Векторные пространства и модули

A7-1. Множество W многочленов из $\mathbb{Z}[x]$ с четным свободным членом является модулем над $\mathbb{Z}[x]$. Является ли этот модуль: **а)** конечно порожденным? **б)** свободным?

A7-2. Убедитесь, что всякий конечно порожденный модуль является гомоморфным образом конечно порожденного свободного модуля. Задайте этот гомоморфизм явно и найдите его ядро для модуля W из предыдущей задачи.

A7-3. Обозначим через $\mathbb{H}_p$ поле вычетов $\mathbb{Z}/p\mathbb{Z}$, где p – простое. Сколько одномерных и двумерных подпространств имеется в векторном пространстве ${\mathbb{H}_p}^3$ и сколько прямых и плоскостей имеется в аффинном пространстве ${\mathbb{H}_p}^3$?

A7-4. Те же вопросы про n-мерные пространства над конечным полем $\mathbb{H}_q$ из q элементов.

A7-5. Пусть $A = (a_{ij})$ есть $n \times n$ матрица, у которой

$$a_{ni} = \sum_{j=1}^{n-1} \lambda_j a_{ji}$$

Решите систему линейных уравнений $Ax = 0$.

A7-6*. Целозначные многочлены. Пусть $M \subset \mathbb{Q}[t]$ – множество всех многочленов, принимающих целые значения при всех целых t (такие многочлены иногда называют *целозначными*). Убедитесь, что они составляют $\mathbb{Z}$-модуль и докажите, что

а) многочлены $\gamma_k(t) \stackrel{\text{def}}{=} \binom{t+k}{k} = \dfrac{\overbrace{(t+1)(t+2)\cdots(t+k)}^{k}}{k!}$ с $k = 0, 1, 2, \ldots$ составляют базис этого модуля (над $\mathbb{Z}$);

б) $\mathbb{Z}$-линейные гомоморфизмы $M \longrightarrow M$, перестановочные со всеми сдвигами

$$T_a: \ f(t) \longmapsto T_a f(t) \stackrel{\text{def}}{=} f(t+a)$$

составляют коммутативное кольцо, изоморфное $\mathbb{Z}[[\nabla]]$, где $M \xrightarrow{\nabla} M$ — разностный оператор, переводящий $f(t)$ в $\nabla f(t) \stackrel{\text{def}}{=} f(t) - f(t-1)$.

Приложение: расширения полей

A7-7. Докажите, что число элементов конечного поля является степенью простого числа.

A7-8. Пусть число p – простое, $q = p^n$, $s = p^m$, $\mathbb{H}_q$ и $\mathbb{H}_s$ — поля из q и s элементов соответственно. Пусть имеется ненулевой гомоморфизм $\mathbb{H}_q \longrightarrow \mathbb{H}_s$. Что можно сказать про n и m ?

A7-9. Убедитесь, что множество решений уравнения $x^{p^k} - x = 0$ в поле характеристики p является подполем.

A7-10. Какова максимальная степень неприводимого многочлена над $\mathbb{H}_p$, делящего $x^{p^k} - x$?

A7-11. Докажите, что имеются единственные с точностью до изоморфизмф поля из 4 и из 8 элементов. Укажите явные конструкции этих полей в виде алгебраических расширений их простого подполя $\mathbb{H}_2$.

А7-12. Пусть L - поле характеристики p . Докажите, что сопоставление $x \mapsto x^p$ (называемое *гомоморфизмом Фробениуса*)

а) является гомоморфным вложением поля в себя;

б) оставляет на месте все элементы простого подполя;

в) является *автоморфизмом* (т. е. изоморфизмом на себя), если поле L конечно;

А7-13*. Докажите, что для любого натурального n и любого простого p существует поле $\mathbb{H}_q$ из $q = p^n$ элементов.

А7-14*. Докажите, что два конечных поля $\mathbb{H}_{q_1}$ и $\mathbb{H}_{q_2}$ изоморфны тогда и только тогда, когда $q_1 = q_2$.

А7-15*. Докажите, что всякий автоморфизм конечного поля является итерацией автомоморфизма Фробениуса. Сколько всего имеется автоморфизмов у поля $\mathbb{H}_{p^n}$?

А7-16*. Докажите, что если неприводимый многочлен из $\mathbb{H}_p[x]$ имеет корень в $\mathbb{H}_{p^n}$, то он полностью разлагается на линейные множители в $\mathbb{H}_{p^n}[x]$.

А7-17*. Используя надлежащую версию обращения Мёбиуса, докажите, что число неприводимых многочленов степени n над полем $\mathbb{Z}/p\mathbb{Z}$ равно $\dfrac{1}{n}\sum\limits_{d|n}\mu\left(\dfrac{n}{d}\right)p^d$.