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 $k(a^{1/m})$.

Обозначим через k^{*m} подгруппу в k^*, состоящую из всех m-х степеней ненулевых элементов из k. Это образ группы k^* при гомоморфизме $x \longmapsto x^m$.

Пусть B — подгруппа k^*, содержащая k^{*m}. Мы будем обозначать символом $k(B^{1/m})$, или K_B, композит всех полей $k(a^{1/m})$ с $a \in B$. Он однозначно определен подгруппой B как подполе в $\bar{k}$.

Пусть $a \in B$ и α — корень m-й степени из a. Многочлен $X^m - a$ разлагается на линейные множители в K_B, и, таким образом, K_B — расширение Галуа над k, поскольку это выполняется для всех $a \in B$. Пусть G — его группа Галуа. Если $\sigma \in G$, то $\sigma\alpha = \omega_\sigma \alpha$, где $\omega_\sigma \in Z_m \subset k^*$ — некоторый корень m-й степени из единицы. Отображение

$$\sigma \longmapsto \omega_\sigma$$

является, очевидно, гомоморфизмом G в Z_m, т. е. для τ, $\sigma \in G$ имеем $\tau\sigma\alpha = \omega_\tau \omega_\sigma \alpha = \omega_\sigma \omega_\tau \alpha$. Мы можем написать $\omega_\sigma = \sigma\alpha/\alpha$. Этот корень из единицы ω_σ не зависит от выбора корня m-й степени из a, поскольку если α' — другой корень m-й степени, то $\alpha' = \zeta\alpha$ для некоторого $\zeta \in Z_m$, откуда

$$\sigma\alpha'/\alpha' = \zeta\sigma\alpha/\zeta\alpha = \sigma\alpha/\alpha.$$

Обозначим ω_σ символом $\langle \sigma, a \rangle$. Соответствие

$$(\sigma, a) \longmapsto \langle \sigma, a \rangle$$

дает нам отображение

$$G \times B \to Z_m.$$

Если a, $b \in B$ и $\alpha^m = a$, $\beta^m = b$, то $(\alpha\beta)^m = ab$ и, следовательно,

$$\sigma(\alpha\beta)/\alpha\beta = (\sigma\alpha/\alpha)(\sigma\beta/\beta).$$

Отсюда, заключаем, что предыдущее отображение билинейно. Кроме того, если $a \in k^{*m}$, то $\langle \sigma, a \rangle = 1$.

Теорема 13. *Пусть k — поле и m — целое число > 0, взаимно простое с характеристикой поля k, причем примитивный корень m-й степени из единицы лежит в k. Пусть B — подгруппа в k^*, содержащая k^{*m}, и $K_B = k(B^{1/m})$. Тогда K_B — абелево расширение Галуа показателя m. Пусть G — его группа Галуа. Имеет место билинейное отображение*

$$G \times B \to Z_m, \quad \textit{задаваемое соответствием} \quad (\sigma, a) \longmapsto \langle \sigma, a \rangle.$$

Если $\sigma \in G$, $a \in B$ и $\alpha^m = a$, то $\langle \sigma, a \rangle = \sigma\alpha/\alpha$. Ядро слева равно 1, а ядро справа есть k^{*m}. Расширение K_B/k конечно тогда и только тогда, когда индекс $(B : k^{*m})$ конечен, и в этом случае

$$[K_B : k] = (B : k^{*m}).$$

Доказательство. Пусть $\sigma \in G$, причем $\langle \sigma, a \rangle = 1$ для всех $a \in B$. Тогда $\sigma\alpha = \alpha$ для всякого примитивного элемента α поля K_B, такого, что $\alpha^m = a \in B$. Следовательно, σ индуцирует тождественное отображение на K_B и ядро слева равно 1. Пусть $a \in B$, причем $\langle \sigma, a \rangle = 1$ для всех $\sigma \in G$. Рассмотрим подполе $k(a^{1/m})$ в K_B. Если $a^{1/m}$ не лежит в k, то существует автоморфизм поля $k(a^{1/m})$ над k, не являющийся тождественным. Продолжим этот автоморфизм на K_B и обозначим продолжение снова через σ. Тогда ясно, что $\langle \sigma, a \rangle \neq 1$. Это доказывает наше утверждение.

В силу теоремы двойственности из гл. I, § 11 мы видим, что группа G конечна тогда и только тогда, когда конечна группа B/k^{*m}, и в этом случае порядок G равен индексу $(B : k^{*m})$.

Теорема 14. *В обозначениях теоремы* 13 *отображение* $B \longmapsto K_B$ *дает биективное соответствие между множеством подгрупп в* k^*, *содержащих* k^{*m}, *и множеством абелевых расширений над* k *показателя* m.

Доказательство. Пусть B_1, B_2 — подгруппы в k^*, содержащие k^{*m}. Если $B_1 \subset B_2$, то $k(B_1^{1/m}) \subset k(B_2^{1/m})$. Обратно, предположим, что $k(B_1^{1/m}) \subset k(B_2^{1/m})$. Мы хотим доказать, что $B_1 \subset B_2$. Пусть $b \in B_1$. Тогда $k(b^{1/m}) \subset k(B_2^{1/m})$, причем $k(b^{1/m})$ содержится в конечно порожденном подрасширении в $k(B_2^{1/m})$. Таким образом, не теряя общности, мы можем предполагать, что группа B_2/k^{*m} — конечно порожденная и, следовательно, конечная. Пусть B_3 — подгруппа в k^*, порожденная B_2 и b. Тогда $k(B_2^{1/m}) = k(B_3^{1/m})$, а из того, что мы видели выше, вытекает, что степень этого поля над k есть

$$(B_2 : k^{*m}) \quad \text{или} \quad (B_3 : k^{*m}).$$

Таким образом, эти два индекса равны и $B_2 = B_3$. Это доказывает, что $B_1 \subset B_2$.

Итак, мы получили вложение нашего множества групп B в множество абелевых расширений поля k, имеющих показатель m. Предположим теперь, что K — некоторое абелево расширение над k показателя m. Любое конечное подрасширение есть композит циклических расширений показателя m, поскольку всякая конечная абелева группа является произведением циклических групп, и мы можем применить следствие 2 теоремы 5, § 1. В силу теоремы 10 всякое циклическое расширение может быть получено присоединением корня m-й степени. Следовательно, K может быть получено присоединением семейства корней m-й степени, скажем корней m-й степени из элементов $\{b_j\}_{j \in J}$, где $b_j \in k^*$. Пусть B — подгруппа в k^*, порожденная всеми b и k^{*m}.

Если $b' = ba^m$, где $a,\ b \in k$, то, очевидно,

$$k\left(b'^{1/m}\right) = k\left(b^{1/m}\right).$$

Следовательно, $k\left(B^{1/m}\right) = K$, что и требовалось доказать.

В случае когда мы имеем дело с абелевыми расширениями показателя p, равного характеристике, мы должны развить аддитивную теорию, находящуюся к теоремам 13 и 14 в таком же отношении, как теорема 11 к теореме 10.

Пусть k — поле характеристики p. Определим оператор $\wp$, положив

$$\wp(x) = x^p - x$$

для $x \in k$. Тогда $\wp$ есть аддитивный гомоморфизм поля k в себя. Подгруппа $\wp(k)$ играет ту же роль, что и подгруппа k^{*m} в мультипликативной теории для случая, когда m — простое число. Теория, касающаяся степеней p, несколько сложнее и принадлежит Витту. Читателя, желающего посмотреть, как она выглядит, мы отсылаем к упражнениям.

Корень многочлена $X^p - X - a$ с $a \in k$ будем обозначать через $\wp^{-1}a$. Для всякой подгруппы B в k, содержащей $\wp k$, положим $K_B = k\left(\wp^{-1}B\right)$. Это поле, полученное присоединением $\wp^{-1}a$ к k для всех $a \in B$. Подчеркнем тот факт, что B — *аддитивная* подгруппа в k.

Теорема 15. *Пусть k — поле характеристики p. Отображение $B \longmapsto k\left(\wp^{-1}B\right)$ является биективным соответствием между подгруппами в k, содержащими $\wp k$, и абелевыми расширениями поля k, имеющими показатель p. Пусть $K = K_B = k\left(\wp^{-1}B\right)$ и G — группа Галуа этого расширения. Имеет место билинейное отображение*

$$G \times B \to \mathbf{Z}/p\mathbf{Z}, \text{ задаваемое правилом } (\sigma,\ a) \longmapsto \langle \sigma,\ a \rangle.$$

Если $\sigma \in G$, $a \in B$ и $\wp\alpha = a$, то $\langle \sigma,\ a \rangle = \sigma\alpha - \alpha$. Ядро слева равно 1, а ядро справа есть $\wp k$. Расширение K_B/k конечно тогда и только тогда, когда индекс $(B : \wp k)$ конечен, и в этом случае

$$[K_B : k] = (B : \wp k).$$

Доказательство. Доказательство полностью аналогично доказательствам теорем 13 и 14. Оно может быть получено заменой умножения сложением и использованием „$\wp$-х корней“ вместо корней m-й степени. Никаких других изменений в доказательстве не требуется.

Аналогичная теорема для абелевых расширений показателя p^n требует векторов Витта и будет изложена в упражнениях.