e_n)^p = \beta_1 e_1^p + \ldots + \beta_n e_n^p = b$.

Вот так вот 2 разных базиса облегчили нам задачу сильно)

Таким образом, из совершенности конечного расширения следует совершенность алгебраического расширения, что мы и хотели. □

Хочется отметить, что поле разложения любого многочлена является конечным расширением изначального поля. Если изначальное поле было совершенным, то полученное расширение является сепарабельным и совершенным, но тогда в совершенном полем нет несепарабельного неприводимого многочлена, так как такой неприводимый многочлен будет с точностью до умножения на коэффициент поля, минимальным многочленом для какого-то элемента поля разложения, а оно сепарабельное.

Тогда в частности, над конечным полем нет неприводимых многочленов.

7 Расширения Галуа

7.1 Определение и базовые свойства

Определение 7.1. *Расширение Галуа поля K есть нормальное и сепарабельное расширение E над K.*

Например, любое нормальное расширение поля характеристики 0 является сепарабельным. Любое конечное поле, является расширением $\mathbb{Z}_p$ и полем разложения $f(x) = x^{p^n} - x$, а следовательно – нормальным полем, сепарабельность в свою очередь следует из того, что $\mathbb{Z}_p$ – совершенное поле, а у нас его алгебраическое расширение.

Теперь рассмотрим некоторые свойства расширений Галуа, которые следуют из нормальности и сепарабельности расширения.

Утверждение 7.1. *Если F – расширение Галуа над K и $K \subseteq E \subseteq F$, то F – расширение Галуа над E.*

Утверждение 7.2. *Если F – расширение Галуа над K, $K \subseteq E \subseteq F$ и и E – нормальное расширение K, то E – расширение Галуа над K.*

Утверждение 7.3. *Если E это расширение Галуа над K и существует композиция EF, то EF – расширение Галуа над KF.*

Утверждение 7.4. *Любая композиция расширений Галуа над K является расширением Галуа над K.*

Утверждение 7.5. *Любое пересечение расширений Галуа над K $E \subseteq \overline{K}$ является расширением Галуа над K.*

7.2 Основная теорема Теории Галуа

Определение 7.2. *Группа Галуа* $\mathrm{Gal}(E : K)$ *расширения Галуа E поля K, так же называемая группа Галуа E над K, есть группа всех K-автоморфизмов E.*

Для примера, группа Галуа $\mathbb{C} = \overline{\mathbb{R}}$ (поэтому нормальна, а сепарабельна по нулевой характеристике) над $\mathbb{R}$ состоит из двух элементов, так как $\sigma(i)^2 + 1 = \sigma(i^2 + 1) = 0, \sigma(i) = \pm i$.

Теперь посмотрим на размерность группы Галуа.

Утверждение 7.6. *Если E это конечное расширение Галуа над K, то* $|\mathrm{Gal}(E : K)| = [E : K]$

Доказательство. В силу сепарабельности E над K, верно, что $[E : K] = [E : K]_s$, воспользуемся этим.

Для начала выберем такое алгебраическое замыкание, что $K \subseteq E \subseteq \overline{K}$.

Тогда любой K-автоморфизм E $\varphi : E \to E \subseteq \overline{K}$, является K-гомоморфизмом в $\overline{K}$, а следовательно $|\mathrm{Gal}(E : K)| \leq [E : K]_s$.

С другой стороны, если $\psi : E \to \overline{K}$ это произвольный K-гомоморфизм, то $\psi(E) = E$ (из-за нормальности над K по утверждению 6.2), тогда $\psi : E \to E$ это K-автоморфизм E (сюръективность есть из того, что выше, а инъективность из того, что у нас гомоморфизм полей.)

Тогда получается, что каждый K-гомоморфизм E в $\overline{K}$ это K-автоморфизм E, тогда

$[E : K]_s \leq |\mathrm{Gal}(E : K)| \Rightarrow |\mathrm{Gal}(E : K)| = [E : K]_s = [E : K]$

Просто следует из того, что для выбранного нами замыкания любой K-гомоморфизм E в $\overline{K}$ это K-автоморфизм E и наоборот. □

Определение 7.3. *Пусть E это поле и G – группа автоморфизмов E.*

Тогда фиксированное поле G это $\mathrm{Fix}_E(G) = \{\alpha \in E \,|\, \forall \sigma \in G : \sigma(\alpha) = \alpha\}$

Я не хочу доказывать, что $\mathrm{Fix}_E(G)$ это подполе E, это достаточно очевидно и проверяется руками. Перейдем к содержательному утверждению.

Утверждение 7.7. *Если G это конечная группа автоморфизмов поля E, то E это конечное расширение Галуа над $F = \mathrm{Fix}_E(G)$ и $\mathrm{Gal}(E : F) = G$.*

Доказательство. $G = \{\sigma_1, \dots, \sigma_n\}$

Покажем, что E является сепарабельным расширением F.

Пусть $\alpha \in E$, рассмотрим $G\alpha = \{\sigma\alpha \in E \,|\, \sigma \in G\} = \{\alpha_1, \dots, \alpha_m\}$ Конечность, в силу того, что $|G| < \infty$, так как $\mathrm{id} \in G$, договоримся, что $\alpha_1 = \alpha$

Поэтому теперь рассмотрим многочлен $f_\alpha(x) = (x - \alpha_1) \dots (x - \alpha_m) \in E[x]$ – сепарабельный многочлен, $f_\alpha(\alpha) = 0$.

Теперь для любого $\sigma \in G$, верно что $\sigma(\alpha_i) = (\sigma\tau)(\alpha), \tau \in G$, так как $\alpha_i \in G\alpha$, но при этом же $\sigma\tau \in G$, а следовательно $\sigma(\alpha_i) \in G\alpha$, причем в силу того, что у нас автоморфизм E, то $\sigma(\alpha_i) = \sigma(\alpha_j) \Leftrightarrow i = j$, а следовательно $\{\sigma(\alpha_1), \dots, \sigma(\alpha_m)\} = \{\alpha_1, \dots, \alpha_m\}$, в силу равенства размерностей и того, что $\sigma(\alpha_i) \in G\alpha$, тогда для $\sigma \in G$, верно что ${}^\sigma f_\alpha(x) = {}^\sigma((x-\alpha_1) \dots (x-\alpha_m)) = (x-\sigma(\alpha_1)) \dots (x-\sigma(\alpha_m)) = (x-\alpha_1) \dots (x-\alpha_m) = f_\alpha(x)$, следовательно, каждый коэффициент $f_\alpha(x)$ остается неподвижным, при действии произвольного $\sigma \in G$, тогда $f_\alpha(x) \in F[x]$, тогда $\mathrm{Irr}(\alpha : F) \,|\, f_\alpha(x)$ тогда в силу 4.2 $\mathrm{Irr}(\alpha : F)$ тоже сепарабельный многочлен ($f_a(x)$ раскладывается на линейные множители в E, а следовательно и $\mathrm{Irr}(\alpha : F)$, а все множители $f_\alpha(x)$ различны по построению) и тогда элемент $\alpha \in E$ сепарабелен над F, а E – сепарабельное расширение F.

Теперь покажем нормальность E над F, пусть $F \subseteq E \subseteq \overline{F}$ и $\varphi : E \to \overline{F}$ – произвольный F-гомоморфизм. $\alpha \in E$, тогда $q(x) = \mathrm{Irr}(\alpha : F)$ и тогда $q(\varphi(\alpha)) = \varphi(q(\alpha)) = 0$, следовательно, $\varphi(\alpha)$ – корень $q(x)$ в $\overline{F}$, но $q(x) | f_\alpha(x)$ как было видно выше, но $f_\alpha(x)$ по построению раскладывается на линейные множители в E, а следовательно, и $q(x)$, тогда все возможные корни $q(x)$ в $\overline{F}$ лежат в E, и тогда и $\varphi(\alpha) \in E$, итого $\varphi(E) \subset E$, а следовательно, E – нормальное расширение F.

Конечность над F согласно утверждению 4.14 следует из того, что E – сепарабельное расширение F, а так же из того, что для любого $\alpha \in E$, верно:

$\deg \mathrm{Irr}(\alpha : F) \leq \deg f_\alpha(x) \leq |G|$.

Тогда так же из того же утверждения, следует, что $[E : F] \leq |G|$

Таким образом, мы показали, что E – конечное расширение Галуа над F. Осталось показать, что $\mathrm{Gal}(E : F) = G$, для начала любой элемент $\sigma \in G$ является F-автоморфизмом E по определению F и тогда $G \subseteq \mathrm{Gal}(E : F)$, но с другой стороны (по 7.6) $|\mathrm{Gal}(E : F)| = [E : F] \leq |G|$, тогда $|\mathrm{Gal}(E : F)| = |G| \Rightarrow$ $\mathrm{Gal}(E : F) = G$ (в силу конечности). □

Утверждение 7.8. *Если E это расширение Галуа над K, то тогда $F = \mathrm{Fix}_E(\mathrm{Gal}(E : K)) = K$.*

Доказательство. Для начала любой элемент $\mathrm{Gal}(E : K)$ это K-автоморфизм, то $K \subset F$, любой элемент K остается на месте.

Теперь пусть $\alpha \in F$, рассмотрим такое алгебраическое замыкание $K \subseteq K(\alpha) \subseteq E \subseteq \overline{K}$.

Тогда пусть $\varphi : K(\alpha) \to \overline{K}, \varphi|_K = \mathrm{id}$, тогда так как E – алгебраическое расширение $K(\alpha)$, то существует продолжение φ, $\tau : E \to \overline{K}$, но так как E – нормальное поле, а перед нами K-гомоморфизм, что $\tau(E) = E$ и тогда τ – K-автоморфизм E, $\tau \in \mathrm{Gal}(E : K)$. Следовательно, если $\alpha \in F$, то $\varphi(\alpha) = \tau(\alpha) = \alpha$, и тогда, так как φ определялось только тем, куда бьет α, то $\varphi = \mathrm{id}$. Получаем, что $[K(\alpha) : K]_s = 1$, но так как E – сепарабельное расширение K, то и $K(\alpha)$ – сепарабельное расширение K, у нас конечное расширение (α алгебраичен), следовательно, верно утверждение 4.7 и $[K(\alpha) : K] = [K(\alpha) : K]_s = 1$, $K(\alpha) = K, \alpha \in K, F \subset K$.

Итого, $K = F$. □

Теперь из утверждений 7.7, 7.8, следует следующая фундаментальная теорема.

Теорема 7.9. *Пусть E – конечное расширение Галуа над K.*

Если F – это подполе E, содержащее K, то E это конечное расширение Галуа над F и F это фиксированное поле $\mathrm{Gal}(E : F)$.

Если H – это подгруппа $\mathrm{Gal}(E : K)$, *то тогда $F = \mathrm{Fix}_E(G)$ это подполе E, содержащее K и* $\mathrm{Gal}(E : F) = H$.

Это задает биекцию, между множеством промежуточных полей между F и E и подгруппами группы $\mathrm{Gal}(E : K)$.

Доказательство. Пусть $\mathfrak{F}$ – множество промежуточных полей между K и E, а $\mathfrak{H}$ – множество подгрупп $\mathrm{Gal}(E:K)$.

Теперь рассмотрим функции $\Phi:\mathfrak{F}\to\mathfrak{H}, F\mapsto \mathrm{Gal}(E:F)$, $\Psi:\mathfrak{H}\to\mathfrak{F}, H\mapsto \mathrm{Fix}_E(H)$.

Для начала покажем, что Ψ отображает подгруппу $H\subseteq \mathrm{Gal}(E:K)$ в подполе E содержащее K, причем такое, что $\mathrm{Gal}(E:\mathrm{Fix}_E(H))=H$.

$H\mapsto \mathrm{Fix}_E(H)=F$, так как все элементы H являются K-автоморфизмами E, то $K\subseteq F$, тогда $K\subseteq F\subseteq E$, согласно 7.7 и тому, что $|H|\leq|\mathrm{Gal}(E:K)|=[E:K]<\infty$ по условию, верно, что E – конечное расширение Галуа над F и $\mathrm{Gal}(E:F)=H$.

Теперь покажем, что Φ работает корректно. $K\subseteq F\subseteq E$ (из того, что E конечное расширение Галуа над K следует, что E – конечное расширение Галуа над F.) тогда $F\mapsto \mathrm{Gal}(E:F)\subseteq\mathrm{Gal}(E:K)$, а то что $F=\mathrm{Fix}_E(\mathrm{Gal}(E:F))$ следует из утверждения 7.8.

Теперь покажем, что Φ и Ψ это обратные друг для друга функции.

Посмотрим на $\Phi\circ\Psi$, $H\in\mathfrak{H}$, $H\overset{\Psi}{\mapsto}\mathrm{Fix}_E(H)\overset{\Phi}{\mapsto}\mathrm{Gal}(E:\mathrm{Fix}_E(H))$. $\mathrm{Gal}(E:\mathrm{Fix}_E(H))=H$, в силу конечности H и утверждению 7.7.

Теперь настало время $\Psi\circ\Phi$, пусть $F\in\mathfrak{F}$, тогда $F\overset{\Phi}{\mapsto}\mathrm{Gal}(E:F)\overset{\Psi}{\mapsto}\mathrm{Fix}_E(\mathrm{Gal}(E:F))$, но $\mathrm{Fix}_E(\mathrm{Gal}(E:F))=F$ по утверждению 7.8.

Таким образом, верно, что $\Phi^{-1}=\Psi$, а так же те условия на функции, которые были описаны в условии теоремы. Они следуют из двух ранее доказанных утверждений. □

7.3 Менее очевидные свойства расширений Галуа

Утверждение 7.10. *Пусть E это конечное расширение Галуа, F_1,F_2,F_3 это промежуточные поля между E и K, а H_1,H_2,H_3 это соответствующие им согласно 7.9 подгруппы* $\mathrm{Gal}(E:K)$. *Тогда верно следующее:*

1. $F_1\subseteq F_2\Leftrightarrow H_1\supseteq H_2$.
2. $F_1=F_2F_3\Leftrightarrow H_1=H_2\cap H_3$.
3. $F_1=F_2\cap F_3\Leftrightarrow H_1$ *это подгруппа сгенерированная* $H_2\cup H_3$
4. *Если* $E\subset\overline{K}$, *то* F_1 *и* F_2 *сопряжены над* K *тогда и только тогда* H_1 *и* H_2 *сопряжены в* $\mathrm{Gal}(E:K)$.

Доказательство. Для начала, общее напоминание из 7.9, что $H_i=\mathrm{Gal}(E:F_i), F_i=\mathrm{Fix}_E(H_i)$.

1. $\Rightarrow$, если σ это F_2-автоморфизм E, то в силу того, что $F_1\subseteq F_2$, то для $k\in F_1$, верно, что $\sigma(k)=k$, тогда σ это F_1-автоморфизм E, а следовательно $\sigma\in H_1,H_2\subseteq H_1$.

$\Leftarrow$, если $u\in F_1=\mathrm{Fix}_E(H_1)$, то для $\sigma\in H_2\subseteq H_1,\sigma(u)=u$, тогда $u\in\mathrm{Fix}_E(H_2)=F_2$.

2.

Отдельно отмечу, что F_i это алгебраическое расширение K, тогда любой элемент $u\in F_iF_j$ принадлежит $K(\alpha_1,\ldots,\alpha_n),\alpha_i\in F_2\cup F_3$, но по 2.6, верно, что $K(\alpha_1,\ldots,\alpha_n)=K[\alpha_1,\ldots,\alpha_n]$, тогда с использованием 1.4 можно сказать, что u, это конечная сумма конечных произведений элементов из $F_2\cup F_3$.

$\Rightarrow$

$F_1=F_2F_3, H_1=\mathrm{Gal}(E:F_2F_3)$, тогда если $\sigma\in H_1$, то в силу того, что $F_2,F_3\subseteq F_2F_3$, то σ это F_3-автоморфизм E и F_2-автоморфизм E, тогда $\sigma\in\mathrm{Gal}(E:F_2)\cap\mathrm{Gal}(E:F_3)=H_2\cap H_3, H_1\subseteq H_2\cap H_3$. Верно, что F_2F_3 состоит из конечных сумм конечных произведений элементов из $F_2\cup F_3$. Тогда если $\sigma\in\mathrm{Gal}(E:F_2)\cap\mathrm{Gal}(E:F_3)=H_2\cap H_3$, то $\sigma(k)=k$ для любого k из $F_2\cup F_3$, тогда используя свойства гомоморфизма, получаем, что $\sigma(u)=u$ для любой конечной суммы конечных произведений элементов из $F_2\cup F_3$, и значит, что для любого элемента F_2F_3, следовательно $\sigma\in\mathrm{Gal}(E:F_2F_3)=H_1, H_1\supseteq H_2\cap H_3$, тогда $H_1=H_2\cap H_3$.

$\Leftarrow$

$F_1=\mathrm{Fix}_E(H_2\cap H_3)$.

Для любого автоморфизма $\sigma\in H_2\cap H_3=\mathrm{Gal}(E:F_2)\cap\mathrm{Gal}(E:F_3)$, верно, что $\sigma(k)=k, k\in F_2\cup F_3$, тогда так как любой элемент $u\in F_2F_3$ это конечная сумма конечных произведений элементов из $F_2\cup F_3$, то $\sigma(u)=u, F_2F_3\subseteq\mathrm{Fix}_E(H_2\cap H_3)=F_1$

Теперь покажем, что $\mathrm{Gal}(E:F_2F_3)\subseteq\mathrm{Gal}(E:\mathrm{Fix}_E(H_2\cap H_3))=H_2\cap H_3$, из этого будет следовать, что $F_2F_3\supseteq\mathrm{Fix}_E(H_2\cap H_3)=F_1$ по ранее доказанному пункту 1.

Если $\sigma\in\mathrm{Gal}(E:F_2F_3)$, то σ это F_2-автоморфизм и F_3-автоморфизм E. Следовательно, $\sigma\in\mathrm{Gal}(E:F_2)\cap\mathrm{Gal}(E:F_3)=H_2\cap H_3$, и тогда необходимое включение на подгруппы доказано, а следовательно, по пункту 1 данного утверждения верно, что $F_2F_3\supseteq F_1\Rightarrow F_2F_3=F_1$.

3.

Отдельно скажу, что подгруппа произвольной группы G, сгенерированная подмножеством $X \subset G$, это такая группа H – множество всех конечных произведений элементов из X и обратных в G к элементам из X. В нашем случае можно считать, что у нас конечное произведение состоящее только из произведений элементов из X, так как в силу того, что X состоит из двух групп, все элементы X содержат в X и обратные к ним, и поэтому не стоит рассматривать обратные отдельно.

Тогда пусть $U = \{\tau_1 \dots \tau_n \,|\, n \in \mathrm{N}, \tau_i \in H_2 \cup H_3\}$

$\Rightarrow$

$H_1 = \mathrm{Gal}(E : F_2 \cap F_3)$, если $\sigma \in U$, то $\sigma = \tau_1 \dots \tau_n, \tau_i \in H_2 \cup H_3$. Но если $u \in F_2 \cap F_3 = \mathrm{Fix}_E(H_2) \cap \mathrm{Fix}_E(H_3)$, то $\tau(u) = u$ для любого $\tau \in H_2 \cup H_3$ (u в фиксированном поле, неважно выберем мы τ из H_2 или из H_3).

Тогда $\sigma(u) = (\tau_1 \dots \tau_n)(u) = u \Rightarrow \sigma \in \mathrm{Gal}(E : F_2 \cap F_3), U \subseteq \mathrm{Gal}(E : F_2 \cap F_3) = H_1$.

В другую сторону воспользуемся уже известным нам приемом, использующим пункт 1.

Покажем, что $\mathrm{Fix}_E(U) \subseteq \mathrm{Fix}_E(\mathrm{Gal}(E : F_2 \cap F_3)) = F_2 \cap F_3$ и получим, что $U \supseteq \mathrm{Gal}(E : F_2 \cap F_3)$.

Если $u \in \mathrm{Fix}_E(U)$, то так как $H_2, H_3 \subseteq U$, то $u \in \mathrm{Fix}_E(H_2) = F_2, u \in \mathrm{Fix}_E(H_3) = F_3$, $u \in F_2 \cap F_3$, что мы и хотели $\mathrm{Fix}_E(U) \subseteq F_2 \cap F_3 \Rightarrow U \supseteq \mathrm{Gal}(E : F_2 \cap F_3)$.

Таким образом, $U = \mathrm{Gal}(E : F_2F_3) = H_1$.

$\Leftarrow$.

$F_1 = \mathrm{Fix}_E(U)$, если $v \in \mathrm{Fix}_E(U)$, то в силу того, что $H_2, H_3 \subseteq U$, то $v \in \mathrm{Fix}_E(H_2) = F_2, v \in \mathrm{Fix}_E(H_3) = F_3 \Rightarrow v \in F_2 \cap F_3, \mathrm{Fix}_E(U) = F_1 \subseteq F_2 \cap F_3$.

$v \in F_2 \cap F_3$, $\sigma \in U, \sigma = \tau_1 \dots \tau_n, \tau_i \in H_2 \cup H_3$, тогда $\tau_i(v) = v$, так как v принадлежит фиксированному полю, как для H_2, так и для H_3, тогда $\sigma(v) = (\tau_1 \dots \tau_n)(v) = v \Rightarrow v \in \mathrm{Fix}_E(U) = F_1 \Rightarrow F_1 \supseteq F_2 \cap F_3$.

Тогда $F_1 = F_2 \cap F_3$.

4.

Напомню, что две подгруппы сопряжены $N_1, N_2 \subseteq G$, если существует $g \in G, gN_1g^{-1} = N_2$

$K \subseteq F_1, F_2 \subseteq E \subseteq \overline{K}$.

$\Rightarrow$

Так как F_1 и F_2 сопряжены, то существует σ – K-автоморфизм $\overline{K}$, что $\sigma(F_1) = F_2$, но можно рассмотреть ограничение $\tau = \sigma|_E$, это K-гомоморфизм из E в $\overline{K}$, но в силу нормальности E над K, $\tau(E) = E$, а следовательно, τ это K-автоморфизм E, $\tau \in \mathrm{Gal}(E : K)$. Теперь $\tau(F_1) = \sigma(F_1) = F_2$.

Покажем, что $\tau^{-1}H_2\tau \subseteq H_1$, если $\chi \in H_2$, то для $u \in F_1$, верно, что $(\tau^{-1}\chi\tau)(u) = (\tau^{-1}\chi)(\tau u) = \tau^{-1}(\tau u) = u$, второе равенство верно, так как $\tau u \in F_2$, тогда действительно $\tau^{-1}\chi\tau \in \mathrm{Gal}(E : F_1) = H_1$.

Так же верно, что $\tau^{-1}\chi\tau = \nu \in H_1 \Leftrightarrow \chi = \tau\nu\tau^{-1} \in \tau H_1\tau^{-1}$, тогда $\tau^{-1}H_2\tau \subseteq H_1 \Leftrightarrow H_2 \subseteq \tau H_1\tau^{-1}$.

Теперь используя то, что $\tau^{-1}(F_2) = F_1$, можно аналогично доказать, что $\tau H_1\tau^{-1} \subseteq H_2$, тогда используя включение выше, получим, что $\tau H_1\tau^{-1} = H_2$, вот и сопряжение.

$\Leftarrow$

Пусть $\tau \in \mathrm{Gal}(E : K)$, и $\tau H_1\tau^{-1} = H_2$.

Покажем, что $\tau F_1 \subseteq F_2$. Пусть $\chi \in H_2$ – произвольный F_2-автоморфизм, тогда $\chi = \tau\nu\tau^{-1}$, $\nu \in \mathrm{Gal}(E : F_1) = H_1$, теперь $u \in F_1$, тогда $\chi(\tau(u)) = (\tau\nu\tau^{-1})(\tau(u)) = (\tau\nu)(u) = \tau(u)$ последнее равенство верно, так как ν – F_1-автоморфизм E, тогда $\tau(u) \in \mathrm{Fix}_E(H_2) = F_2$.

Теперь покажем, что для $v \in F_2, \tau^{-1}(v) \in F_1$, из этого будет следовать обратное включение, что $v = \tau(\tau^{-1}(v)) \in \tau F_1$.

$H_1 = \tau^{-1}H_2\tau$, тогда если $\nu \in H_1$, то $\nu = \tau^{-1}\chi\tau, \chi \in H_2$, поэтому $\nu(\tau^{-1}v) = (\tau^{-1}\chi\tau)(\tau^{-1}v) = (\tau^{-1}\chi)(v) = \tau^{-1}v$, тогда $\tau^{-1}v \in \mathrm{Fix}_E(H_1) = F_1$, тогда $v = \tau(\tau^{-1}v) \in \tau F_1, F_2 \subseteq \tau F_1$.

Итого $\tau F_1 = F_2$, так как $E \subseteq \overline{K}$, то по 3.6, можно продлить τ до σ – K-автоморфизма $\overline{K}$, и тогда $\sigma F_1 = F_2$, то есть F_1 и F_2 сопряжены над K. □

Утверждение 7.11. *Если E это конечное расширение Галуа над K, то тогда промежуточное поле $K \subseteq F \subseteq E$ является нормальным над K тогда и только тогда, когда $\mathrm{Gal}(E : F)$ нормально в $\mathrm{Gal}(E : K)$.*

Если же F нормально над K, то $\mathrm{Gal}(F : K) \simeq \mathrm{Gal}(E : K)/\mathrm{Gal}(E : F)$.

Доказательство. Рассмотрим для удобства замыкание $K \subseteq F \subseteq E \subseteq \overline{K}$.

Из доказательства пункта 4 утверждения 7.10 следует, что для промежуточных полей F_1, F_2, соответствующих им подгрупп $\mathrm{Gal}(E : F_1), \mathrm{Gal}(E : F_2) \subseteq \mathrm{Gal}(E : K)$ и для $\tau \in \mathrm{Gal}(E : K)$, верно, что $\tau F_1 = F_2 \Leftrightarrow \tau\mathrm{Gal}(E : F_1)\tau^{-1} = \mathrm{Gal}(E : F_2)$.

Так же заметим, что F это нормальное расширение K тогда и только тогда, когда $\tau F = F$ для любого $\tau \in \mathrm{Gal}(E : K)$ (для алгебраического замыкания F, содержащего E). Достаточно очевидно, почему верно $\Rightarrow$, в другую же сторону, можно рассмотреть продолжение σ K-гомоморфизма из F в $\overline{K}$ до τ K-гомоморфизма

из E, который будет в силу нормальности E лежать в $\mathrm{Gal}(E:K)$, тогда $\sigma F = \tau F = F$, что и будет давать нормальность.

Тогда F – нормальное расширение $K \Leftrightarrow \forall \tau \in \mathrm{Gal}(E:K) : \tau F = F \Leftrightarrow \forall \tau \in \mathrm{Gal}(E:K) : \tau \mathrm{Gal}(E:F)\tau^{-1} = \mathrm{Gal}(E:F)$, вторая эквивалентность непосредственно следует из доказательства пункта 4 утверждения выше. Так же в данном случае, можно было сказать по-другому, а именно, что количество сопряжений F над K и сопряжений $\mathrm{Gal}(E:F)$ в $\mathrm{Gal}(E:K)$ одинаково, это следует опять же непосредственно из пункта 4 утверждения выше, так как каждое сопряжение поля, дает сопряжение подгруппы, а сопряжение подгруппы дает сопряжение поля. Хорошо, теперь покажем вторую часть.

Рассмотрим отображение $\Phi : \mathrm{Gal}(E:K) \to \mathrm{Gal}(F:K)$, такое что $\sigma \mapsto \sigma|_F$.

Для начала покажем корректность, $\sigma \in \mathrm{Gal}(E:K)$, тогда используя доказанную выше эквивалентность, получаем, что $\sigma F = F$, тогда $\sigma|_F$ это K-автоморфизм F, $\sigma|_F \in \mathrm{Gal}(F:K)$.

Теперь покажем, что это гомоморфизм, пусть $\sigma, \tau \in \mathrm{Gal}(E:K)$, тогда $u \in F$, $(\sigma\tau)|_F(f) = (\sigma\tau)(f)$ (по определению ограничения).

Теперь $(\sigma|_F \tau|_F)(f) = \sigma|_F(\tau(f)) = (\sigma\tau)(f) = (\sigma\tau)|_F(f)$, все хорошо во втором равенстве, так как опять же из доказанной выше эквивалентности следует, что $\tau f \in F$, тогда $\Phi(\sigma\tau) = \Phi(\sigma)\Phi(\tau)$, тогда перед нами гомоморфизм.

Заметим, что он является и сюръективным, так как любой K-автоморфизм F, продляется до K-автоморфизма E по 3.6, тому что $F \subseteq E \subseteq \overline{K}$ и нормальности E над K, а ядро Φ это в точности $\mathrm{Gal}(E:F)$.

Тогда по теореме о гомоморфизме $\mathrm{Gal}(F:K) \simeq \mathrm{Gal}(E:K)/\mathrm{Gal}(E:F)$. □

Утверждение 7.12. *Если E это конечное расширение Галуа над K, то для промежуточного поля $K \subseteq F \subseteq E$ $[\mathrm{Gal}(E:K) : \mathrm{Gal}(E:F)] = [F:K]$.*

Доказательство. Выберем замыкание $K \subseteq F \subseteq E \subseteq \overline{K}$.

Поскольку, E это конечное сепарабельное расширение K, то и F конечное сепарабельное расширение K.

Напомним, что индекс группы по подгруппе это количество смежных классов группы по подгруппе. Пусть $\mathrm{Gal}(E:K)/\mathrm{Gal}(E:F)$ это множество смежных классов $\mathrm{Gal}(E:K)$ по $\mathrm{Gal}(E:F)$, оно необязательно будет факторгруппой. Теперь рассмотрим отображение Ψ бьющее из $\mathrm{Gal}(E:K)/\mathrm{Gal}(E:F)$ в множество K-гомоморфизмов из F в $\overline{K}$, $\tau\mathrm{Gal}(E:F) \mapsto \tau|_F$.

Для начала покажем, что оно корректно, если $\tau\mathrm{Gal}(E:F) = \sigma\mathrm{Gal}(E:F)$, то тогда $\tau = \sigma\chi, \chi \in \mathrm{Gal}(E:F)$, тогда для $f \in F$ $\tau(f) = (\sigma\chi)(f) = \sigma(\chi(f)) = \sigma(f)$, тогда $\sigma|_F = \tau|_F$. Таким образом, отображение определено корректно, так как один и тот же класс бьет в одно и то же ограничение вне зависимости от выбора ведущего элемента класса.

Покажем, что оно инъективно, если $\Psi(\tau\mathrm{Gal}(E:F)) = \tau|_F = \sigma|_F = \Psi(\sigma\mathrm{Gal}(E:F))$, то
$\tau^{-1}\sigma \in \mathrm{Gal}(E:F) \Rightarrow \tau\mathrm{Gal}(E:F) = \sigma\mathrm{Gal}(E:F)$

Теперь покажем, что оно сюръективно, тогда если $\varphi : F \to \overline{K}$, это K-гомоморфизм, тогда так как E это алгебраическое расширение F, то по 3.6 можно продлить φ, до $\tau : E \to \overline{K}$, но в силу нормальности E над K, $\tau(E) = E, \tau \in \mathrm{Gal}(E:K)$, и $\Psi(\tau\mathrm{Gal}(E:F)) = \tau|_F = \varphi$.

Тогда мы показали, что множество смежных классов $\mathrm{Gal}(E:K)$ по $\mathrm{Gal}(E:F)$ находится в биекции с множеством K-гомоморфизмов из F в $\overline{K}$, тогда $[\mathrm{Gal}(E:K) : \mathrm{Gal}(E:F)] = [F:K]_s = [F:K]$, последнее равенство верно, так как F это конечное сепарабельное расширение K. □

8 Многочлены

8.1 Общие сведения

Определение 8.1. *Группа Галуа $\mathrm{Gal}(f:K)$ многочлена $f(x) \in K[x]$ есть группа K-автоморфизмов поля разложения $f(x)$ над K.*

Для удобства остановимся на замыкании $K \subseteq E \subseteq \overline{K}$.

Если $E \subseteq \overline{K}$ это поле разложения $f(x) \in K[x]$, то $E = K(\alpha_1, \ldots, \alpha_n), \alpha_i \in \overline{K}, f(\alpha_i) = 0$.

Тогда E это конечное расширение K, причем еще и нормальное (по 6.2), так как E– поле разложения $f(x)$. Следовательно, любой K-гомоморфизм из E в $\overline{K}$ является K-автоморфизмом E, тогда если $G = \mathrm{Gal}(f:K)$ это группа K-автоморфизмов E, то она же является множеством K-гомоморфизмов из E в $\overline{K}$ и
$|G| = [E:K]_s \leq [E:K] < \infty$.

Тогда по утверждению 7.7 верно, что E это конечное расширение Галуа над $F = \mathrm{Fix}_E(G)$ и $\mathrm{Gal}(f:K) = G = \mathrm{Gal}(E:F)$, поскольку $[E:F] < \infty$, то по утверждению 4.13 верно, что $E = F(\alpha), \alpha \in E$ и тогда E это

поле разложения $\mathrm{Irr}(\alpha : F)$. Во-первых, в силу нормальности E над F $\mathrm{Irr}(\alpha : F)$ раскладывается на линейные множители в E (по 6.2), тогда все корни $\mathrm{Irr}(\alpha : F)$ в $\overline{K}$ лежат в $E = F(\alpha)$. Во-вторых, так как все корни выражаются как $g(\alpha), g(x) \in F[x]$, то можно записать $F(\alpha_1, \ldots, \alpha_n) = F(\alpha)$, где α_i – корень $\mathrm{Irr}(\alpha : F)$ в E и E сгенерировано над F корнями $\mathrm{Irr}(\alpha : F)$ в $\overline{K}$

Следовательно, поле разложения любого многочлена, является полем разложения какого-то неприводимого многочлена в возможно большем поле, а группа Галуа многочлена есть группа Галуа E над каким-то промежуточным полем между E и K.

Если же многочлен $f(x) \in K[x]$ является сепарабельным над K, следовательно, его корни в $\overline{K}$ сепарабельны над K (по 4.2) и тогда $E = K(\alpha_1, \ldots, \alpha_n), f(\alpha_i) = 0$ это конечное и сепарабельное расширение K (по 4.7), но оно так же является и нормальным, так как поле разложения многочлена $f(x)$, а, следовательно, группа K-автоморфизмов E $\mathrm{Gal}(f : K)$ является по определению $\mathrm{Gal}(E : F)$, а поле $F = \mathrm{Fix}_E(G)$ совпадает с K.

Утверждение 8.1. *Пусть $f(x) \in K[x]$ это некоторый многочлен, а $E \subseteq \overline{K}$ это поле разложения $f(x)$ над K. Если $\alpha_1, \ldots, \alpha_n$ это различные корни $f(x)$ в $E \subseteq \overline{K}$, то $\tau \in \mathrm{Gal}(f : K)$, переставляет эти корни, а следовательно $\mathrm{Gal}(f : K)$ изоморфно подгруппе $G \subseteq S_n$.*

Если $f(x)$ это неприводимый и сепарабельный многочлен, то n делит $|G|$ и G это транзитивная подгруппа S_n.

Доказательство. Для начала покажем, что $\tau \in \mathrm{Gal}(f : K)$ (это группа конечна, так как E это конечное расширение над K) переставляет корни $\alpha_1, \ldots, \alpha_n$, $f(\tau(\alpha_i)) = \tau(f(\alpha_i)) = \tau(0) = 0$, это верно, так как перед нами K-автоморфизм E, следовательно $\tau(\alpha_i)$ – корень $f(x)$. Поскольку τ это инъекция, то $\tau(\alpha_i) = \tau(\alpha_j) \Leftrightarrow i = j$, то есть разные корни переходят в разные корни под действием τ, а значит, что τ индуцирует некоторую перестановку корней $\sigma_\tau \in S_n$, такую что $\sigma_\tau(i) = j \Leftrightarrow \tau(\alpha_i) = \alpha_j$.

Теперь рассмотрим отображение $\Phi : \mathrm{Gal}(f : K) \to S_n, \tau \mapsto \sigma_\tau$.

Покажем, что это отображение является гомоморфизмом групп. $\tau, \chi \in \mathrm{Gal}(f : K)$. Пусть $\sigma_{\tau\chi}(i) = j$, то есть $(\tau\chi)(\alpha_i) = \alpha_j$, посмотрим на $(\sigma_\tau\sigma_\chi)(i)$, пусть $\sigma_\chi(i) = m$, тогда $\chi(\alpha_i) = \alpha_m$, а следовательно, $\alpha_j = (\tau\chi)(\alpha_i) = \tau(\chi(\alpha_i)) = \tau(\alpha_m)$, тогда $\sigma_\tau(m) = j$, а следовательно $\sigma_\tau(\sigma_\chi(i)) = \sigma_\tau(m) = j = \sigma_{\tau\chi}(i)$, а следовательно отображение Φ является гомоморфизмом.

Поскольку, $E = K(\alpha_1, \ldots, \alpha_n)$ в силу того, что у нас поле разложения $f(x)$, то если $\Phi(\tau) = \mathrm{id}$, то для $\forall u \in E \quad \tau(u) = u$, так как τ – K-автоморфизм E, любой элемент E есть (по 1.3 и 2.6) конечная линейная комбинация конечных произведений степеней $\alpha_1, \ldots, \alpha_n$ с коэффициентами из K, тогда все α_i и элементы K остаются неизменными, а значит из свойств гомоморфизма следует, что и любой элемент $u \in E$ остается на месте, а следовательно $\tau = \mathrm{id}$. Тогда гомоморфизм является инъективным, а следовательно по теореме о гомоморфизме
$\mathrm{Gal}(f : K) \simeq \mathrm{Im}\,\Phi \subseteq S_n$.

Теперь покажем про вторую часть. Напомним, что подгруппа $G \subseteq S_n$ является транзитивной, если для любого $i, j \in \{1, \ldots, n\}$, верно, что существует $\sigma \in G$, что $\sigma(i) = j$.

Теперь рассмотрим случай с сепарабельным и неприводимым многочленом $f(x)$, будем считать, что этот многочлен является приведенным, так как поле разложения и все его корни от этого не меняются, поле разложения для многочлена $g(x)$ и $g(x)$ умноженного на коэффициент из K одинаковы. Тогда пусть $\alpha_1, \ldots, \alpha_n$ это различные корни $f(x)$, тогда в силу сепарабельности все эти корни имеют степень 1, а в силу неприводимости $f(x) = \mathrm{Irr}(\alpha_i : K)$, тогда $K \subseteq K(\alpha_i) \subseteq E$ и по утверждению 2.2 $[K(\alpha_i) : K] = n = \deg f(x)$. Так же в силу того, что $f(x)$ сепарабельный многочлен, то $\mathrm{Gal}(f : K) = \mathrm{Gal}(E : K)$, так как E– расширение Галуа над K (почему это так было описано выше). Тогда E это также расширение Галуа над $K(\alpha_i)$, по утверждению 7.12 верно, что $[\mathrm{Gal}(E : K) : \mathrm{Gal}(E : K(\alpha_i))] = [K(\alpha_i) : K] = n$, тогда по теореме Лагранжа $|\mathrm{Gal}(E : K)| = [\mathrm{Gal}(E : K) : \mathrm{Gal}(E : K(\alpha_i))] \cdot |\mathrm{Gal}(E : K(\alpha_i))|$, а следовательно $|\mathrm{Gal}(E : K)|$ кратна n, а следовательно и $|\mathrm{Im}\,\Phi|$ кратна n.

Теперь покажем транзитивность, из утверждения 2.4 и того, что $f(x) = \mathrm{Irr}(\alpha_i : K)$ верно, что существует K-гомоморфизм $\varphi_j : K(\alpha_i) \to \overline{K}$, что $\varphi_j(\alpha_i) = \alpha_j, \varphi_j|_K = \mathrm{id}$, но так как E – алгебраическое расширение $K(\alpha_i)$, то по 3.6 можно продлить φ_j до $\tau_j : E \to \overline{K}$, в силу нормальности E и тому, что τ_j это K-гомоморфизм верно, что $\tau_j(E) = E$, и тогда $\tau_j \in \mathrm{Gal}(f : K), \tau_j(\alpha_i) = \varphi_j(\alpha_i) = \alpha_j$ и верно, что $\Phi(\tau_j)(i) = j$. Поскольку мы выбирали i, j произвольно, то $\mathrm{Im}\,\Phi$ это транзитивная подгруппа.

□

В частности из этой теоремы следует, что для неприводимого и сепарабельного многочлена $f(x) \in K[x]$ степени 2, верно, что $\mathrm{Gal}(f : K) \subseteq S_2$, а для многочлена $f(x)$ степени 3, верно, что $\mathrm{Gal}(f : K) \subseteq S_3$ или

$\mathrm{Gal}(f:K) \subseteq A_3$. Напомню, что A_n это группа всех четных перестановок в S_n. A_3 это единственная подгруппа порядка 3 в S_3. Таким образом, нам не очень интересно рассматривать неприводимые и сепарабельные полиномы степени 2 там группа Галуа многочлена всегда изоморфна S_2, поэтому начнем сразу со степени 3.

Так же отдельно заметим, что поскольку отображение Φ инъективно, то каждый $\tau \in \mathrm{Gal}(f:K)$ однозначно определяется тем, куда переходят корни $f(x)$, так же это понятно из того, как выглядят элементы $E = K(\alpha_1, \ldots, \alpha_n)$.

8.2 Полиномы степени 3

Для начала рассмотрим пример поля разложения.

Пусть $f(x) = x^3 - 2$, по критерию Эйзейнштейна (4.17), верно, что этот многочлен неприводим над $\mathbb{Q}$.

Тогда пусть $\rho = \sqrt[3]{2}$, $j = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)$, тогда корни $f(x)$ в $\mathbb{C}$ это $\rho, \rho j, \rho j^2$, тогда $\mathbb{Q}(\rho, \rho j, \rho j^2) = \mathbb{Q}(\rho, j)$, рассмотрим промежуточное поле $\mathbb{Q}(\rho)$, оно не равно $\mathbb{Q}(\rho, j)$, так как $\mathbb{Q}(\rho) \subseteq \mathbb{R}$, а $(j - j^2)^2 = -3$, тогда в силу того, что $f(x) = \mathrm{Irr}(\rho : \mathbb{Q})$, то $[\mathbb{Q}(\rho) : \mathbb{Q}] = 3$, а в силу того, что $j^2 + j + 1 = 0$ и того, что $j \notin \mathbb{Q}(\rho)$, верно, что $[\mathbb{Q}(\rho, j) : \mathbb{Q}(\rho)] = 2$, итого $[\mathbb{Q}(\rho, j) : \mathbb{Q}] = 6$ по 2.1 и тогда, $\mathrm{Gal}(f:K) \simeq S_3$ (используя 8.1 и то, что $f(x)$ неприводим и сепарабелен).

Тогда в $\mathrm{Gal}(f:K)$ есть все возможные перестановки корней многочлена. Поскольку S_3 сгенерировано циклами $(1\,2\,3)$, $(2\,3)$, то $\mathrm{Gal}(f:K)$ сгенерировано K-автоморфизмами E (соответствующими перестановкам) γ, τ , такими, что :

$$\gamma\rho = j\rho, \quad \gamma(j\rho) = j^2\rho, \quad \gamma(j^2\rho) = \rho, \quad \gamma j = j$$

$$\tau\rho = \rho, \quad \tau(j\rho) = j^2\rho, \quad \tau(j^2\rho) = j\rho, \quad \tau j = j^2$$

Тогда $\mathrm{Gal}(f:K) = G = \left\{\mathrm{id}, \gamma, \gamma^2, \tau, \gamma\tau, \gamma^2\tau\right\}$

Перечислим все подгруппы G, согласно теореме Лагранжа их порядок делит $|G|$, поэтому все возможные подгруппы это :

$$1, G, \{1, \tau\}, \{1, \gamma\tau\}, \left\{1, \gamma^2\tau\right\}, \left\{1, \gamma, \gamma^2\right\}$$

По основной теореме Галуа (7.9) верно, что каждой из подгрупп соответствует свое промежуточное подполе, причем оно нормально тогда и только тогда когда нормальна соответствующая подгруппа Галуа.

Теперь возьмемся за перечисление промежуточных подполей между K и F, нетривиальными их них будет только 4 подполя.

Заранее так же отметим, что для промежуточного подполя $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\rho, j)$, верно, что $|\mathrm{Gal}(\mathbb{Q}(\rho, j) : F)| = [\mathbb{Q}(\rho, j) : F]$. Начнем перечисление подполей.

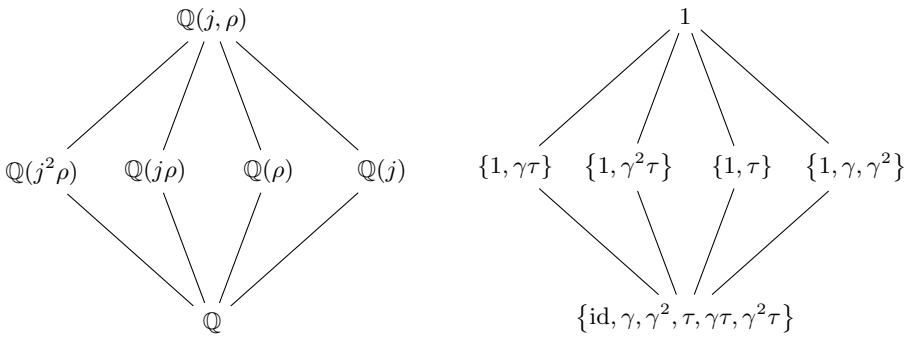
1. Фиксированное поле F для $\{1, \tau\}$ содержит ρ, и при этом, так как $[\mathbb{Q}((\rho, j), F] = 2$, то $[F : \mathbb{Q}] = 3$, $\rho \in F$, тогда $\mathbb{Q}(\rho) \subseteq F$, но $f(x) = \mathrm{Irr}(\rho : \mathbb{Q})$, поэтому $[\mathbb{Q}(\rho) : \mathbb{Q}] = 3$, поэтому $\mathbb{Q}(\rho) = F$, это не нормальное расширение, так как $\gamma^2\tau\gamma = \gamma\tau$.

2. Фиксированное поле F для $\{1, \gamma\tau\}$ содержит $j^2\rho$, по аналогичным объяснениям, что и в пункте 1. $F = \mathbb{Q}(j^2\rho)$ и это не нормальное расширение.

3. Фиксированное поле F для $\left\{1, \gamma^2\tau\right\}$ содержит $j\rho$, по аналогичным объяснениям, что и в пункте 1. $F = \mathbb{Q}(j\rho)$ и это не нормальное расширение.

4. Фиксированное поле F для $\left\{1, \gamma, \gamma^2\right\}$ содержит j, а так же, по причинам описанным в пункте 1., верно, что $[F : \mathbb{Q}] = 2$, тогда $j \notin \mathbb{Q}$ и $x^2 + x + 1 = \mathrm{Irr}(j : \mathbb{Q})$, поэтому $F = \mathbb{Q}(j)$. $\mathbb{Q}(j)$ это нормальное расширение $\mathbb{Q}$, так как $\left\{1, \gamma, \gamma^2\right\} \simeq A_3$, а A_3 нормальна в S_3.

Добавим для приличия красивую картинку, показывающую связь подгрупп и подполей.



Теперь для того, чтобы доказать критерий, когда группа Галуа для неприводимого и сепарабельного многочлена степени 3 изоморфна A_3 рассмотрим такой красивый и элегантный факт.

Определение 8.2. *Пусть $f(x) \in K[x]$, $f(x) = a(x-\alpha_1)\dots(x-\alpha_n), \alpha_i \in \overline{K}$, эти корни необязательно разные. Тогда дискриминант многочлена $f(x)$ это:*

$$D(f) = a^{2n-2} \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2 \in \overline{K}$$

Это вообще говоря, однородный и симметрический многочлен степени $2n-2$ в $K[x]$ от корней многочлена $f(x)$, тогда по теореме Виета и теореме о симметрических многочленах (из курса алгебры четвертого модуля) он выражается через коэффициенты $f(x)$, а следовательно $D(f) \in K$, поэтому теперь перейдем к утверждению.

Утверждение 8.2. *Если $f(x) \in K[x]$ – сепарабельный многочлен и $\operatorname{char} K \neq 2$, то тогда $\mathrm{Gal}(f:K)$ содержит K-автоморфизм, задающий нечетную перестаноку корней $f(x)$ тогда и только тогда, когда $D(f)$ не содержит корня в K.*

Доказательство. Пусть E это поле разложения $f(x)$, оно является расширением Галуа над K, так как $f(x)$ – сепарабельный многочлен, следовательно $\mathrm{Gal}(f:K) = \mathrm{Gal}(E:K)$.

Также пусть $D(f) = d^2, d = a^{n-1}\prod_{1\le i<j\le n}(\alpha_i - \alpha_j) \in E$, d лежит в поле разложения, так как там же лежат и все корни $f(x)$ (это $\alpha_i \in E$), $d \neq 0$ в силу сепарабельности $f(x)$.

Теперь пусть $\tau \in \mathrm{Gal}(E:K)$, тогда $\tau(d) = \mathrm{sgn}(\sigma_\tau)\cdot d$. Это связано с тем, что $\tau(a^{n-1})$ остается на месте, так как τ – K-автоморфизм, в свою очередь количество скобок сменивших знак как раз равно числу инверсий у σ_τ ($i<j$ дает инверсию тогда и только тогда, когда скобка $\alpha_{\sigma_\tau(i)} - \alpha_{\sigma_\tau(j)}$ войдет в $\tau(d)$ со знаком отличным от того, что было в d), если количество инверсий четно, то количество скобок сменивших знак четно и $\tau(d) = d$, если же количество инверсий нечетно, то $\tau(d) = -d \neq d$ в силу характеристики 2.

Итого, $\tau \in \mathrm{Gal}(E:K)$ задает нечетную перестановку тогда и только тогда, когда $\tau(d) = -d$.

Теперь корень $D(f)$ это d или $-d$, тогда наличие квадратного корня в K равносильно тому, что $d \in K$.

А теперь покажем, что в $\mathrm{Gal}(E:K)$ есть автоморфизм задающий нечетную перестановку тогда и только тогда, когда $d \notin K$.

$\Rightarrow$, если $\tau \in \mathrm{Gal}(E:K)$ задает нечетную перестановку, то $\tau(d) = -d \neq d$, следовательно
$d \notin \mathrm{Fix}_E(\mathrm{Gal}(E:K)) = K$.

$\Leftarrow$, если $d \notin K = \mathrm{Fix}_E(\mathrm{Gal}(E:K))$, то существует $\tau \in \mathrm{Gal}(E:K)$, что $\tau(d) \neq d$, но так как d – корень $x^2 - d^2 \in K[x]$, то $\tau(d) = -d$, а следовательно τ задает нечетную перестановку. □

Следствие 8.2.1. *Для неприводимого и сепарабельного многочлена $f(x) \in K[x]$ степени 3* $\mathrm{Gal}(f:K) \simeq S_3$ *тогда и только тогда, когда у $D(f)$ нет корня в K.*

Тут я позволю себе безосновательно сказать, что для многочлена вида $x^3 + px + q$ дискриминант равен $-4p^3 - 27q^2$, это выводится руками из того, как выглядит дискриминант и теоремы о симметрических многочленах.

Докажем мини-лемму.

Лемма 8.3. *Если $f(x) \in \mathbb{Z}[x]$, то если $\frac{v}{u} \in \mathbb{Q}, (v,u) = 1$ это корень $f(x)$, то $v|a_0, u|a_n$.*

Доказательство. $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, тогда $f\left(\frac{v}{u}\right) = a_n \left(\frac{v}{u}\right)^n + a_{n-1}\left(\frac{v}{u}\right)^{n-1} + a_1 \frac{v}{u} + a_0 = 0$, тогда умножая все выражение на u^n получаем $a_n v^n + a_{n-1}v^{n-1}u + \ldots + a_1 v u^{n-1} + a_0 u^n = 0$.

Тогда все выражение делится как на u, так и на v, но все слагаемые кроме при n-го явно содержат u, а следовательно и делятся на u, тогда и коэффициент при n-ом слагаемом делится на u, $u|\,(a_n \cdot v^n)$, но в силу взаимной простоты u и v u должен делить a_n. Аналогично и v делит a_0. □

Поэтому теперь мы перейдем к рассмотрению многочлена $f(x) = x^3 - 3x - 1$, он является неприводимым, так как если бы он был бы приводимым, то у него был бы корень в $\mathbb{Q}$, но тогда он равен $\frac{v}{u}$, и $v|1$, $u|1$, тогда корень равен ± 1, но это не является корнем $f(x)$.

Тогда дискриминантом $f(x)$ является $-4 \cdot (-27) - 27 = 3 \cdot 27 = 9^2$, тогда дискриминант $f(x)$ содержит корень в $\mathbb{Q}$, а следовательно по следствию 8.2.1 верно, что $\mathrm{Gal}(f : \mathbb{Q}) \simeq A_3$.

8.3 Метод нахождения корней многочлена степени 4

Давайте запишем достаточно красивый способ найти корни многочлена степени 4, который связан с характеризацией групп Галуа для многочлена степени 4.

Пусть $f(x) = ax^4 + bx^3 + cx^2 + dx + e \in K[x], a \neq 0$ и характеристика K не равна 2. Для удобства решения сделаем замену в $f(x)$ переменной $x = y - \frac{b}{4a}$, тогда $g(y) = a(y^4 + py^2 + qy + r)$, где $p, q, r \in K$ это некоторые рациональные функции от a, b, c, d, e, эта замена была сделана чтобы сделать коэффициент при y^3 равным нулю.

Тогда если $\alpha_1, \ldots, \alpha_n$ – корни $f(x)$ в $\overline{K}$, тогда $\beta_i = \alpha_i + \frac{b}{4a}$ это корень $g(y)$.

В частности, из-за этой постоянной прибавки для всех корней следует, что $D(f) = D(g)$.

Теперь в $\overline{K}[x]$, верно, что $g(y) = a(y^4 + py^2 + qy + r) = a(y - \beta_1)(y - \beta_2)(y - \beta_3)(y - \beta_4)$, следовательно из теоремы Виета $\sum_{i=1}^4 \beta_i = (-1) \cdot 0 = 0$, $\sum_{1 \leq i < j \leq 4} \beta_i \beta_j = (-1)^2 \cdot p = p$, $\sum_{1 \leq i < j < k \leq 4} \beta_i \beta_j \beta_k = (-1)^3 q = -q$, $\beta_1\beta_2\beta_3\beta_4 = (-1)^4 r = r$.

Теперь рассмотрим такие коэффициенты:

$$u = -(\beta_1 + \beta_2)(\beta_3 + \beta_4) = (\beta_1 + \beta_2)^2$$
$$v = -(\beta_1 + \beta_3)(\beta_2 + \beta_4) = (\beta_1 + \beta_3)^2$$
$$w = -(\beta_1 + \beta_4)(\beta_2 + \beta_3) = (\beta_1 + \beta_4)^2$$

Или что эквивалентно:

$$u = -\left(\alpha_1 + \alpha_2 + \frac{b}{2a}\right)\left(\alpha_3 + \alpha_4 + \frac{b}{2a}\right) = \left(\alpha_1 + \alpha_2 + \frac{b}{2a}\right)^2$$
$$v = -\left(\alpha_1 + \alpha_3 + \frac{b}{2a}\right)\left(\alpha_2 + \alpha_4 + \frac{b}{2a}\right) = \left(\alpha_1 + \alpha_3 + \frac{b}{2a}\right)^2$$
$$w = -\left(\alpha_1 + \alpha_4 + \frac{b}{2a}\right)\left(\alpha_2 + \alpha_3 + \frac{b}{2a}\right) = \left(\alpha_1 + \alpha_4 + \frac{b}{2a}\right)^2$$

Непосредственно руками, при помощи теоремы о симметрических многочленах, проверяется, что :

$$u + v + w = -2p \quad uv + uw + vw = p^2 - 4r \quad uvw = q^2$$

Тогда u, v, w это корни такого многочлена, назовем резольвентой $f(x)$ и $g(y)$:
$s(x) = (x - u)(x - v)(x - w) = x^3 + 2px^2 + (p^2 - 4r)x - q^2 \in K[x]$.
Так же непосредственной проверкой получается, что:

$$u - v = (\beta_1 - \beta_4)(\beta_2 - \beta_3), u - w = (\beta_1 - \beta_3)(\beta_2 - \beta_4), v - w = (\beta_1 - \beta_2)(\beta_3 - \beta_4)$$

Тогда

$$D(s) = (u - v)^2(u - w)^2(v - w)^2 = \sum_{1 \leq i < j \leq 4} (\beta_i - \beta_j)^2, \quad D(f) = D(g) = a^6 D(s)$$

Будем активно использовать теорему Виета далее.

Теперь $u' = \beta_1 + \beta_2, \quad v' = \beta_1 + \beta_3, \quad w' = \beta_1 + \beta_4$ это квардатные корни u, v, w соответственно, а так же $u'v'w' = (\beta_1 + \beta_2)(\beta_1 + \beta_3)(\beta_1 + \beta_4) = \beta_1^3 + \beta_1^2\beta_3 + \beta_1^2\beta_2 + \beta_1\beta_2\beta_3 + \beta_1^2\beta_4 + \beta_1\beta_3\beta_4 + \beta_1\beta_2\beta_4 + \beta_2\beta_3\beta_4 = \beta_1^2\left(\sum_{i=1}^4 \beta_i\right) + \sum_{1\le i<j<k\le 4}\beta_i\beta_j\beta_k = \beta_1^2 \cdot 0 - q = -q$

Так же верно, что $u'+v'+w' = 3\beta_1+\beta_2+\beta_3+\beta_4 = 2\beta_1, \quad u'-v'-w' = \beta_2-\beta_1-\beta_3-\beta_4 = 2\beta_2 \quad -u'+v'-w' = 2\beta_3, -u'-v'+w' = 2\beta_4$.

Итого из всего это, можно вывести следующее утверждение:

Утверждение 8.4. *Если* $\operatorname{char} K \neq 2$ *и* $p, q, r \in K$*, то корни многочлена* $x^4 + px^2 + qx + r$ *в* $\overline{K}$ *это:*

$$\beta_1 = \frac{1}{2}\left(u' + v' + w'\right), \quad \beta_2 = \frac{1}{2}\left(u' - v' - w'\right)$$

$$\beta_3 = \frac{1}{2}\left(-u' + v' - w'\right), \quad \beta_4 = \frac{1}{2}\left(-u' - v' + w'\right)$$

Где $u', v', w' \in \overline{K}$ *это квадратные корни корней* u, v, w *резольвенты* $s(x) = x^3 + 2px^2 + (p^2 - 4r)x - q^2$*, такие что* $u'v'w' = -q$.

Действительно, это верно, потому что корни резольвенты по построению это $\pm(\beta_1+\beta_2), \pm(\beta_1+\beta_3), \pm(\beta_1+\beta_4)$, из того, что мы разобрали выше, если везде $+$, то $u'v'w' = -q$. Тогда если $u'v'w' = -q$, то у нас либо везде $+$, либо $2-$ и $1+$, тогда несложно проверить, что эти же равенства, что и выше работают (просто β_i будет равен β_j, если мы изменим 2 минуса и все будет нормально).

Теперь если характеристика поля не равна $2, 3$, то можно воспользоваться небезызвестными формулами Кардано для нахождения корней из резольвенты, а следовательно и найти корни $f(x)$ выразив их явно, используя формулы выше.

8.4 Описание групп Галуа неприводимых и сепарабельных многочленов степени 4

Для начала выпишу небольшую теорему из теории групп для удобства, она достаточно проста в доказательстве (надо воспользоваться действиями групп), но записывать ее доказательство я не очень хочу.

Определение 8.3. *Пусть* G *это конечная группа, и* $|G| = p^n s, (p, s) = 1$*, тогда силовская* p*-подгруппа, это подгруппа* G *порядка* p^n.

Теорема 8.5 (БД.)**.** *Пусть* G *конечная подгруппа, тогда:*

1. *Силовская* p*-группа существует.*
2. *Всякая* p*-подгруппа лежит в некоторой силовской* p*-подгруппе. Все силовские подгруппы сопряжены.*
3. *Количество силовских* p*-подгрупп* N_p *сравнимо с единицей по модулю* p *(*$N_p \equiv 1 \mod p$*), и делит* s*, где* $|G| = p^n s, (p, s) = 1$.

Теперь собственно запишем интересные нам виды подгрупп D_4 это группа симметрий квадрата ее мощность равна восьми и она силовская 2-подгруппа в S_4, в свою очередь $V_4 \subseteq S_4$ это так называемая четвертая группа Клейна, она равна $V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$ и она нормальна.

Теперь перейдем к теореме.

Теорема 8.6. *Пусть* $f(x) = ax^4 + bx^3 + cx^2 + dx + e \in K[x]$ *это неприводимый и сепарабельный многочлен и* $\operatorname{char} K \neq 2$.

Пусть $F \subseteq \overline{K}$ *это поле разложения его резольвенты. Тогда* $[F : K]$ *делит* 6 *и:*

- *Если* $[F : K] = 6$*, то* $\operatorname{Gal}(f : K) \simeq S_4$.
- *Если* $[F : K] = 3$*, то* $\operatorname{Gal}(f : K) \simeq A_4$.
- *Если* $[F : K] = 2$ *и многочлен* $f(x)$ *неприводим над* F*, то* $\operatorname{Gal}(f : K) \simeq D_4/$
- *Если* $[F : K] = 2$ *и многочлен* $f(x)$ *приводим над* F*, то* $\operatorname{Gal}(f : K) \simeq Z_4$.
- *Если* $[F : K] = 1$*, то* $\operatorname{Gal}(f : K) \simeq V_4$.

Доказательство. Для начала резольвента $s(x)$ многочлена $f(x)$ является сепарабельной, так как $D(s) = D(f)/a^6 \neq 0$ в силу сепарабельности, а тогда корни $s(x)$, $u, v, w \in \overline{K}$ различны.

Пусть $E \subseteq \overline{K}$ и $F = K(u, v, w)$ это поля разложения над K $f(x), s(x)$ соответственно, а следовательно поля Гаула над K.

Согласно утверждению 8.4, верно, что $E = K(u', v', w')$ (корни выражаются через u', v', w', но и u', v', w' выражаются через корни), где u', v', w' это квадратные корни u, v, w причем такие, что $u'v'w' \in K$. Тогда $E = F(u', v')$ (w' можно выразить через как элемент K деленый на $u'v'$, в силу различности корней, можно выбрать так, что $u'v' \neq 0$). Тогда так как $x^2 - u \in F[x]$ зануляет u', и $x^2 - v \in F[x]$ зануляет v, то $[E : F] \leq 4$. В силу того, что $\mathrm{Gal}(s : K) = \mathrm{Gal}(F : K)$ изоморфно подгруппе S_3, то $[F : K] = |\mathrm{Gal}(s : K)|$ и делит 6.

Давайте опишем группу $\sigma \in S_4$ таких, что σ коммутирует со всеми элементами V_4, для этого опишем коммутрирующие с $(12)(34)$, затем обобщим выводы на произвольный элемент V_4, и пересечем множества коммутирующих с каждым элементом из V_4.

Если $\tau(12)(34) = (12)(34)\tau$, то это эквивалетно, тому что $(\tau(1)\tau(2))(\tau(3)\tau(4)) = \tau(12)(34)\tau^{-1} = (12)(34)$, таким, образом, для того, чтобы τ коммутировало с $(12)(34)$ нам необходимо и достаточно, что $\tau\{1, 2\} = \{1, 2\}, \tau\{3, 4\} = \{3, 4\}$ или $\tau\{1, 2\} = \{3, 4\}, \tau\{3, 4\} = \{1, 2\}$, перечислим все возможные варианты:

$$\{1, (12), (12)(34), (34), (13)(24), (1324), (14)(23), (1423)\} = V_4 \cup \{(12), (34), (1324), (1423)\}$$

Тогда аналогично коммутирующие с $(13)(24)$ это:

$$V_4 \cup \{(13), (24), (1234), (1432)\}$$

И для $(14)(23)$

$$V_4 \cup \{(14), (23), (1243), (1342)\}$$

Тогда со всеми элементами из V_4 коммутируют только сами элементы V_4, как пересечение множеств коммутирующих с одним из элементов V_4, то есть $\sigma \in S_4$ коммутирует с любым элементом V_4 тогда и только тогда, когда $\sigma \in V_4$.

Перейдем теперь к теореме. Теперь согласно утверждению 8.1 верно, что $\mathrm{Gal}(f : K) \simeq G \subseteq S_4$, и любой $\tau \in \mathrm{Gal}(f : K)$ переставляет корни $f(x)$ $\alpha_1, \ldots, \alpha_n \in E$ и задает перестановку σ_τ, такую, что $\tau\alpha_i = \alpha_{\sigma_\tau(i)}$. Рассмотрим равенства из уравнений на корни резольвенты:

$$u = -\left(\alpha_1 + \alpha_2 + \frac{b}{2a}\right)\left(\alpha_3 + \alpha_4 + \frac{b}{2a}\right) = \left(\alpha_1 + \alpha_2 + \frac{b}{2a}\right)^2$$

$$v = -\left(\alpha_1 + \alpha_3 + \frac{b}{2a}\right)\left(\alpha_2 + \alpha_4 + \frac{b}{2a}\right) = \left(\alpha_1 + \alpha_3 + \frac{b}{2a}\right)^2$$

$$w = -\left(\alpha_1 + \alpha_4 + \frac{b}{2a}\right)\left(\alpha_2 + \alpha_3 + \frac{b}{2a}\right) = \left(\alpha_1 + \alpha_4 + \frac{b}{2a}\right)^2$$

Из того, что τ переставляет α_i и оставляет на месте элементы K, следует, что τ переставляет и u, v, w.

Теперь если $\sigma_\tau \in V_4$, то $\tau(u) = u, \tau(v) = v, \tau(w) = w$ (проверяется глазами).

В свою очередь, если $\tau(u) = u, \tau(w) = w, \tau(v) = v$, то в силу того, что корни попарно не равны, то из условия $\tau(u) = u$ следует, что в скобках набор α_i должен быть тем же, что и в u (то есть в одной скобке слагаемыми будут α_1, α_2, а во второй α_3, α_4), следовательно $\tau(u) = u$ дает условия $\sigma_\tau\{1, 2\} = \{1, 2\}, \sigma_\tau\{3, 4\} = \{3, 4\}$ или $\sigma_\tau\{1, 2\} = \{3, 4\}, \sigma_\tau\{3, 4\} = \{1, 2\}$, заметим, что это условия коммутирования σ_τ с $(12)(34)$, абсолютно аналогичные условия выводятся из $\tau(v) = v, \tau(w) = w$, то есть условия на коммутирование σ_τ с $(13)(24)$ и $(14)(23)$ соответственно, а следовательно σ_τ коммутирует со всеми элементами V_4, и тогда по тому, что мы доказали выше принадлежит V_4.

Таким образом $\tau \in \mathrm{Gal}(E : F) \subseteq \mathrm{Gal}(E : K)$ тогда и только тогда, когда $\sigma_\tau \in V_4$, а следовательно $\mathrm{Gal}(E : F) \simeq G \cap V_4$. В свою очередь F это расширение Гаула над K, так как поле разложение сепарабельного многочлена $s(x)$, тогда по утверждению 7.11 верно, что $\mathrm{Gal}(F : K) \simeq \mathrm{Gal}(E : K)/\mathrm{Gal}(E : F) \simeq G/(G \cap V_4)$.

Теперь перейдем к уже собственно характеризации групп.

По утверждению 8.1 верно, что $\mathrm{Gal}(f : K) \simeq G \subseteq S_4$, где G это транзитивная подгруппа и ее порядок делится на 4, тогда $|G| = 4, 8, 12, 24$ (так как мощность G делит 24).

Рассмотрим все случаи.

Если $|G| = 24$, тогда $\mathrm{Gal}(f : K) \simeq S_4$ и $[F : K] = 6$, так как $[F : K] \leq 6, [E : F] \leq 4$, нам остается взять по максимуму.

Если $|G| = 12$, то $\mathrm{Gal}(f : K) \simeq A_4$, так как в S_4 есть только одна подгруппа индекса 12 (так как из S_n только один нетривиальный гомоморфизм в $\{-1, 1\}$ – знак перестановки, если бы была другая подгруппа индекса 2, то был бы другой гомоморфизм). Тогда $V_4 \subseteq A_4$, тогда $[F : K] = |\mathrm{Gal}(F : K)| = |A_4/V_4| = 3$.

Если $|G| = 8$, то G это одна из силовских 2-подгрупп в S_4 (по 8.5), и поскольку их количество будет делить 3, и сравнимо с единицей по модулю 2, то их будет ровным счетом 3, мы их нашли выше, и все они изоморфны D_4, так они сопряжены. Еще они содержат V_4, как мы убедились выше и тогда $V_4 \subseteq G$, и $\mathrm{Gal}(F : K) \simeq D_4/V_4$ и $[F : K] = |\mathrm{Gal}(F : K)| = 2$, поскольку $\mathrm{Gal}(E : F) \simeq V_4$ в нашем случае, а V_4 это транзитивная подгруппа S_4, то существуют $\tau \in \mathrm{Gal}(E : F)$, такие, что $\tau(\alpha_1) = \alpha_i, i \in \{1, 2, 3, 4\}$ а следовательно, у многочлена $\mathrm{Irr}(\alpha_1 : F)$ есть 4 разлиных корня (α_i попарно различны, так как f сепарабелен), и тогда $\mathrm{Irr}(\alpha_1 : F)$ равен $f(x)$ с точностью до умножения на коэффициент из F, и тогда $f(x)$ неприводим над F.

Если $|G| = 4$, если $G = V_4$, то тогда $[F : K] = |\mathrm{Gal}(F : K)| = |V_4/V_4| = 1$.

Если же $G = \mathbb{Z}_4$, то G сгенерировано каким-то циклом длины 4, и тогда его пересечение с V_4 имеет мощность 2, тогда $\mathrm{Gal}(F : K) \simeq G/(G \cap V_4)$ и $[F : K] = |\mathrm{Gal}(F : K)| = |G/(G \cap V_4)| = 2$. Так же $\mathrm{Gal}(E : F) \simeq G \cap V$, но если бы многочлен $f(x)$ был бы неприводим над F, то мощность $|\mathrm{Gal}(E : F)|$ была бы кратной четырем, а этого не наблюдается, а следовательно $f(x)$ является приводимым многочленом.

При разборе случая $|G| = 4$ мы разобрали только 2 случая, так как подгруппа порядка p^2 коммутативна (было в алгебре на 4 модуле), а тогда изоморфна либо $\mathbb{Z}_4$, либо $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, это мы и разобрали.

Итого мы разобрали все возможные G, и заметили, что каждая из G однозначно определяет размерность поля разложения резольвенты, а значит рассматривая поле разложения резольвенты, мы $\square$

8.5 Примеры многочленов

Давайте рассмотрим примеры на все группы.

Напомню, что для многочлена вида $x^3 + px + q$ является выражение: $-4p^3 - 27q^2$

Рассмотрим $f(x) = x^4 + 2x + 2$ этот многочлен неприводим по критерию Эйзейнштейна (4.17), его резольвента равна $s(x) = x^3 - 8x - 4$, покажем, что резольвента неприводима. По 8.3, верно, что все возможные корни это $\pm 1, \pm 2, \pm 4$, но они не подходят, тогда $s(x)$ – неприводимый многочлен.

Тогда по тому, что я писал выше, его дискриминант равен $1616 = 101 \cdot 4^2$, он не имеет квадрата в $\mathbb{Q}$, следовательно по 8.2.1, верно, что $\mathrm{Gal}(s : \mathbb{Q}) \simeq S_3$, тогда размерность поля разложения резольвенты над $\mathbb{Q}$ равна 6, и тогда $\mathrm{Gal}(f : K) \simeq S_4$.

Теперь рассмотрим многочлен $f(x) = x^4 + 8x + 12$. Его потенциальные корни это: $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$, они не подходят, поэтому если он неприводим, то по утверждению 4.16.1, верно, что $f(x)$ раскладывется на два многочлена степени 2 в $\mathbb{Z}[x]$, рассматривая его факторизацию в $\mathbb{Z}_5$ (просто перевели все коэффициенты в классы из $\mathbb{Z}_5$, это отображение вполне корректно и сохраняет умножение и сложение, то есть является гомоморфизмом колец многочленов), получаем, что и в нем $f(x)$ раскладывается на два многочлена степени 2 из $\mathbb{Z}_5[x]$, но при этом же: $x^4 + 8x + 12 \simeq (x - 4)(x^3 + 4x^2 + x + 2) \mod 5$, в силу единственности разложения на неприводимые множители в $Z_5[x]$ и того, что у $f(x)$ есть в $\mathbb{Z}_5[x]$ факторизация на 2 многочлена следует то, что в разложении $f(x)$ есть хотя бы 2 линейных множителя, (так как один из степени 2 будет делится на $x - 4$), но это невозможно, так как у $x^3 + 4x^2 + x + 2$ нет корней в $\mathbb{Z}_5$, а следовательно мы получили противоречие, и сам многочлен $f(x)$ не раскладывается в $\mathbb{Q}$ на 2 многочлена степени 2, а следовательно, он неприводим над $\mathbb{Q}$.

Хорошо, тогда его резольвента равна: $x^3 - 48x - 64$, она опять же неприводима, так как у нее нет целых корней (а все корни в $\mathbb{Q}$ у резольвенты целые по 8.3). Но дискриминант резольвенты в нашем случае равен $-4 \cdot (-48)^3 - 27 \cdot 64^2 = 331776 = 576^2$, у дискриминанта есть корень в $\mathbb{Q}$, а, следовательно, $\mathrm{Gal}(s : \mathbb{Q}) \simeq A_3$ по 8.2.1 и тогда $[F : K] = |A_3|$, и тогда $\mathrm{Gal}(f : \mathbb{Q}) \simeq A_4$.

Рассмотрим многочлен $f(x) = x^4 + 4x^2 + 1$, у него рациональных и даже действительных корней, но при этом есть факторизация в $\mathbb{R}[x]$, такая $x^4 + 4x^2 + 1 = (x^2 - \sqrt{3} + 2)(x^2 + \sqrt{3} + 2)$, в силу того в $\mathbb{R}[x]$ единственная факторизация на неприводимые с точностью до умножения на коэффициент, то нет факторизации в $\mathbb{Q}[x]$ (если бы она была, то мы бы получили противоречие, так как взяв старший член в факторах из $\mathbb{Q}[x]$ равным единице мы бы получили другую факторизацию в $\mathbb{Q}[x] \subseteq \mathbb{R}[x]$, что невозможно), тогда $f(x)$ приводим в $\mathbb{R}[x]$, но неприводим в $\mathbb{Q}[x]$, тогда посмотрим на его резольвенту $s(x) = x^3 + 8x^2 + 12x = x(x^2 + 8x + 12) = x(x + 2)(x + 6)$, тогда резольвента раскладывается в $\mathbb{Q}$ на линейные множители, а значит $\mathbb{Q}$ это и есть поле ее разложения, тогда $[F : K] = 1$ и тогда $\mathrm{Gal}(f : K) \simeq V_4$.

Рассмотрим многочлен $f(x) = x^4 - 4x^2 + 2$, он неприводим над $\mathbb{Q}$ по критерию Эйзейнштейна, при этом его резольвента равна $s(x) = x^3 - 8x^2 + 8x = x(x^2 - 8x + 8)$, корни резольвенты это $0, 4 - 2\sqrt{2}, 4 + 2\sqrt{2}$, тогда

поле разложение резольвенты это $\mathbb{Q}(\sqrt{2})$, но в $\mathbb{Q}(\sqrt{2})$ у $f(x)$ есть разложение $f(x) = (x^2 - 2 - \sqrt{2})(x^2 + \sqrt{2} - 2)$, следовательно, по теореме выше $\mathrm{Gal}(f : \mathbb{Q}) \simeq \mathbb{Z}_4$.

Рассмотрим многочлен $f(x) = x^4 + 3x + 3$ он неприводим по критерию Эйзенштейна и его резольвента равна $s(x) = x^3 - 12x - 9 = (x + 3)(x^2 - 3x - 3)$.

Корни резольвенты это -3, $\frac{3 \pm \sqrt{21}}{2}$. Тогда поле разложения $s(x)$ равно $\mathbb{Q}(\sqrt{21})$, у $f(x)$ нет действительных корней, поэтому единственная возможная факторизация $f(x)$ в $\mathbb{Q}(\sqrt{21})$ это на 2 многочлена степени 2.

Проанализируем это случай.

Пусть $x^4 + 3x + 3 = (x^2 + Ax + B)(x^2 + Cx + D)$

Это дает условия:

$$A + C = 0, \quad B + D + AC = 0, \quad AD + BC = 3, \quad BD = 3$$

Тогда $C = -A$, $B + D = A^2$, $A(D - B) = 3$, из последнего получаем, что $A \neq 0$, и тогда $D - B = \frac{3}{A}$, тогда подставляя $D = A^2 - B$, получает $A^2 - 2B = \frac{3}{A}$, следовательно, $B = \frac{A^3 - 3}{2A}$, тогда условие $BD = 3$ дает нам по итогу:

$$3 = BD = \frac{A^3 - 3}{2A}\left(A^2 - \frac{A^3 - 3}{2A}\right) = \frac{A^3 - 3}{2A} \cdot \frac{A^3 + 3}{2A} = \frac{A^6 - 9}{4A^2}$$

Умножая на $4A^2 \neq 0$, получаем $A^6 - 9 = 12A^2 \Rightarrow A^6 - 12A^2 - 9 = 0$, тогда получаем уравнение

$$A^6 - 12A^2 - 9 = (A^2 + 3)(A^4 - 3A^2 - 3) = 0$$

Поскольку $\mathbb{Q}(\sqrt{21}) \subseteq \mathbb{R}$, то $A^2 + 3$ никогда не равно нулю, поэтому осталось рассмотреть $A^4 - 3A^2 - 3$, если рассматривать это как многочлен от A, то он неприводим над $\mathbb{Q}$ по критерию Эйзенштейна, следовательно, он является минимальным многочленом для любого его корня α, но тогда если $\alpha \in \mathbb{Q}(\sqrt{21})$, то $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{21})$, но при этом $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, так как $\deg \mathrm{Irr}(\alpha : \mathbb{Q}) = 4$, но $[\mathbb{Q}(\sqrt{21}) : \mathbb{Q}] = 2$, а размерность подпространства не больше чем размерность самого пространства, следовательно, у $(A^2 + 3)(A^4 - 3A^2 - 3)$ нет корня в $\mathbb{Q}(\sqrt{21})$, а следовательно и нет факторизации, $f(x)$ неприводим над $\mathbb{Q}(\sqrt{21})$, а следовательно $\mathrm{Gal}(f : \mathbb{Q}) \simeq D_4$.