Основы теории Галуа

Конечные расширения полей

Если поле K содержит поле F, то говорят, что K является *расширением* поля F и пишут $K > F$.

Расширение K поля F называется *алгебраическим*, если любой элемент $\alpha \in K$ является корнем многочлена $f(x)$ с коэффициентами из поля F, т.е. $f(\alpha) = 0$, где $f(x) \in F[X]$.

Расширение $K > F$ называется *конечным*, если поле K, рассматриваемое как линейное пространство над F, конечномерно. Размерность K над F принято обозначать $[K : F]$ и называть *степенью расширения.*

Вот несколько простых и важных фактов, касающихся введенных понятий.

$\bullet$Всякое конечное расширение является алгебраическим.

$\bullet\bullet$*Лемма о башне 1.*
Если $K > L > F$ — башня конечных расширений, то $[K : F] = [K : L][L : F]$.
Набросок доказательства. Если $\alpha_1, \dots, \alpha_s$ — базис K над L, а $\mu_1, \dots, \mu_t$ — базис L над F, то $\{\alpha_i \mu_j\}$ — базис K над F.$\square$

$\bullet\bullet\bullet$Расширение $K > F$ называется *простым*, если оно получается присоединением к полю F одного элемента α, алгебраического над F, т.е. $K = F(\alpha)$.

Легко видеть, что любое конечное расширение $K > F$ включается в башню

$$K = K_n > K_{n-1} > \ldots > K_1 > F,$$

где K_{i+1} — простое расширение поля K_i.
Например, можно построить башню так: если $\mu_1, \dots, \mu_n$ — базис K над F, то положим $K_1 = F(\mu_1), K_2 = K_1(\mu_2)$ и т.д.$\square$

Докажем фундаментальную лемму о простом расширении.

Лемма о простом расширении. Пусть $m(x)$ — неприводимый многочлен степени n из кольца $F[X]$, имеющий своим корнем α. Тогда имеется естественный изоморфизм поля $F[X]/(m(x))$ (поле многочленов $\mod m(x)$) и поля $F(\alpha)$. В частности, любой элемент поля $F(\alpha)$ однозначно представим в виде $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$, $a_i \in F$.

Доказательство. Рассмотрим гомоморфизм вычисления $\varphi : F[X] \longrightarrow F(\alpha)$, который каждому многочлену $p(x) \in F[X]$ ставит в соответствие его значение в точке α: $p \mapsto p(\alpha)$. Легко проверить, что ядро этого отображения состоит из многочленов $p(x)$, кратных $m(x)$. Так как многочлен $m(x)$ неприводим, то факторкольцо $F[X] \mod m(x)$ есть поле. По теореме о гомоморфизме образ $\operatorname{Im}\varphi$ есть подполе в $F(\alpha)$, содержащее элемент α. Следовательно, $\operatorname{Im}\varphi = F(\alpha)$. Остается заметить, что каждый элемент из $F[X]/(m(x))$ имеет единственного представителя среди многочленов, степень которых меньше n.$\square$

Следствие. Если $\deg m(x) = n$, то $[F(\alpha) : F] = n$.
Степени $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ составляют базис $F(\alpha)$ над F. $\square$

Пример.
а) Расширение $\mathbb{Q}(\sqrt{2})$ состоит из чисел вида $a+b\sqrt{2}, a, b\in\mathbb{Q}$ (здесь $m(x)=x^2-2$).
б) Расширение $\mathbb{Q}(\sqrt[3]{2})$ степени 3 состоит из чисел вида $a+b\sqrt[3]{2}+c\sqrt[3]{4}$
(здесь $m(x)=x^3-2$).

Замечание. В башне расширений $K>L>F$ (не обязательно конечных) расширение $K>F$ является алгебраическим, если таковы расширения $K>L$ и $L>F$ (очень советую продумать это до конца).

Теория, о которой я хочу немного рассказать, стоит на трех китах. Первый — это полезная интерпретация леммы о простом расширении:

Обозначим через $\overline{F}$ *алгебраическое замыкание* поля F, т.е. поле, образованное присоединением к F корней всех многочленов из $F[X]$.
Замечание. Любопытно отметить, что а) поле $\overline{F}$ алгебраически замкнуто; б) если расширение $K>F$ алгебраично, то $\overline{K}=\overline{F}$. (Почему?)

Так вот, построенный в лемме гомоморфизм φ можно интерпретировать как вложение поля $F[X]/(m(x))$ в поле $\overline{F}$, которое определяется с помощью корня α многочлена $m(x)$. А один из важных вопросов в теории полей звучит так: дано расширение $K>F$; сколько существует различных вложений поля K в $\overline{F}$ над F, т.е. таких гомоморфизмов $\varphi: K\longrightarrow\overline{F}$, что $a^\varphi=a$ для любого $a\in F$?

Предположим, что неприводимый многочлен $m(x)$ имеет m различных корней $(\alpha_1,\dots,\alpha_m)$ в $\overline{F}$. Тогда, как показывает лемма о простом расширении, гомоморфизмы вычисления $\varphi_i : F[X]\longrightarrow\overline{F}$, $p(x)\mapsto p(\alpha_i)$ дают m различных вложений поля $F[X] \bmod m(x)$ в поле $\overline{F}$. Других вложений нет, так как любой гомоморфизм нашего поля в $\overline{F}$ обязан элемент $\overline{x}\equiv x \mod m(x)$ переводить в один из корней α_i. Итак, мы показали, что

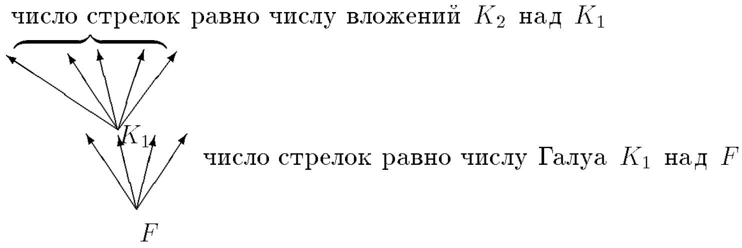
Кит 1. Простое расширение $F(\alpha)>F$, допускает столько различных вложений в поле $\overline{F}$, сколько различных корней в $\overline{F}$ имеет минимальный многочлен $m(x)$ элемента α.

Следствие. Согласно основной теореме алгебры, число вложений K над F в случае простого расширения не превосходит степени $[K:F]$. Это число в точности равно $[K:F]$, если у неприводимого над F многочлена $m(x)$ нет кратных корней. В характеристике 0 это всегда так.

Назовем число различных вложений над F произвольного конечного расширения $K>F$ в поле $\overline{F}$ *числом Галуа K над F*.

Обобщенный Кит 1. Число Галуа K над F не превосходит $[K:F]$.

Схема доказательства показана на картинке, где каждая стрелка i-го этажа представляет вложение K_i в $\overline{F}$ над фиксированным вложением K_{i-1}.



Вложения K над F находятся в биективном соответствии с путями на построенном дереве, ведущими из корня в висячие вершины. Число таких путей равно произведению чисел Галуа K_i над K_{i-1}. Но число Галуа K_i над K_{i-1} не превосходит степени $[K_i : K_{i-1}]$ (Кит 1). В итоге получаем, что число Галуа K над F не превосходит произведения $\prod [K_i : K_{i-1}] = [K : F]$ (лемма о башне). $\square$

Если число Галуа K над F равно $[K : F]$, то расширение называется *сепарабельным.*

Контрольный вопрос. Эквивалентно ли это определение следующему: конечное расширение $K > F$ называется сепарабельным, если минимальный многочлен $m_\alpha(x)$ над F любого элемента $\alpha \in K$ не имеет кратных корней?

Пример. Рассмотрим расширение $K = \mathbb{Q}(\sqrt{2}, \sqrt{-1})$ поля $\mathbb{Q}$. Включим его в башню квадратичных расширений (расширений степени 2)

$$\mathbb{Q}(\sqrt{2}, \sqrt{-1}) > \mathbb{Q}(\sqrt{2}) > \mathbb{Q}.$$

Любой элемент поля K однозначно записывается в виде $\omega = a + b\sqrt{-1}$, где $a, b \in \mathbb{Q}(\sqrt{2})$. Обозначим через τ гомоморфизм $\mathbb{Q}(\sqrt{2}) \longrightarrow \overline{\mathbb{Q}}$, который число $p + q\sqrt{2}$ переводит $p - q\sqrt{2}$, $p, q \in \mathbb{Q}$. Тогда гомоморфизмы

$$\begin{aligned}
&\omega \mapsto \omega \\
&\omega \mapsto a^\tau + b^\tau \sqrt{-1} = \omega^\tau \\
&\omega \mapsto a - b\sqrt{-1} = \overline{\omega} \\
&\omega \mapsto a^\tau - b^\tau \sqrt{-1} = \overline{\omega^\tau}
\end{aligned}$$

определяют четыре вложения поля K в $\overline{\mathbb{Q}}$ над $\mathbb{Q}$.

В дальнейшем нас будет интересовать группа автоморфизмов $Aut(K/F)$ поля K над полем F. Эта группа состоит из автоморфизмов поля K, тождественных на его подполе F. Она называется *группой Галуа* поля K и обозначается $\mathrm{Gal}(K/F)$.

Удобно считать, что все рассматриваемые расширения основного поля F вложены в его алгебраическое замыкание $\overline{F}$.
Так как автоморфизм $\sigma : K \longrightarrow K$ над F является частным случаем вложения K в $\overline{F}$ над F, то как мы уже знаем, порядок группы $\mathrm{Gal}(K/F)$ не превосходит $[K : F]$.

Конечное расширение $K > F$ называется *расширением Галуа*, если порядок его группы Галуа равен $[K : F]$.

Пример. Группа $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ тривиальна (почему?),
а $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{-1})/\mathbb{Q}) = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ (почему?).
Таким образом, расширение $\mathbb{Q}(\sqrt{2}, \sqrt{-1}) > \mathbb{Q}$ — это расширение Галуа,
а расширение $\mathbb{Q}(\sqrt[3]{2}) > \mathbb{Q}$ таковым не является.
Контрольный вопрос. Вычислить группу $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

*Обозначение.*Если G — группа автоморфизмов поля L, то через L^G обозначим подполе в L, состоящее из G-инвариантных элементов.

Кит 2 — это лемма о неподвижном поле.

Лемма о неподвижном поле. Если $K > F$ — расширение Галуа с группой Галуа $G = \mathrm{Gal}(K/F)$, то $K^G = F$.

Доказательство. Предположим, что $K > K^G > F$ и $[K^G : F] > 1$. Но, по определению, группа G является подгруппой группы $\mathrm{Aut}(K/K^G)$. Следовательно, $|G| \leqslant |\,\mathrm{Aut}(K/K^G)| \leqslant [K : K^G] < [K : F]$. С другой стороны, $|G| = [K : F]$. Противоречие.$\square$

Как построить расширение Галуа? Две конструкции

Конструкция 1 (Галуа, Абель). Пусть $f(x) \in F[X]$ — неприводимый (для простоты) и сепарабельный (по необходимости) многочлен. (Напомню, что последнее означает, что у $f(x)$ нет кратных корней.) Рассмотрим поле разложения E_f многочлена f, т.е. поле $F(\Theta_1, \ldots, \Theta_s)$, где $\Theta_1, \ldots, \Theta_s$ — различные корни многочлена f, лежащие в $\overline{F}$.

Утверждается, что поле разложения есть расширение Галуа. Для начала покажем, что любое вложение $\sigma : E_f \longrightarrow \overline{F}$ над F является автоморфизмом поля E_f. В самом деле, гомоморфизм σ переводит корень Θ многочлена $f(x)$ в корень этого же многочлена: если $a_0 + a_1\Theta + a_2\Theta^2 + \ldots + a_s\Theta^s = 0$, то и $(a_0 + a_1\Theta + a_2\Theta^2 + \ldots + a_s\Theta^s)^\sigma =$ $= a_0^\sigma + a_1^\sigma\Theta^\sigma + a_2^\sigma(\Theta^\sigma)^2 + \ldots + a_s^\sigma(\Theta^\sigma)^s = a_0 + a_1^\sigma + \ldots + a_s(\Theta^\sigma)^s = 0$.

С другой стороны, поле разложения является полем рациональных дробей от элементов $\Theta_1, \ldots, \Theta_s$, и гомоморфизм σ, переставляя эти элементы между собой, сохраняет поле E_f. (Почему $E_f^\sigma = E_f$?) Итак, все вложения $E_f \longrightarrow \overline{F}$ над F — автоморфизмы поля E_f. Далее рассмотрим башню простых расширений

$$E_f = F(\Theta_1, \ldots, \Theta_s) > F(\Theta_1, \ldots, \Theta_{s-1}) > \ldots > F(\Theta_1) > F.$$

Применяя Кит 1 к каждому этажу (с учетом сепарабельности $f(x)$), получаем, что число Галуа E_f над F равно $[E_f : F]$, т.е. порядок группы $\mathrm{Aut}(E_f/F)$ равен $[E_f : F]$.

В связи с конструкцией 1 можно говорить о группе Галуа многочлена $f(x)$, подразумевая под этим группу Галуа его поля разложения.

Комментарии.

1) Очень трудный пример: простая группа Клейна порядка 168, изоморфная группе $\mathrm{PSL}(3, \mathbb{F}_2)$ реализуется как группа Галуа поля разложения многочлена $x^7 - 7x + 3$ над $\mathbb{Q}$. (Сможете ли вы доказать неприводимость этого многочлена над $\mathbb{Q}$?)

2) Вопрос о том, какие простые группы реализуются как группы Галуа над $\mathbb{Q}$, по-видимому, до сих пор открыт.

3) И. Р. Шафаревич доказал, что любая разрешимая группа реализуется как группа Галуа над $\mathbb{Q}$.

4) Несложно доказать (вы это сможете сделать сами), что любое конечное расширение Галуа получается как поле разложения некоторого сепарабельного многочлена.

Конструкция 2 (Э. Артин) Пусть G — конечная группа автоморфизмов поля E. Тогда верна

Лемма Артина (Кит 3). Конечное расширение $E > E^G$ есть расширение Галуа с группой Галуа G.

Доказательство. Ясно, что $[E : E^G] \geqslant |G|$. Действительно, $|G|$ вложений E над E^G в поле $\overline{E}$ у нас уже имеются, а всех таких вложений не больше, чем $[E : E^G]$. (Заметьте, что мы пока не знаем, конечно ли расширение $E > E^G$.)
Докажем, следуя Э. Артину, что $[E : E^G] = |G|$. Этого уже будет достаточно для справедливости утверждения леммы (почему?).

Доказываем от противного: если $[E : E^G] > |G|$, то существует коллекция $(\Theta_1, \ldots, \Theta_s)$, состоящая из $s = [E : E^G]$ элементов поля E, линейно независимых над полем $F = E^G$. Кроме того, $s > |G| = n$. Перенумеруем элементы группы $G = \sigma_1, \ldots, \sigma_n$ ($\sigma_1 = 1$) и рассмотрим s вектор-столбцов высоты n:

$$\begin{pmatrix} \Theta_1^{\sigma_1} \\ \vdots \\ \Theta_1^{\sigma_n} \end{pmatrix} \cdots\cdots \begin{pmatrix} \Theta_s^{\sigma_1} \\ \vdots \\ \Theta_s^{\sigma_n} \end{pmatrix}$$

Ясно, что эти столбцы линейно зависимы над E (ведь $s > n$), а значит существуют их нетривиальные линейные комбинации с некоторыми коэффициентами $(x_1, \ldots, x_s)$ из E, равные нулевому столбцу. Выберем из них линейную комбинацию с минимальным числом ненулевых коэффициентов, скажем t:

$$\begin{cases} x_1\Theta_1 + x_2\Theta_2 + \ldots + x_t\Theta_t = 0 \\ \vdots \\ x_1\Theta_1^{\sigma_i} + x_2\Theta_2^{\sigma_i} + \ldots + x_t\Theta_t^{\sigma_i} = 0 \\ \vdots \\ x_1\Theta_1^{\sigma_n} + x_2\Theta_2^{\sigma_n} + \ldots + x_t\Theta_t^{\sigma_n} = 0 \end{cases} \qquad (*)$$

где $t \geqslant 2$ (почему?). (Заметим, что поскольку $t \leqslant s$, то может оказаться, что $t \leqslant n$; но на дальнейшие рассуждения это не влияет.) Деля на $x_1 \neq 0$, будем считать, что в нашей системе уравнений $x_1 = 1$.
Заметим, что все x_i не могут лежать в поле $F = E^G$ (иначе среди Θ_i нашлось бы линейно зависимое над F подмножество, что не так). Поэтому можно считать, что $x_2 \notin E^G$.
Следовательно, существует такой автоморфизм $\sigma \in G$, что $x_2^\sigma \neq x_2$. Применим автоморфизм σ ко всем уравнениям системы $(*)$. Тогда мы получим систему $(*)^\sigma$ точно такого же вида, но со строкой неизвестных $(x_1^\sigma, \ldots, x_t^\sigma)$ (почему?). А именно:

$$\begin{cases} x_1^\sigma\Theta_1 + x_2^\sigma\Theta_2 + \ldots + x_t^\sigma\Theta_t = 0 \\ \vdots \\ x_1^\sigma\Theta_1^{\sigma_i} + x_2^\sigma\Theta_2^{\sigma_i} + \ldots + x_t^\sigma\Theta_t^{\sigma_i} = 0 \\ \vdots \\ x_1^\sigma\Theta_1^{\sigma_n} + x_2^\sigma\Theta_2^{\sigma_n} + \ldots + x_t^\sigma\Theta_t^{\sigma_n} = 0 \end{cases} \qquad (*)^\sigma$$

Вычитая $(*)^\sigma$ из $(*)$ (напомним, что $x_1 = 1 = x_1^\sigma$), получим n уравнений, подобных уравнениям системы $(*)$, но число ненулевых неизвестных в каждом уравнении уменьшилось. Новый ненулевой набор неизвестных выглядит так: $(x_2^\sigma - x_2, \ldots, x_t^\sigma - x_t)$, причем $x_2^\sigma - x_2 \neq 0$. Мы приходим к противоречию с предположением о минимальности исходного набора $(x_1 = 1, \ldots, x_t)$.□

Основная теорема теории Галуа

Вот ее формулировка:

Пусть $K > F$ — расширение Галуа. Тогда существует взаимно-однозначное соответствие между подгруппами H группы $\mathrm{Gal}(K/F)$ и подполями поля K, содержащими F, причем соответствующие пары H и L таковы, что $L = K^H$, а $H = \mathrm{Gal}(K/L)$.

Доказательство. Скомбинировать Кит 1, Кит 2 и Кит 3. □

Следствие. В башне $K > L > F$ с расширением Галуа $K > F$ расширение $L > F$ будет расширением Галуа в том и только том случае, когда $\mathrm{Gal}(K/L)$ — нормальная подгруппа в $\mathrm{Gal}(K/F)$. (Указание: воспользоваться тем простым фактом, что для любой подгруппы $H < \mathrm{Gal}(K/F)$ и любого $\sigma \in \mathrm{Gal}(K/F)$ $(K^H)^\sigma = K^{\sigma H \sigma^{-1}}$.)

Основная теорема звучит как известная из топологии теорема о соответствии подгрупп в накрытиях.

Комментарий. Мы несколько увлеклись конечными расширениями, где наши простые определения хорошо работают. Но имеет смысл говорить о расширениях Галуа и группах Галуа в контексте алгебраических расширений. Чтобы дать определение, пригодное для алгебраических расширений, обратимся к следующему факту:

Факт. Если $K > F$ — конечное расширение Галуа, то оно
а) сепарабельно,
б) нормально. (Слово "нормально" может означать многое, но в данном случае речь идет о следующем: если любой неприводимый многочлен $f(x)$ из $F[X]$ имеет корень в поле K, то и все его корни лежат в этом поле.)

Доказательство ("трюк Галуа"). Пусть $\alpha \in K$ и $m_\alpha(x)$ — минимальный многочлен α над полем F. Рассмотрим элементы $\alpha^\sigma, \sigma \in \mathrm{Gal}(K/F)$. Все они — корни минимального многочлена $m_\alpha(x)$, лежащие в K. По теореме Безу $m_\alpha(x)$ делится на многочлен $\prod(x - \alpha^\sigma)$. Но коэффициенты этого многочлена, являясь по теореме Виета симметрическими функциями от α^σ, инвариантны под действием группы $\mathrm{Gal}(K/F)$ (почему?). Следовательно, согласно Кит 2, многочлен $\prod(x - \alpha^\sigma)$ лежит в кольце $F[X]$, а потому совпадает (с точностью до множителя) с неприводимым над F многочленом $m_\alpha(x)$. Это доказывает сразу и а) и б). □

Теперь можно свойства а) и б) взять в качестве определения расширения Галуа в категории алгебраических расширений. А именно: *алгебраическое расширение называется расширением Галуа, если оно нормально и сепарабельно.*

Сложите из кубиков Кит 1, Кит 2 и Кит 3 доказательство того, что для конечных расширений это определение эквивалентно ранее сформулированному.

Норма и след.
Одна задача линейной алгебры, связанная с полями

Пусть K - конечное расширение поля F степени n и x — любой элемент поля K. Тогда x действует на K левым умножением $y \mapsto xy$ для любого $y \in K$. Это действие линейно: $x(y_1 + y_2) = xy_1 + xy_2$, $x(\lambda y) = \lambda xy$, $\lambda \in F$. Таким образом, x становится линейным оператором на конечномерном векторном пространстве K над полем F. Выберем базис $x_1, \ldots, x_n$ в пространстве K. Тогда можно записать

$$xx_i = \sum_j a_{ij}x_j, \;\; a_{ij} \in F \tag{1}$$

Перепишем (1) в виде $\sum_j (\delta_{ij}x - a_{ij})x_i = 0$, т.е. в виде однородной системы линейных уравнений с матрицей коэффициентов $(\delta_{ij}x - a_{ij})$. Эта система имеет нетривиальное решение $(x_1, \ldots, x_n)$. Следовательно, $\det(\delta_{ij}x - a_{ij}) = 0$, т.е. x является корнем характеристического многочлена матрицы (a_{ij}), или характеристического многочлена элемента x, который рассматривается как линейный оператор в К. Характеристический многочлен этого линейного оператора обозначим через $F_x(T)$.

Мы доказали теорему Гамильтона-Кэли: x является корнем характеристического многочлена $F_x(T)$.

С другой стороны, пусть $m_x(T)$ — минимальный многочлен элемента x со старшим коэффициентом 1. Интересно узнать, как связаны $F_x(T)$ и $m_x(T)$.

Теорема 1. Если $\deg m_x(T) = m$, то m делит n, и $F_x(T) = (m_x(T))^{\frac{n}{m}}$

Доказательство. Рассмотрим башню расширений $K > F(x) > F$. Мы знаем, что $1, x, \ldots, x^{m-1}$ составляют базис $F(x)$ над F. Выберем базис $\mu_1, \ldots, \mu_t$, $t = n/m$ в K над $F(x)$. Тогда $\mu_s x^l$ образуют базис K над F. Умело упорядочив этот базис и вычислив в нем характеристический многочлен линейного преобразования x, мы докажем теорему: заметим, что в базисе K над F

$$\mu_1,\, x\mu_1, \ldots, x^{m-1}\mu_1,\;\; \mu_2,\, x\mu_2, \ldots, x^{m-1}\mu_2, \ldots, \mu_t,\, x\mu_t, \ldots, x^{m-1}\mu_t$$

матрица оператора x имеет вид тензорного произведения единичной матрицы на матрицу оператора x, действующего в пространстве $F(x)$ над полем F:

$$E_t \otimes \{\text{матрица оператора } x \text{ в базисе } 1, \ldots, x^{m-1}\}$$

Другими словами, она имеет блочно-диагональный вид

$$\begin{pmatrix} \square & & & 0 \\ & \square & & \\ & & \ddots & \\ 0 & & & \square \end{pmatrix}$$

где каждый блок есть матрица оператора $x : F(x) \longrightarrow F(x)$ в базисе $1, x, \ldots, x^{m-1}$. Но характеристический многочлен оператора $x : F(x) \longrightarrow F(x)$ имеет степень m (размерность пространства $F(x)$ над F), равную степени минимального многочлена $m_x(T)$. А раз у этих двух многочленов есть общий корень x и совпадают коэффициенты при старшей степени, то они равны. Отсюда легко следует утверждение теоремы. $\square$

Два важных определения. Пусть K — конечное расширение поля F.

Следом элемента $x \in K$ (обозначается $\mathrm{tr}_{K/F}(x)$) над F называется след $\mathrm{tr}\, x$ линейного оператора $x : K \longrightarrow K$.

Нормой элемента $x \in K$ (обозначается $N_{K/F}(x)$) над F называется определитель $\det x$ линейного преобразования $x : K \longrightarrow K$.

Отметим, что норма является мультипликативной функцией на K: $N_{K/F}(xy) = N_{K/F}(x)N_{K/F}(y)$, т.е. определяет характер $N_{K/F} : K^* \longrightarrow F^*$ мультипликативной группы поля K со значениями в основном поле F.
След, как и положено, является линейной функцией на K со значениями в F.

Если теорему 1 скомбинировать с теоремой Виета, то получим следующее очень полезное утверждение (пожалуйста, докажите его самостоятельно):

Теорема 2. Если $m_x(T)$ — минимальный многочлен элемента x над F и $\beta_1, \ldots, \beta_m$ — его различные корни в $\overline{F}$ (разумеется, x — один из них), то

$$\mathrm{tr}_{K/F}(x) = \tfrac{n}{m}(\beta_1 + \ldots + \beta_m)$$
$$N_{K/F}(x) = (\beta_1 + \ldots + \beta_m)^{\frac{n}{m}}$$

В случае сепарабельного расширения $K > F$ результат теоремы 2 допускает изящную переформулировку, которая и есть наша окончательная цель.
А именно, рассмотрим n вложений $\sigma_1, \ldots, \sigma_n$ поля K в алгебраическое замыкание $\overline{F}$. Тогда из теоремы 2 немедленно следует, что

$$\mathrm{tr}_{K/F}(x) = \sum_{i=1}^{n} x^{\sigma_i}, \quad N_{K/F}(x) = \prod x^{\sigma_i}$$

И напоследок еще одна приятная вещь.

Теорема 3. Если $K > L > F$ — сепарабельная башня, то

$$N_{K/F}(x) = N_{L/F}\left(N_{K/L}(x)\right)$$
$$\mathrm{tr}_{K/F}(x) = \mathrm{tr}_{L/F}\left(\mathrm{tr}_{K/L}(x)\right)$$

Для доказательства нужно воспользоваться теоремой о продолжении вложений в сепарабельной башне (Кит 1).

Теория Галуа продолжается... Но мы поставим здесь точку.

Рекомендуемая литература:

Э.Артин. *Теория Галуа.* Москва, МЦНМО, 2004
Э.Б.Винберг. *Курс алгебры.* Москва, Факториал, 2004