для всех $x \in K$. Поскольку $K$ бесконечно, это возможно только при $s = r$. Но тогда $\sigma_i = \sigma_j$ вопреки тому факту, что мы начинали с различных автоморфизмов.

## § 12. Теорема о нормальном базисе

Теорема 20. *Пусть $K/k$ — конечное расширение Галуа степени $n$ и $\sigma_1, \ldots, \sigma_n$ — элементы его группы Галуа $G$. Тогда существует элемент $w \in K$, такой, что $\sigma_1 w, \ldots, \sigma_n w$ образуют базис $K$ над $k$.*

Доказательство. Здесь мы докажем это только для случая, когда $k$ бесконечно. В случае конечного поля $k$ доказательство можно будет провести позднее методами линейной алгебры как упражнение.

Для всякого $\sigma \in G$ пусть $X_\sigma$ — переменная и $t_{\sigma, \tau} = X_{\sigma^{-1}\tau}$. Положим $X_i = X_{\sigma_i}$. Пусть

$$f(X_1, \ldots, X_n) = \det(t_{\sigma_i, \sigma_j}).$$

Тогда $f$ не является тождественным нулем, что видно, если подставить 1 вместо $X_{\mathrm{Id}}$ и 0 вместо $X_\sigma$ для $\sigma \neq \mathrm{id}$. Так как $k$ бесконечно, то по теореме 19 определитель не может быть равным нулю при всех $x \in K$, если мы в $f$ подставим $\sigma_i(x)$ вместо $X_i$. Следовательно, существует элемент $w \in K$, для которого

$$\det(\sigma_i^{-1}\sigma_j(w)) \neq 0.$$

Предположим, что элементы $a_1, \ldots, a_n \in k$ таковы, что

$$a_1\sigma_1(w) + \cdots + a_n\sigma_n(w) = 0.$$

Применим $\sigma_i^{-1}$ к этому соотношению для каждого $i = 1, \ldots, n$. Поскольку $a_j \in k$, мы получим систему линейных уравнений относительно неизвестных $a_j$. Так как определитель из коэффициентов $\neq 0$, то

$$a_j = 0 \quad \text{для} \quad j = 1, \ldots, n$$

и, следовательно, $w$ будет искомым элементом.

### УПРАЖНЕНИЯ

1. Пусть $k$ — поле, $X$ — переменная над $k$ и

$$\varphi(X) = \frac{f(X)}{g(X)}$$

— рациональная функция из $k(X)$, представленная в виде отношения двух взаимно простых многочленов $f$, $g$. Определим степень $\varphi$ как $\max(\deg f,$

$\deg g$) и положим $Y = \varphi(X)$. (а) Показать, что степень $\varphi$ равна степени расширения $k(X)$ над $k(Y)$ (в предположении, что $Y \notin k$). (б) Показать, что всякий автоморфизм поля $k(X)$ над $k$ может быть представлен рациональной функцией $\varphi$ степени 1 и, обратно, что всякая такая функция $\varphi$ определяет некоторый автоморфизм. (в) Показать, что эта группа автоморфизмов порождается следующими отображениями ($a$, $b \in k$):

$$X \longmapsto aX, \quad a \neq 0; \quad X \longmapsto X + b; \quad X \longmapsto \frac{1}{X}.$$

2. Пусть $k$ — поле из $q$ элементов и $K = k(X)$ — поле рациональных функций от одной переменной над $k$. Пусть $G$ — группа автоморфизмов поля $K$, задаваемых отображениями

$$X \longmapsto \frac{aX + b}{cX + d},$$

где $a$, $b$, $c$, $d$ лежат в $k$ и $ad - bc \neq 0$. Доказать следующие утверждения:

(i) Порядок $G$ равен $q^3 - q$.

(ii) Неподвижное поле группы $G$ равно $k(Y)$, где

$$Y = \frac{(X^{q^2} - X)^{q+1}}{(X^q - X)^{q^2+1}}.$$

(iii) Пусть $H_1$ — подгруппа в $G$, состоящая из отображений $X \longmapsto aX + b$ с $a \neq 0$. Неподвижное поле группы $H_1$ совпадает с $k(T)$, где $T = (X^q - X)^{q-1}$.

(iv) Пусть $H_2$ — подгруппа в $H_1$, состоящая из отображений $X \longmapsto X + b$ с $b \in k$. Неподвижное поле группы $H_2$ равно $k(Z)$, где $Z = X^q - X$.

3. Пусть $\overline{\mathbf{Q}}$ — фиксированное алгебраическое замыкание поля $\mathbf{Q}$, $E$ — максимальное подполе в $\overline{\mathbf{Q}}$, не содержащее $\sqrt{2}$ (такое подполе существует в силу леммы Цорна). Показать, что всякое конечное расширение поля $E$ — циклическое. (Ваше доказательство должно остаться пригодным, если вместо $\sqrt{2}$ взять любое алгебраическое иррациональное число.)

4. Пусть $k$ — поле, $\overline{k}$ — его алгебраическое замыкание, $\sigma$ — автоморфизм $\overline{k}$, оставляющий $k$ неподвижным, и $F$ — неподвижное поле относительно $\sigma$. Показать, что всякое конечное расширение поля $F$ — циклическое.

(Две предыдущие задачи — это примеры Артина, показывающие, как выкапывать ямы в алгебраически замкнутом поле.)

5. (i) Пусть $K$ — циклическое расширение поля $F$ с группой Галуа $G$, порожденной $\sigma$. Предположим, что характеристика равна $p$ и что $[K:F] = p^{m-1}$, где $m$ — некоторое целое число $\geqslant 2$. Пусть $\beta$ — элемент поля $K$, для которого $\mathrm{Tr}_F^K(\beta) = 1$. Показать, что в $K$ существует элемент $\alpha$, такой, что

$$\sigma\alpha - \alpha = \beta^p - \beta.$$

(ii) Доказать, что многочлен $X^p - X - \alpha$ неприводим в $K[X]$.

(iii) Доказать, что если $\theta$ — корень этого многочлена, то $F(\theta)$ — расширение Галуа поля $F$, циклическое и имеющее степень $p^m$, и что его группа Галуа порождается продолжением $\sigma^*$ автоморфизма $\sigma$, для которого

$$\sigma^*(\theta) = \theta + \beta.$$

6. Пусть $E$ — алгебраическое расширение поля $k$, такое, что всякий многочлен $f(X)$ из $k[X]$ степени $\geqslant 1$ имеет хотя бы один корень в $E$. Доказать, что $E$ алгебраически замкнуто. [*Указание*: рассмотреть отдельно

сепарабельный и чисто несепарабельный случай и воспользоваться теоремой о примитивном элементе.]

7. *Относительные инварианты* (Сато). Пусть $k$ — поле, $K$ — его расширение и $G$ — группа автоморфизмов $K$ над $k$, причем $k$ совпадает с неподвижным полем группы $G$. (Мы не предполагаем, что $K$ алгебраично над $k$.) Под *относительным инвариантом* группы $G$ в $K$ мы будем понимать элемент $P \in K$, $P \neq 0$, такой, что для всякого $\sigma \in G$ существует элемент $\chi(\sigma) \in k$, для которого $P^{\sigma} = \chi(\sigma) P$. Так как $\sigma$ — автоморфизм, то $\chi(\sigma) \in k^*$. Мы будем говорить, что отображение $\chi$: $G \to k^*$ *принадлежит* $P$, и будем называть его *характером*. Доказать следующие утверждения:

(а) Определенное выше отображение $\chi$ — гомоморфизм.

(б) Если один и тот же характер $\chi$ принадлежит относительным инвариантам $P$ и $Q$, то существует такой элемент $c \in k^*$, что $P = cQ$.

(в) Относительные инварианты образуют мультипликативную группу, которую мы обозначаем через $I$.

Элементы $P_1, \ldots, P_m$ из $I$ называются *мультипликативно независимыми* по модулю $k^*$, если их образы в факторгруппе $I/k^*$ мультипликативно независимы, т. е. если из соотношения

$$P_1^{\nu_1} \ldots P_m^{\nu_m} = c \in k^*,$$

где $\nu_1, \ldots, \nu_m$ — целые числа, следует, что $\nu_1 = \ldots = \nu_m = 0$.

(г) Доказать, что если $P_1, \ldots, P_m$ мультипликативно независимы по модулю $k^*$, то они алгебраически независимы над $k$. [*Указание*: воспользоваться теоремой Артина о характерах.]

(д) Пусть $K = k(X_1, \ldots, X_n)$ — поле частных кольца многочленов $k[X_1, \ldots, X_n] = k[X]$, причем $G$ индуцирует автоморфизмы этого кольца многочленов. Доказать: если $F_1(X)$ и $F_2(X)$ — относительно инвариантные многочлены, то их н. о. д. является относительным инвариантом; если $P(X) = F_1(X)/F_2(X)$ — относительный инвариант, являющийся отношением двух взаимно простых многочленов, то $F_1(X)$ и $F_2(X)$ — относительные инварианты. Доказать, что относительно инвариантные многочлены порождают $I/k^*$. Пусть $S$ — множество относительно инвариантных многочленов, которые не могут быть разложены в произведение двух относительно инвариантных многочленов степени $\geqslant 1$. Показать, что элементы из $S/k^*$ мультипликативно независимы и что, следовательно, $I/k^*$ — свободная абелева группа. [Если вы знакомы с понятием степени трансцендентности, то, используя (г), вы сможете заключить, что эта группа — конечно порожденная.]

8. Пусть $E$ — конечное сепарабельное расширение над $k$ степени $n$, $W = (w_1, \ldots, w_n)$ — система элементов из $E$ и $\sigma_1, \ldots, \sigma_n$ — различные вложения $E$ в $\bar{k}$ над $k$. Определим дискриминант системы $W$, положив

$$D_{E/k}(W) = \det(\sigma_i w_j)^2.$$

Доказать: (а) Если $V = (v_1, \ldots, v_n)$ — какая-нибудь другая система (столбец) элементов из $E$ и $X = (x_{ij})$ — матрица из элементов поля $k$, такая, что $W = XV$, то

$$D_{E/k}(W) = \det(X)^2 D_{E/k}(V).$$

(б) Дискриминант является элементом из $k$.

(в) Пусть $E = k(\alpha)$ и $f(X) = \operatorname{Irr}(\alpha, k, X)$. Пусть $\alpha_1, \ldots, \alpha_n$ — корни $f$ и, скажем, $\alpha = \alpha_1$. Тогда

$$f'(\alpha) = \prod_{j=2}^{n} (\alpha - \alpha_j).$$

Показать, что

$$D_{E/k}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N_k^E (f'(\alpha)).$$

(г) Пусть обозначения те же, что и в (а). Показать, что

$$\det(\mathrm{Tr}(w_i w_j)) = (\det(\sigma_i w_j))^2.$$

[*Указание*: пусть $A$ — матрица $(\sigma_i w_j)$. Показать, что ${}^tAA$ есть матрица $(\mathrm{Tr}(w_i w_j))$.]

**9.** Пусть $F$ — конечное поле и $K$ — его конечное расширение. Показать, что норма $N_F^K$ и след $\mathrm{Tr}_F^K$ сюръективны (как отображения $K$ в $F$).

**10.** Пусть $a \neq 0, \neq \pm 1$ — целое число, свободное от квадратов. Для каждого простого числа $p$ пусть $K_p$ — поле разложения многочлена $X^p - a$ над $\mathbf{Q}$. Показать, что $[K_p : \mathbf{Q}] = p(p-1)$. Для всякого целого числа $m > 0$, свободного от квадратов, пусть

$$K_m = \prod_{p \mid m} K_p$$

— композит всех полей $K_p$ с $p \mid m$, и пусть $d_m = [K_m : \mathbf{Q}]$ — степень $K_m$ над $\mathbf{Q}$. Показать, что если $m$ нечетно, то $d_m = \prod_{p \mid m} d_p$, а если $m$ четно, $m = 2n$, то $d_{2n} = d_n$ или $2d_n$, в зависимости от того, содержится или нет $\sqrt{a}$ в поле корней $m$-й степени из единицы $\mathbf{Q}(\zeta_m)$.

**11.** Пусть $A$ — абелева группа и $G$ — конечная циклическая группа с образующей $\sigma$, действующая на $A$ [посредством гомоморфизма $G \to \mathrm{Aut}(A)$]. Определим след $\mathrm{Tr}_G = \mathrm{Tr}$ на $A$, положив $\mathrm{Tr}(x) = \sum_{\tau \in G} \tau x$. Обозначим через $A_{\mathrm{Tr}}$ ядро следа и рассмотрим $(1-\sigma)A$ — подгруппу в $A$, состоящую из всех элементов вида $y - \sigma y$. Показать, что $H^1(G, A) \approx A_{\mathrm{Tr}}/(1-\sigma)A$.

**12.** Какова группа Галуа следующих многочленов: (а) $X^3 - X - 1$ над $\mathbf{Q}$. (б) $X^3 - 10$ над $\mathbf{Q}$. (в) $X^3 - 10$ над $\mathbf{Q}(\sqrt{2})$. (г) $X^3 - 10$ над $\mathbf{Q}(\sqrt{-3})$. (д) $X^3 - X - 1$ над $\mathbf{Q}(\sqrt{-23})$. (е) $X^4 - 5$ над $\mathbf{Q}$, $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{-5})$, $\mathbf{Q}(i)$. (ж) $X^4 - a$ над $\mathbf{Q}$, где $a$ — любое целое число $\neq 0, \neq \pm 1$ и свободное от квадратов. (з) $X^n - a$ над $\mathbf{Q}$, где $n$ нечетное $> 1$, $a$ — любое свободное от квадратов целое положительное число. (и) $X^4 + 2$ над $\mathbf{Q}$, $\mathbf{Q}(i)$. (к) $(X^2-2)(X^3-3)(X^2-5)(X^2-7)$ над $\mathbf{Q}$. (л) $(X^2 - p_1) \ldots (X^2 - p_n)$ над $\mathbf{Q}$ ($p_1, \ldots, p_n$ — различные простые числа). (м) $(X^3-2)(X^3-3)(X^2-2)$ над $\mathbf{Q}(\sqrt{-3})$. (н) $X^n - t$ над $\mathbf{C}(t)$, где $t$ трансцендентно над полем комплексных чисел $\mathbf{C}$, а $n$ — целое положительное число. (о) $X^4 - t$ над $\mathbf{R}(t)$, где $t$ такое же, как и выше.

**13.** Пусть $k$ — поле, $n$ — нечетное целое число $\geqslant 1$ и $\zeta$ — примитивный корень $n$-й степени из единицы, лежащий в $k$. Показать, что $k$ содержит также примитивный корень $2n$-й степени из единицы.

**14.** Пусть $k$ — конечное расширение поля рациональных чисел. Показать, что в $k$ имеется только конечное число корней из единицы.

**15.** Определить, какие корни из единицы имеются в следующих полях: $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{-2})$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{-5})$.

**16.** Для каких целых чисел $m$ примитивный корень $m$-й степени из единицы имеет степень 2 над $\mathbf{Q}$?

**17.** Пусть $k$ — поле характеристики 0, причем для всякого конечного расширения $E$ поля $k$ индекс $(E^*:E^{*n})$ конечен, каково бы ни было целое положительное $n$. Доказать, что для всякого такого $n$ существует только конечное число абелевых расширений над $k$ степени $n$.

**18.** Пусть $f(z)$ — рациональная функция с коэффициентами в конечном расширении поля рациональных чисел, причем существует бесконечно много корней из единицы $\zeta$, для которых $f(\zeta)$ есть корень из единицы. Показать, что существует такое целое число $n$, что $f(z)=cz^n$, где $c$ — некоторая константа (являющаяся на самом деле корнем из единицы).

Это упражнение может быть обобщено следующим образом. Пусть $\Gamma_0$ — конечно порожденная мультипликативная группа комплексных чисел и $\Gamma$ — группа всех комплексных чисел $\gamma$, таких, что $\gamma^m$ лежит в $\Gamma_0$ для некоторого целого $m\neq 0$. Пусть $f(z)$ — рациональная функция с комплексными коэффициентами, такая, что существует бесконечно много $\gamma\in\Gamma$, для которых $f(\gamma)$ лежит в $\Gamma$. Тогда снова $f(z)=cz^n$ для некоторых $c$ и $n$.

Мною дано доказательство соответствующего утверждения для случая, когда значения $\gamma$ и $f$ берутся в $\Gamma_0$, а не в $\Gamma$ (см. „Diophantine Geometry", гл. VII, теорема 7).

**19.** Пусть $K/k$ — расширение Галуа. На группе $G(K/k)=G$ определяем топологию Крулля, беря в качестве фундаментальной системы открытых окрестностей единицы множество подгрупп, которые принадлежат конечным расширениям $E$ поля $k$, содержащимся в $K$. Используя представление на левых смежных классах, находим, что нормальные подгруппы кофинальны в этом семействе и что, следовательно, семейство нормальных подгрупп, принадлежащих конечным нормальным расширениям, определяет ту же самую топологию. Показать, что группа $G$ алгебраически и топологически изоморфна проективному пределу конечных факторгрупп $G/U$, где $U$ пробегает все такие нормальные подгруппы. Вывести отсюда, что $G$ компактна и вполне несвязна. Такие группы называются *проконечными*. Показать, что всякая замкнутая подгруппа конечного индекса открыта. Показать, что замкнутые подгруппы — это в точности те подгруппы, которые принадлежат промежуточным подполям $k\subset F\subset K$. Показать, что если $H$ — произвольная подгруппа в $G$ и $F$ — ее неподвижное поле, то подгруппа в $G$, принадлежащая $F$, совпадает с замыканием $H$ в $G$.

**20.** Пусть $k$ — такое поле, что всякое его конечное расширение — циклическое и что для всякого целого $n$ оно имеет одно расширение степени $n$. Показать, что группа Галуа $G=G(\bar{k}/k)$ есть обратный предел $\varprojlim \mathbf{Z}/m\mathbf{Z}$, где $m\mathbf{Z}$ пробегает все подгруппы в $\mathbf{Z}$, упорядоченные по включению. Показать, что этот предел изоморфен прямому произведению пределов

$$\varinjlim_{n\to\infty} \mathbf{Z}/p^n\mathbf{Z},$$

взятому по всем простым числам $p$, другими словами, он изоморфен произведению всех аддитивных групп целых $p$-адических чисел.

**21.** *Векторы Витта.* Пусть $x_1, x_2, \ldots$ — последовательность алгебраически независимых элементов над кольцом целых чисел $\mathbf{Z}$. Для всякого $n\geqslant 1$ положим

$$x^{(n)}=\sum_{d\mid n} d x_d^{n/d}.$$

Показать, что $x_n$ может быть выражено через $x^{(d)}$, где $d\mid n$, с рациональными коэффициентами.

Используя векторную терминологию, мы называем $(x_1, x_2, \ldots)$ компонентами Витта вектора $x$, а $(x^{(1)}, x^{(2)}, \ldots)$ — его *призрачными* компонентами. Сам $x$ мы называем *вектором Витта*.

Рассмотрим степенной ряд

$$f_x(t) = \prod_{n \geqslant 1} (1 - x_n t^n).$$

Показать, что

$$-t \frac{d}{dt} \log f_x(t) = \sum_{n \geqslant 1} x^{(n)} t^n.$$

[Под $\frac{d}{dt} \log f(t)$ мы понимаем $f'(t)/f(t)$, где $f(t)$ — степенной ряд, производная которого $f'(t)$ берется формально.]

Если $x$, $y$ — два вектора Витта, то их сумму и произведение определяем покомпонентно *относительно призрачных компонент*, т. е. полагаем

$$(x \dot{+} y)^{(n)} = x^{(n)} \dot{+} y^{(n)}.$$

Каковы $(x + y)_n$? Показать, что

$$f_x(t) f_y(t) = f_{x+y}(t).$$

Стало быть, $(x + y)_n$ — многочлен с целочисленными коэффициентами от $x_1, y_1, \ldots, x_n, y_n$. Показать также, что

$$f_{xy}(t) = \prod_{d,\, e \geqslant 1} \left(1 - x_d^{m/d} y_e^{m/e} t^m\right)^{de/m},$$

где $m$ — наименьшее общее кратное $d$, $e$ и $d$, $e$ пробегают все целые числа $\geqslant 1$. Таким образом, $(xy)_n$ также есть многочлен от $x_1, y_1, \ldots, x_n, y_n$ с целочисленными коэффициентами.

Предыдущие соображения принадлежат Витту (устное сообщение) и отличаются от приведенных в его первоначальной работе.

Проверить, что формулы, выражающие компоненты $(x + y)_{p^n}$ и $(xy)_{p^n}$, зависят только от компонент $x_{p^k}$ и $y_{p^k}$, где $k = 0, 1, \ldots, n$.

Если $A$ — коммутативное кольцо, то, взяв гомоморфный образ кольца многочленов над $\mathbf{Z}$ в $A$, мы увидим, что можно определить сложение и умножение векторов Витта с компонентами в $A$ и что эти векторы Витта образуют кольцо $W(A)$. Показать, что $W$ есть функтор, т. е. что любой гомоморфизм $\varphi$ кольца $A$ в коммутативное кольцо $A'$ индуцирует гомоморфизм $W(\varphi)$: $W(A) \to W(A')$.

22. Пусть $p$ — простое число. Рассмотрим векторы Витта с компонентами, равными 0, за исключением тех, которые занумерованы степенями $p$. Применим log по основанию $p$ к номерам этих компонент, — так что мы будем писать $x_n$ вместо $x_{p^n}$. Например, $x_0$ теперь обозначает то, что раньше было $x_1$. Если $k$ — поле характеристики $p$, то тем же символом $W(k)$ обозначается совокупность векторов Витта только что указанного вида. В силу упражнения 21 $W(k)$ является кольцом. Для вектора Витта $x = (x_0, x_1, \ldots, x_n, \ldots)$ положим

$$Vx = (0, x_0, x_1, \ldots) \quad \text{и} \quad Fx = (x_0^p, x_1^p, \ldots).$$

Таким образом, $V$ есть оператор сдвига. Очевидно, $V \circ F = F \circ V$. Показать, что

$$(Vx)^{(n)} = px^{(n-1)} \quad \text{и} \quad x^{(n)} = (Fx)^{(n-1)} + p^n x_n.$$

Кроме того, по определению имеем

$$x^{(n)} = x_0^{p^n} + px_1^{p^{n-1}} + \ldots + p^n x_n.$$

**23.** Рассмотрим снова $W(k)$, где $k$ — поле характеристики $p$. Тогда $V$ — аддитивный эндоморфизм кольца $W(k)$ и $F$ — кольцевой гомоморфизм $W(k)$ в себя. Кроме того, для всякого $x \in W(k)$ имеем

$$px = VFx.$$

Если $x, y \in W(k)$, то $(V^i x)(V^j y) = V^{i+j}(F^j x, F^i x)$. Обозначая для $a \in k$ через $\{a\}$ вектор Витта $(a, 0, 0, \ldots)$, мы можем символически записать

$$x = \sum_{i=0}^{\infty} V^i \{x_i\}.$$

Показать, что если $x \in W(k)$ и $x_0 \neq 0$, то $x$ есть единица в $W(k)$. [*Указание*: имеем $1 - x\{x_0^{-1}\} = Vy$ и затем

$$x\{x_0^{-1}\} \sum_0^{\infty} (Vy)^i = (1 - Vy) \sum_0^{\infty} (Vy)^i = 1.\Big]$$

**24.** Пусть $n$ — целое число $\geqslant 1$, $p$, как обычно, — простое число и $k$ — поле характеристики $p$. Обозначим символом $W_n(k)$ кольцо усеченных векторов Витта $(x_0, \ldots, x_{n-1})$ с компонентами в $k$. Мы рассматриваем $W_n(k)$ как аддитивную группу. Для $x \in W_n(k)$ положим $\wp(x) = Fx - x$. Очевидно, $\wp$ — гомоморфизм. Если $K$ — расширение Галуа поля $k$, $\sigma \in G(K/k)$ и $x \in W_n(K)$, то мы можем определить $\sigma x$ как вектор с компонентами $(\sigma x_0, \ldots, \sigma x_{n-1})$. Доказать аналог теоремы 90 Гильберта для векторов Витта и показать, что первая группа когомологий тривиальна. [Берем вектор, след которого является единицей в $W_n(k)$, и тем же путем, что и в доказательстве теоремы 17, § 10, устанавливаем, что цикл является кограницей.]

**25.** Показать, что если $x \in W_n(k)$, то существует вектор $\xi \in W_n(\bar{k})$, для которого $\wp(\xi) = x$. Сделать это по индукции сначала для первой компоненты, а затем показать, что вектор $(0, \alpha_1, \ldots, \alpha_{n-1})$ лежит в образе $\wp$ тогда и только тогда, когда $(\alpha_1, \ldots, \alpha_{n-1})$ лежит в образе $\wp$. Доказать по индукции, что если $\xi, \xi' \in W_n(k')$ для некоторого расширения $k'$ поля $k$ и если $\wp\xi = \wp\xi'$, то $\xi - \xi'$ — вектор, компоненты которого лежат в простом поле. Следовательно, решения уравнения $\wp\xi = x$ для заданного $x \in W_n(k)$ отличаются все между собой на векторы с компонентами из простого поля, а таких векторов имеется $p^n$ штук. Полагаем

$$k(\xi) = k(\xi_0, \ldots, \xi_{n-1})$$

или символически

$$k(\wp^{-1}x).$$

Доказать, что это расширение Галуа поля $k$, и показать, что циклические расширения поля $k$, имеющие степень $p^n$, — это в точности расширения типа $k(\wp^{-1}x)$, где вектор $x$ таков, что $x_0 \notin \wp k$.

**26.** Развить теорию Куммера для абелевых расширений показателя $p^n$ поля $k$, используя $W_n(k)$. Другими словами, показать, что между подгруп-

пами $B$ в $W_n(k)$, содержащими $\wp W_n(k)$, и абелевыми расширениями указанного выше типа имеется биективное соответствие

$$B \longmapsto K_B,$$

где $K_B = k(\wp^{-1}B)$. Все это принадлежит Витту (см. Witt E., Journal für die reine und angewandte Mathematik, 1935 и 1936 гг.). Доказательства, с небольшими изменениями, те же самые, что и данные в тексте для теории Куммера.

27. Дать пример поля $K$, имеющего степень 2 над двумя различными подполями $E$ и $F$ соответственно, но такого, что $K$ не алгебраично над $E \cap F$.

28. Пусть $F = \mathbf{F}_p$ — простое поле характеристики $p$, $K$ — поле, полученное из $F$ присоединением всех примитивных корней $l$-й степени из единицы для всех простых чисел $l \neq p$. Показать, что $K$ алгебраически замкнуто. [*Указание*: показать, что если $q$ — простое число и $r$ — целое число $\geqslant 1$, то существует простое число $l$, такое, что период $p \bmod l$ равен $q^r$. Для этого используется старый прием Ван дер Вардена. Пусть $l$ — простое число, делящее целое число

$$b = \frac{p^{q^r}-1}{p^{q^{r-1}}-1} = (p^{q^{r-1}}-1)^{q-1} + q(p^{q^{r-1}}-1)^{q-2} + \ldots + q.$$

Если $l$ не делит $p^{q^{r-1}}-1$, то все готово. В противном случае $l = q$. Но при этом $q^2$ не делит $b$ и, следовательно, существует простое число $l \neq q$, делящее $b$. Тогда степень $F(\zeta_l)$ над $F$ есть $q^r$, так что $K$ содержит подполя произвольной степени над $F$.]