влечет, что $1 \neq 0$ и $\mathfrak{p}B = B$ тогда и только тогда, когда $1 \in \mathfrak{p}B$.) Если $\mathfrak{p}B = B$, то 1 представляется в виде линейной комбинации элементов из B с коэффициентами в $\mathfrak{p}$

$$1 = a_1 b_1 + \cdots + a_n b_n,$$

где $a_i \in \mathfrak{p}$ и $b_i \in B$. Пусть $B_0 = A[b_1, \ldots, b_n]$. Тогда $\mathfrak{p}B_0 = B_0$ и B_0 — конечный A-модуль в силу предложения 2. Следовательно, $B_0 = 0$ в силу леммы Накаямы, — противоречие.

Чтобы доказать наше второе утверждение, рассмотрим следующую коммутативную диаграмму:

$$\begin{array}{ccc} B & \longrightarrow & B_{\mathfrak{p}} \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_{\mathfrak{p}} \end{array}$$

Мы только что доказали, что $\mathfrak{m}_{\mathfrak{p}} B_{\mathfrak{p}} \neq B_{\mathfrak{p}}$. Следовательно, $\mathfrak{m}_{\mathfrak{p}} B_{\mathfrak{p}}$ содержится в некотором максимальном идеале $\mathfrak{M}$ кольца $B_{\mathfrak{p}}$. Переходя к прообразам, мы видим, что прообраз $\mathfrak{M}$ в $A_{\mathfrak{p}}$ есть идеал, содержащий $\mathfrak{m}_{\mathfrak{p}}$. Так как идеал $\mathfrak{m}_{\mathfrak{p}}$ максимальный, то $\mathfrak{M} \cap A_{\mathfrak{p}} = \mathfrak{m}_{\mathfrak{p}}$. Пусть $\mathfrak{P}$ — прообраз $\mathfrak{M}$ в B. Тогда $\mathfrak{P}$ — простой идеал в B. Прообраз $\mathfrak{m}_{\mathfrak{p}}$ в A есть просто $\mathfrak{p}$. Беря полный прообраз $\mathfrak{M}$ по обоим путям в диаграмме, находим

$$\mathfrak{P} \cap A = \mathfrak{p},$$

что и требовалось показать.

Предложение 10. *Пусть A — подкольцо в B, причем кольцо B — целое над A. Простой идеал $\mathfrak{P}$ в B, лежащий над простым идеалом $\mathfrak{p}$ кольца A, максимален в том и только в том случае, если $\mathfrak{p}$ максимален.*

Доказательство. Предположим, что $\mathfrak{p}$ максимален в A. Тогда $A/\mathfrak{p}$ — поле и $B/\mathfrak{P}$ — целостное кольцо, целое над $A/\mathfrak{p}$. Если $\alpha \in B/\mathfrak{P}$, то элемент α алгебраичен над $A/\mathfrak{p}$, а мы знаем, что тогда $A/\mathfrak{p}[\alpha]$ — поле. Следовательно, всякий ненулевой элемент из $B/\mathfrak{P}$ обратим в кольце $B/\mathfrak{P}$, которое поэтому является полем. Обратно, предположим, что $\mathfrak{P}$ — максимальный идеал в B. Тогда $B/\mathfrak{P}$ — поле, целое над целостным кольцом $A/\mathfrak{p}$. Если $A/\mathfrak{p}$ — не поле, то оно содержит ненулевой максимальный идеал $\mathfrak{m}$. В силу предложения 9 в $B/\mathfrak{P}$ существует простой идеал $\mathfrak{M}$, лежащий над $\mathfrak{m}$, $\mathfrak{M} \neq 0$, — противоречие.

§ 2. Целые расширения Галуа

Мы исследуем здесь взаимоотношение между теорией Галуа многочлена и теорией Галуа того же самого многочлена, приведенного по модулю простого идеала.

Предложение 11. *Пусть A — целостное кольцо, целозамкнутое в своем поле частных K; L — конечное нормальное расши-*

рение поля K с группой Галуа G; $\mathfrak{p}$ — максимальный идеал в A и $\mathfrak{P}$, $\mathfrak{Q}$ — простые идеалы целого замыкания B кольца A в L, лежащие над $\mathfrak{p}$. Тогда существует элемент $\sigma \in G$, такой, что $\sigma\mathfrak{P} = \mathfrak{Q}$.

Доказательство. Предположим, что $\mathfrak{Q} \neq \sigma\mathfrak{P}$ ни для одного $\sigma \in G$. Тогда $\tau\mathfrak{Q} \neq \sigma\mathfrak{P}$ ни для какой пары элементов σ, $\tau \in G$. Существует элемент $x \in B$, такой, что

$$x \equiv 0 \pmod{\sigma\mathfrak{P}} \quad \text{для всех} \quad \sigma \in G,$$
$$x \equiv 1 \pmod{\sigma\mathfrak{Q}} \quad \text{для всех} \quad \sigma \in G$$

(использовать китайскую теорему об остатках). Норма

$$N_K^L(x) = \Big(\prod_{\sigma \in G} \sigma x\Big)^{[L:K]_i}$$

лежит в $B \cap K = A$ (так как A целозамкнуто) и, значит, в $\mathfrak{P} \cap A = \mathfrak{p}$. Но $x \notin \sigma\mathfrak{Q}$ ни при каком $\sigma \in G$, так что $\sigma x \notin \mathfrak{Q}$ ни при каком $\sigma \in G$. Это противоречит тому факту, что норма элемента x лежит в $\mathfrak{p} = \mathfrak{Q} \cap A$.

Локализацией можно снять предположение о максимальности $\mathfrak{p}$; достаточно предполагать, что $\mathfrak{p}$ простой.

Следствие. *Пусть A — кольцо, целозамкнутое в своем поле частных K; E — конечное алгебраическое расширение поля K; B — целое замыкание A в E и $\mathfrak{p}$ — максимальный идеал в A. Тогда существует лишь конечное число простых идеалов в B, лежащих над $\mathfrak{p}$* [1]).

Доказательство. Пусть L — наименьшее нормальное расширение поля K, содержащее E. Если $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ — два различных простых идеала в B, лежащих над $\mathfrak{p}$, и $\mathfrak{P}_1$, $\mathfrak{P}_2$ — два простых идеала из целого замыкания A в L, лежащих над $\mathfrak{Q}_1$ и $\mathfrak{Q}_2$ соответственно, то $\mathfrak{P}_1 \neq \mathfrak{P}_2$. Это соображение сводит наше утверждение к случаю, когда E — нормальное расширение над K, а тогда оно становится непосредственным следствием предложения 11.

Пусть кольцо A целозамкнуто в своем поле частных K и B — его целое замыкание в конечном расширении Галуа L с группой G. Тогда $\sigma B = B$ для всякого $\sigma \in G$. Пусть $\mathfrak{p}$ — некоторый максимальный идеал в A и $\mathfrak{P}$ — максимальный идеал в B, лежащий над $\mathfrak{p}$. Обозначим через $G_{\mathfrak{P}}$ подгруппу в G, состоящую из всех автоморфизмов σ, для которых $\sigma\mathfrak{P} = \mathfrak{P}$. Тогда группа $G_{\mathfrak{P}}$ естественным образом действует на поле классов вычетов $B/\mathfrak{P}$ и оставляет неподвижным поле $A/\mathfrak{p}$. Каждому $\sigma \in G_{\mathfrak{P}}$ мы можем сопоставить автоморфизм σ' поля $B/\mathfrak{P}$ над $A/\mathfrak{p}$, и отображение, задаваемое правилом

$$\sigma \mapsto \sigma',$$

[1]) Именно в таком виде следствие используется в § 4 гл. XII. В формулировке автора на E налагается условие сепарабельности. — *Прим. ред.*

индуцирует гомоморфизм $G_{\mathfrak{P}}$ в группу автоморфизмов поля $B/\mathfrak{P}$ над $A/\mathfrak{p}$.

Группа $G_{\mathfrak{P}}$ будет называться *группой разложения* идеала $\mathfrak{P}$. Ее неподвижное поле будет обозначаться через L^d и будет называться *полем разложения* идеала $\mathfrak{P}$. Пусть B^d — целое замыкание A в L^d и $\mathfrak{Q} = \mathfrak{P} \cap B^d$. В силу предложения 11 $\mathfrak{P}$ — единственный простой идеал в B, лежащий над $\mathfrak{Q}$.

Пусть $G = \bigcup \sigma_j G_{\mathfrak{P}}$ — разложение на смежные классы группы G по $G_{\mathfrak{P}}$. Тогда простые идеалы $\sigma_j\mathfrak{P}$ — это в точности все различные простые идеалы в B, лежащие над $\mathfrak{p}$. Действительно, для двух элементов σ, $\tau \in G$ тогда и только тогда $\sigma\mathfrak{P} = \tau\mathfrak{P}$, когда $\tau^{-1}\sigma\mathfrak{P} = \mathfrak{P}$, т. е. $\tau^{-1}\sigma$ лежит в $G_{\mathfrak{P}}$. Таким образом, τ, σ лежат в одном и том же смежном классе $\bmod G_{\mathfrak{P}}$.

Непосредственно ясно, что группой разложения простого идеала $\sigma\mathfrak{P}$ будет $\sigma G_{\mathfrak{P}}\sigma^{-1}$.

Предложение 12. *Поле L^d — это наименьшее подполе E в L, содержащее K и такое, что $\mathfrak{P}$ — единственный простой идеал в B, лежащий над идеалом $\mathfrak{P} \cap E$ (который является простым в $B \cap E$).*

Доказательство. Пусть E обладает указанными свойствами, и пусть H — группа Галуа расширения L над E. Положим $\mathfrak{q} = \mathfrak{P} \cap E$. В силу предложения 11 все простые идеалы в B, лежащие над $\mathfrak{q}$, сопряжены посредством элементов из H. Так как имеется только один такой простой идеал, а именно $\mathfrak{P}$, то это означает, что H оставляет $\mathfrak{P}$ инвариантным. Следовательно, $H \subset G_{\mathfrak{P}}$ и $E \supset L^d$. Но, как мы уже отмечали, само L^d обладает требуемыми свойствами.

Предложение 13. *В тех же обозначениях имеем $A/\mathfrak{p} = B^d/\mathfrak{Q}$ (относительно канонического вложения $A/\mathfrak{p} \to B^d/\mathfrak{Q}$).*

Доказательство. Если σ — элемент из G, не лежащий в $G_{\mathfrak{P}}$, то $\sigma\mathfrak{P} \neq \mathfrak{P}$ и $\sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$. Положим

$$\mathfrak{Q}_\sigma = \sigma^{-1}\mathfrak{P} \cap B^d.$$

Тогда $\mathfrak{Q}_\sigma \neq \mathfrak{Q}$. Пусть x — произвольный элемент из B^d. В B^d существует элемент y, такой, что

$$y \equiv x \pmod{\mathfrak{Q}},$$
$$y \equiv 1 \pmod{\mathfrak{Q}_\sigma}$$

для всякого σ из G, не лежащего в $G_{\mathfrak{P}}$. В частности,

$$y \equiv x \pmod{\mathfrak{P}},$$
$$y \equiv 1 \pmod{\sigma^{-1}\mathfrak{P}}$$

для всякого σ вне $G_{\mathfrak{P}}$. Второе сравнение переписывается в виде

$$\sigma y \equiv 1 \pmod{\mathfrak{P}}$$

для всех $\sigma \notin G_{\mathfrak{P}}$. Норма элемента y из L^d в K есть произведение y на множители вида σy с $\sigma \notin G_{\mathfrak{P}}$. Следовательно,

$$N_K^{L^d}(y) \equiv x \pmod{\mathfrak{P}}.$$

Но норма лежит в K и даже в A, поскольку она является произведением элементов, целых над A. Так как и x, и норма лежат в B^d, то последнее сравнение выполняется по модулю $\mathfrak{Q}$. Но именно это и утверждается нашим предложением.

Пусть x — элемент из B. Мы будем обозначать через x' его образ относительно гомоморфизма $B \to B/\mathfrak{P}$. Тогда σ' есть автоморфизм поля $B/\mathfrak{P}$, удовлетворяющий соотношению

$$\sigma' x' = (\sigma x)'.$$

Пусть $f(X)$ — многочлен с коэффициентами в B. Мы будем обозначать через $f'(X)$ его естественный образ при предыдущем гомоморфизме. Таким образом, если

$$f(X) = b_n X^n + \cdots + b_0,$$

то

$$f'(X) = b_n' X^n + \cdots + b_0'.$$

Предложение 14. *Пусть кольцо A целозамкнуто в своем поле частных K; B — его целое замыкание в конечном расширении Галуа L поля K с группой G; $\mathfrak{p}$ — максимальный идеал в A и $\mathfrak{P}$ — максимальный идеал в B, лежащий над $\mathfrak{p}$. Тогда $B/\mathfrak{P}$ — нормальное расширение поля $A/\mathfrak{p}$ и отображение $\sigma \mapsto \sigma'$ индуцирует гомоморфизм $G_{\mathfrak{P}}$ на группу Галуа $G'_{\mathfrak{P}}$ расширения $B/\mathfrak{P}$ над $A/\mathfrak{p}$.*

Доказательство. Пусть $B' = B/\mathfrak{P}$ и $A' = A/\mathfrak{p}$. Любой элемент из B' может быть записан как x' для некоторого $x \in B$. Элемент x' порождает некоторое сепарабельное подрасширение в B' над A'. Пусть f — неприводимый многочлен для x над K. Коэффициенты f лежат в A, поскольку сам x — целый над A и все корни f — целые над A. Таким образом,

$$f(X) = \prod_{i=1}^{m} (X - x_i)$$

разлагается на линейные множители в B. Так как

$$f'(X) = \prod_{i=1}^{m} (X - x_i')$$

и все x'_i лежат в B', то f' разлагается на линейные множители в B'. Заметим, что $f(x)=0$ влечет $f'(x')=0$. Следовательно, B' нормально над A' и

$$[A'(x'):A'] \leqslant [K(x):K] \leqslant [L:K].$$

Это означает, что максимальное сепарабельное подрасширение поля A' в B' имеет конечную степень над A' (использовать теорему о примитивном элементе из элементарной теории полей). Эта степень в действительности ограничена числом $[L:K]$.

Остается доказать, что отображение $\sigma \longmapsto \sigma'$ дает сюръективный гомоморфизм группы $G_{\mathfrak{P}}$ на группу Галуа расширения B' над A'. Чтобы сделать это, мы сначала приведем соображение, сводящее задачу к случаю, когда $\mathfrak{P}$ — единственный простой идеал в B, лежащий над $\mathfrak{p}$. Именно, *в силу предложения 13 поля вычетов основного кольца и кольца B^d в поле разложения одинаковы*. Значит, для доказательства сюръективности мы можем взять в качестве основного поля L^d. Это и есть желаемая редукция, так что мы можем считать, что $K=L^d$, $G=G_{\mathfrak{P}}$.

Так и считая, выберем образующую максимального сепарабельного подрасширения в B' над A'; пусть это будет x' для некоторого элемента x из B. Пусть f — неприводимый многочлен элемента x над K. Всякий автоморфизм поля B' определяется его действием на x', а x' он переводит в некоторый корень многочлена f'. Положим $x=x_1$. Для любого данного корня x_i многочлена f существует элемент σ группы $G=G_{\mathfrak{P}}$, такой, что $\sigma x = x_i$. Следовательно, $\sigma' x' = x'_i$, так что автоморфизмы B' над A', индуцированные элементами из G, действуют транзитивно на корнях f'. Значит, они дают нам все автоморфизмы поля вычетов, что и требовалось показать.

Следствие 1. *Пусть A — кольцо, целозамкнутое в своем поле частных K; L — конечное расширение Галуа поля K; B — целое замыкание A в L; $\mathfrak{p}$ — некоторый максимальный идеал в A; φ: $A \to A/\mathfrak{p}$ — канонический гомоморфизм и ψ_1, ψ_2 — два гомоморфизма кольца B в заданное алгебраическое замыкание поля $A/\mathfrak{p}$, продолжающие φ. Тогда существует такой автоморфизм σ поля L над K, что*

$$\psi_1 = \psi_2 \circ \sigma.$$

Доказательство. Ядра ψ_1, ψ_2 — это простые идеалы в B, сопряженные между собой согласно предложению 11. Следовательно, существует такой элемент τ группы Галуа G, что ψ_1, $\psi_2 \circ \tau$ имеют одно и то же ядро. Не теряя общности, мы можем поэтому считать, что ψ_1, ψ_2 имеют одно и то же ядро $\mathfrak{P}$. Следовательно, существует автоморфизм ω поля $\psi_1(B)$ на $\psi_2(B)$, такой, что $\omega \circ \psi_1 = \psi_2$. В силу

предыдущего предложения существует элемент σ группы $G_{\mathfrak{P}}$, для которого $\omega \circ \psi_1 = \psi_1 \circ \sigma$. Это доказывает нужное нам утверждение.

Замечание. Во всех предыдущих предложениях можно было бы предполагать, что $\mathfrak{p}$ — произвольный простой, а не обязательно максимальный идеал. В этом случае, чтобы иметь возможность применить наши доказательства, достаточно произвести локализацию в $\mathfrak{p}$.

Ядро отображения

$$G_{\mathfrak{P}} \to G'_{\mathfrak{P}},$$

с которым мы имели дело выше, называется *группой инерции* идеала $\mathfrak{P}$. Она состоит из тех автоморфизмов в $G_{\mathfrak{P}}$, которые индуцируют тривиальный автоморфизм на поле вычетов. Неподвижное поле этой группы называется *полем инерции* и обозначается через L^t.

Следствие 2. *Сохраняя предпосылки следствия* 1, *предположим еще, что* $\mathfrak{P}$ *— единственный простой идеал в* B, *лежащий над* $\mathfrak{p}$. *Пусть* $f(X)$ *— многочлен из* $A[X]$ *со старшим коэффициентом* 1, *неприводимый в* $K[X]$ *и имеющий корень* α *в* B. *Тогда многочлен* f' *является степенью неприводимого многочлена из* $A'[X]$.

Доказательство. Как следует из доказательства предложения 14, любые два корня f' сопряжены относительно некоторого изоморфизма B' над A' и, следовательно, f' не может разлагаться на взаимно простые множители. Поэтому f' есть степень неприводимого многочлена.

Предложение 15. *Пусть* A *— целостное кольцо, целозамкнутое в своем поле частных* K, *и* L *— конечное расширение Галуа поля* K, *причем* $L = K(\alpha)$, *где* α *— целый элемент над* A, *являющийся корнем неприводимого многочлена*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0, \qquad a_i \in A.$$

Пусть $f'(X)$ *— соответствующий многочлен с коэффициентами из* $A/\mathfrak{p}$, *где* $\mathfrak{p}$ *— некоторый максимальный идеал в* A. *Пусть, наконец,* $\mathfrak{P}$ *— лежащий над* $\mathfrak{p}$ *простой идеал из целого замыкания* B *кольца* A *в* L *и* $G_{\mathfrak{P}}$ *— его группа разложения. Если у* f' *нет кратных корней, то отображение* $\sigma \mapsto \sigma'$ *имеет тривиальное ядро и является изоморфизмом группы* $G_{\mathfrak{P}}$ *на группу Галуа многочлена* f' *над* $A/\mathfrak{p}$.

Доказательство. Пусть

$$f(X) = \prod (X - x_i)$$

— разложение f в L. Как мы знаем, $x_i \in B$. Если $\sigma \in G_{\mathfrak{P}}$, то, как и прежде, обозначим через σ' гомоморфный образ σ в группе $G'_{\mathfrak{P}}$.

Имеем

$$f'(X) = \prod (X - x_i').$$

Предположим, что $\sigma' x_i' = x_i'$ для всех i. Так как $(\sigma x_i)' = \sigma' x_i'$ и так как f' не имеет кратных корней, то автоморфизм σ также тождественный. Следовательно, наше отображение инъективно, а группа инерции тривиальна. Поле $A'[x_1', \ldots, x_n']$ есть подполе в B', и любой автоморфизм B' над A', ограничение которого на это подполе тождественно, должен быть тождественным, поскольку $G_{\mathfrak{P}} \to G'_{\mathfrak{P}}$ — сюръективное отображение на группу Галуа B' над A'. Следовательно, B' чисто несепарабельно над $A'[x_1', \ldots, x_n']$, а потому группа $G_{\mathfrak{P}}$ изоморфна группе Галуа многочлена f' над A'.

Предложение 15 дает очень эффективный инструмент для исследования многочленов над кольцом. Например, рассмотрим „общий" многочлен

$$f_w(X) = X^n + w_{n-1}X^{n-1} + \ldots + w_0,$$

где $w_0, \ldots, w_{n-1}$ алгебраически независимы над полем k. Как мы знаем, группой Галуа этого многочлена над $k(w_0, \ldots, w_n)$ является симметрическая группа. Пусть $t_1, \ldots, t_n$ — его корни, и пусть α — образующая поля разложения. Не теряя общности, мы можем считать элемент α целым над кольцом $k[w_0, \ldots, w_{n-1}]$ (умножая любую заданную образующую на подходяще выбранный многочлен и используя предложение 1). Пусть $g_w(X)$ — неприводимый многочлен элемента α над $k(w_0, \ldots, w_{n-1})$. Коэффициентами g служат многочлены от (w). Если мы сможем подставить вместо (w) значения (a) с такими $a_0, \ldots, a_{n-1} \in k$, что g_a останется неприводимым, то, согласно предложению 15, мы тотчас получим заключение, что группа Галуа многочлена g_a также будет симметрической. Аналогично, если всякое поле между $k(w_0, \ldots, w_{n-1})$ и $k(t_1, \ldots, t_n)$ порождается n алгебраически независимыми элементами, то мы можем применить подобную конструкцию для получения расширений с заданными группами Галуа. Может ли это быть сделано, является одной из основных нерешенных задач теории Галуа. Это по существу есть параметризация всех расширений Галуа независимыми элементами.

В качестве другого примера рассмотрим многочлен $X^5 - X - 1$ над $\mathbf{Z}$.

Редукция по модулю 5 показывает, что этот многочлен неприводим. Редукция по модулю 2 дает неприводимые множители

$$(X^2 + X + 1)(X^3 + X^2 + 1) \pmod 2.$$

Следовательно, группа Галуа над полем рациональных чисел (как группа перестановок корней многочлена) содержит 5-цикл и произведение 2-цикла и 3-цикла. Отсюда легко вытекает, что она должна быть полной симметрической группой.