Дополнительные задачи.

(1) Пусть p — простое число, а n натуральное число. Докажите, что $n \mid \varphi(p^n - 1)$, где φ — функция Эйлера.
(2) Докажите, что при $a \neq 0$ многочлен $x^p - x - a$ неприводим над $\mathbb{F}_p$.
(3) $\alpha \in \mathbb{F}_{p^n}$ является образующей мультипликативной группы $\mathbb{F}_{p^n}^*$. Докажите, что минимальный многочлен элемента α не может быть возвратным.
(4) Каким может быть максимальный период последовательности, заданной возвратным многочленом степени n над полем $\mathbb{F}_p$?
(5) Найдите минимальный и характеристический многочлены автоморфизма Фробениуса $\Phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ (напомним, что $\Phi(z) = z^p$), рассматриваемого как линейный оператор на n-мерном линейном пространстве над $\mathbb{F}_p$.
(6) Верно ли, что любое инвариантное подпространство автоморфизма Фробениуса в конечном поле является подполем?
(7) Верно ли, что для любого натурального числа N можно найти такие p и n, что в мультипликативной группе поля $\mathbb{F}_{p^n}$ есть элемент порядка N? Как искать такие p и n в случае, когда они существуют?
(8) В каких случаях мультипликативная группа $(\mathbb{F}_p[x]/(Q(x)^k))^*$ является циклической? ($Q(x)$ — неприводимый многочлен, $k > 1$)? Интересны любые частичные результаты, даже для $Q(x) = x$.
(9) По многочлену $f(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ можно построить новый многочлен

$$P_f(x_1, \ldots, x_n) = \sum_{(a_1,\ldots,a_n)\in\mathbb{F}_p^n} f(a_1, \ldots, a_n) x_1^{a_1} \ldots x_n^{a_n}.$$

(Здесь при возведении в степень мы интерпретируем элементы $\mathbb{F}_p$ как натуральные числа от 0 до $p - 1$.) Докажите, что это отображение биективно на множестве многочленов, в которых все переменные входят в степенях, меньших p. Докажите, что при $p = 2$ это инволюция. Можно ли что-нибудь сказать об этом отображении при $p > 2$?

(10) Пусть α — обратимый элемент конечномерной алгебры A над конечным полем, L — линейная функция на A. Докажите, что $x_n = L(\alpha^n)$ является линейной рекуррентной последовательностью. Докажите, что любая линейная рекуррентная последовательность элементов конечного поля получается таким образом. Как связаны между собой характеристический многочлен рекуррентной последовательности и минимальный многочлен элемента α?

(11) Докажите, что мультипликативная группа кольца $\mathbb{Z}_{p^n}$ циклическая, если простое число p отлично от 2 и является произведением циклической на группу порядка два при $p = 2$, $n > 2$.

(12) Разложить на множители как многочлен над полем характеристики p (например, конечным полем) определитель

$$\det \begin{pmatrix} x_0 & x_0^p & x_0^{p^2} & x_0^{p^3} & \dots & x_0^{p^n} \\ x_1 & x_1^p & x_1^{p^2} & x_1^{p^3} & \dots & x_1^{p^n} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & x_n^p & x_n^{p^2} & x_n^{p^3} & \dots & x_n^{p^n} \end{pmatrix}.$$

Пусть $q = p^k$. Разложить на множители как многочлен над полем $\mathbb{F} \supset \mathbb{F}_q$ определитель

$$\det \begin{pmatrix} x_0 & x_0^q & x_0^{q^2} & x_0^{q^3} & \dots & x_0^{q^n} \\ x_1 & x_1^q & x_1^{q^2} & x_1^{q^3} & \dots & x_1^{q^n} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & x_n^q & x_n^{q^2} & x_n^{q^3} & \dots & x_n^{q^n} \end{pmatrix}.$$

(13) Пусть p и q разные простые числа. Найти количество неприводимых многочленов степени q над $\mathbb{F}_p$.

(14) Пусть $\mathbb{F}$ — конечное расширение $\mathbb{F}_p$, и $f(t) \in \mathbb{F}[t]$ такой многочлен, что $f(a+b) = f(a) + f(b)$ для всех $a, b \in \mathbb{F}$. Всегда ли можно представить многочлен в виде

$$f(t) = \lambda_0 t + \lambda_1 t^p + \lambda_2 t^{p^2} + \ldots + \lambda_m t^{p^m}?$$

А если $\mathbb{F}$ — бесконечное поле характеристики p?

(15) Докажите, что число неприводимых многочленов степени n над полем $\mathbb{F}_p$ равно

$$\frac{1}{n} \sum_{k|n} \mu(k) p^{\frac{n}{k}},$$

где μ — функция Мебиуса.

(16) Показать, что если α не квадрат в поле $\mathbb{F}$, то α не квадрат ни в каком расширении поля $\mathbb{F}$ нечетной степени и квадрат в каждом расширении четной степени.

(17) Пусть $f(x) \in \mathbb{F}[x]$ — многочлен, такой что $f' = 0$. Показать, что многочлен f приводим. Пусть $\beta \in \mathbb{F}_{q^2}$. Показать, что $\beta^{q+1} \in \mathbb{F}_q$. Показать, что для любого элемента $\alpha \in \mathbb{F}_q$ найдется $\beta \in \mathbb{F}_{q^2}$, такой что $\alpha = \beta^{q+1}$.

(18) Пусть $\alpha \in \mathbb{F}_q$ имеет порядок $q-1$. Показать, что тогда найдется $\beta \in \mathbb{F}_{q^2}$ порядка q^2-1, такой что $\alpha = \beta^{q+1}$.

(19) Доказать формальное равенство

$$\sum \frac{1}{\deg f^s} = \frac{1}{1-q^{1-s}},$$

где левая сумма берется по всем приведенным многочленам $f(x) \in \mathbb{F}_q[x]$.

Пусть $d(f)$ — количество приведенных делителей многочлена $f(x)$, и $\sigma(f) = \sum_{g|f} \deg g$, сумма по всем приведенным делителям. Показать, что

$$\sum_f \frac{d(f)}{\deg f^s} = \frac{1}{(1-q^{1-s})^2};$$

$$\sum_f \frac{\sigma(f)}{\deg f^s} = \frac{1}{(1-q^{1-s})(1-q^{1-s})}.$$