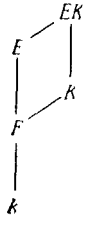
над k. Имеется автоморфизм σ поля $k(\alpha)$ над k, такой, что $\sigma\alpha = \alpha + 1$ (поскольку $\alpha + 1$ также корень). Степени σ^i автоморфизма σ дают $\sigma^i(\alpha) = \alpha + i$ для $i = 1, \ldots, p$ и поэтому все различны. Следовательно, группа Галуа состоит из этих степеней, а потому является циклической, что и доказывает теорему.

§ 7. Разрешимые и радикальные расширения

Конечное расширение E/k (которое мы для удобства будем предполагать сепарабельным) называется *разрешимым*, если группа Галуа наименьшего расширения Галуа K над k, содержащего E, является разрешимой группой. Это эквивалентно тому, что существует разрешимое расширение Галуа L поля k, такое, что $k \subset E \subset L$. Действительно, имеем $k \subset E \subset K \subset L$ и $G(K/k)$ есть гомоморфный образ группы $G(L/k)$.

Предложение 2. *Разрешимые расширения образуют отмеченный класс расширений.*

Доказательство. Пусть E/k разрешимо и F — поле, содержащее k, причем E, F — подполя некоторого алгебраически замкнутого поля. Пусть K — разрешимое расширение Галуа над k и $E \subset K$. Тогда KF будет расширением Галуа над F и $G(KF/F)$ — подгруппой в $G(K/k)$ в силу теоремы 4 из § 1. Следовательно, EF/F разрешимо. Ясно, что подрасширение разрешимого расширения разрешимо. Пусть $E \supset F \supset k$ — башня с разрешимыми расширениями E/F и F/k. Пусть K — конечное разрешимое расширение Галуа поля k, содержащее F. Как мы только что видели, EK/K разрешимо. Пусть L — разрешимое расширение Галуа поля K, содержащее EK. Если σ — произвольное вложение L над k в заданное алгебраическое замыкание, то $\sigma K = K$ и, следовательно, σL — разрешимое расширение поля K. Пусть M — композит всех расширений σL для всех вложений σ поля L над k. Тогда M — расширение Галуа над k, а следовательно, и над K. Группа Галуа поля M над K является подгруппой произведения $\prod_{\sigma} G(\sigma L/K)$,



в силу теоремы 5 из § 1. Следовательно, она разрешима. По теореме 3 из § 1 имеет место сюръективный гомоморфизм $G(M/k) \to G(K/k)$. Значит, группа Галуа расширения M/k имеет разрешимую нормальную подгруппу, факторгруппа по которой разрешима. Поэтому она сама разрешима. Так как $E \subset M$, то наше доказательство закончено.

Конечное расширение F поля k называется *разрешимым в радикалах*, если оно сепарабельно и если существует конечное расширение E поля k, содержащее F и обладающее разложением в башню

$$k \subset E_0 \subset E_1 \subset E_2 \subset \ldots \subset E_m = E,$$

таким, что каждый этаж E_{i+1}/E_i принадлежит к одному из следующих типов:

(1) получается присоединением корня из единицы;

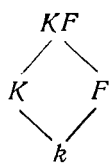
(2) получается присоединением корня многочлена $X^n - a$, где $a \in E_i$ и n взаимно просто с характеристикой;

(3) получается присоединением корня уравнения $X^p - X - a$, где $a \in E_i$ и p — характеристика > 0.

Сразу же видно, что класс расширений, разрешимых в радикалах, является отмеченным классом.

Теорема 12. *Пусть E — сепарабельное расширение поля k. Тогда E разрешимо в радикалах в том и только в том случае, если E/k разрешимо.*

Доказательство. Предположим, что E/k разрешимо. Пусть K — конечное разрешимое расширение Галуа поля k, содержащее E; m — произведение всех степеней простых чисел, не равных характеристике и делящих степень $[K : k]$; $F = k(\zeta)$, где ζ — примитивный корень m-й степени из единицы. Тогда F/k абелево. Поднимем K над F. Тогда KF разрешимо над F. Между F и KF имеется башня подполей



такая, что каждый ее этаж — циклический простого порядка, поскольку всякая разрешимая группа обладает башней подгрупп такого типа, и мы можем применить теорему 3 из § 1. В силу теорем 10 и 11 заключаем, что KF разрешимо в радикалах над F и, следовательно, разрешимо в радикалах над k. Это доказывает, что E/k разрешимо в радикалах.

Обратно, предположим, что E/k разрешимо в радикалах. Для любого вложения σ поля E в $\bar{E}$ над k расширение $\sigma E/k$ также

разрешимо в радикалах. Следовательно, наименьшее содержащее E расширение Галуа K поля k, которое является композитом E и его сопряженных, разрешимо в радикалах. Пусть m — произведение всех степеней простых чисел, не равных характеристике и делящих степень $[K:k]$. Положим снова $F=k(\zeta)$, где ζ — примитивный корень m-й степени из единицы. Достаточно доказать, что KF разрешимо над F, поскольку отсюда будет вытекать, что KF разрешимо над k и, следовательно, группа $G(K/k)$, являющаяся гомоморфным образом группы $G(KF/k)$, разрешима. Но KF/F может быть разложено в башню расширений, каждый этаж которой имеет простую степень и принадлежит к типу, описанному в теоремах 10 и 11, причем соответствующие корни из единицы лежат в поле F. Следовательно, KF/F разрешимо, и наша теорема доказана.

Замечание. Можно было бы так видоизменить предыдущее изложение, чтобы не предполагать сепарабельности. Тогда нужно было бы иметь дело с нормальными расширениями вместо расширений Галуа и считать уравнения $X^p-a=0$ разрешимыми в радикалах, когда p равно характеристике. При этом будет иметь место теорема, соответствующая теореме 12. Доказательства очевидны ввиду § 7 из гл. VII.

§ 8. Теория Куммера

В этом параграфе мы дадим обобщение теоремы, касающейся циклических расширений, на тот случай, когда основное поле содержит достаточно много корней из единицы.

Пусть k — поле и m — положительное целое число. Расширение Галуа K поля k с группой G называется расширением *показателя* m, если $\sigma^m=1$ для всех $\sigma\in G$.

Мы будем исследовать абелевы расширения показателя m. Сначала предположим, что m взаимно просто с характеристикой поля k и что k содержит примитивный корень m-й степени из единицы. Обозначим через Z_m группу корней m-й степени из 1. Будем предполагать в этом параграфе, что все наши алгебраические расширения содержатся в некотором фиксированном алгебраическом замыкании $\bar{k}$.

Пусть $a\in k$. Выражение $a^{1/m}$ $\left(\text{или } \sqrt[m]{a}\right)$ не определено однозначно. Если $\alpha^m=a$ и ζ — корень m-й степени из единицы, то также и $(\zeta\alpha)^m=a$. Мы будем использовать символ $a^{1/m}$ для обозначения любого такого элемента α и все такие элементы α будем называть корнями m-й степени из a. Заметим, что, поскольку корни m-й степени из единицы лежат в основном поле, поле $k(\alpha)$ будет одним и тем же независимо от того, какой корень m-й степени α из a мы выберем. Мы будем обозначать это поле символом $k(a^{1/m})$.