Введение в теорию полей

Листок 2

Линейные пространства, базисы. Алгебраические расширения полей. Поле разложения многочлена

Определение 1. Пусть $\mathbb{F}$ — поле, $\mathbf{V}$ — множество с операциями сложения и умножения слева на элементы этого поля.

Множество $\mathbf{V}$ называется *линейным* (*векторным*) *пространством* над $\mathbb{F}$, если выполнены следующие аксиомы:

1)–4) Множество $\mathbf{V}$ является абелевой группой по сложению;

5) $\forall \alpha, \beta \in \mathbb{F}\ \forall x \in \mathbf{V}\ (\alpha\beta) \cdot x = \alpha \cdot (\beta \cdot x)$;

6) $\forall \alpha, \beta \in \mathbb{F}\ \forall x \in \mathbf{V}\ (\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$;

7) $\forall \alpha \in \mathbb{F}\ \forall x, y \in \mathbf{V}\ \alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$;

8) $\forall x \in \mathbf{V}\ 1 \cdot x = x$.

Элементы множества $\mathbf{V}$ принято называть *векторами.*

Задача 1. Найдите аксиому, которая следует из остальных, и выведите ее.

Задача 2. Выведите из аксиом, что $\forall x \in \mathbf{V}\ 0 \cdot x = 0$.

Задача 3. Какие из следующих множеств являются линейными пространствами над соответствующими полями:

а) векторы координатной действительной плоскости относительно сложения векторов и умножения их на числа;

б) последовательности длины n действительных чисел относительно покомпонентного их сложения и умножения на числа;

в) бесконечные последовательности нулей и единиц относительно сложения по модулю два над полем $\mathbb{Z}_2$;

г) многочлены степени не выше n над полем действительных чисел;

д) многочлены степени выше n над полем действительных чисел;

е) множество векторов вида $(a, 2a)$, где $a \in \mathbb{R}$;

ж) множество векторов вида (a, a^2), где $a \in \mathbb{R}$;

з) множество векторов вида $(a, a + 1)$, где $a \in \mathbb{R}$;

и) поле над своим подполем?

Определение 2. Если $\{v_1, \dots, v_n\}$ — любой конечный набор векторов линейного пространства $\mathbf{V}$ над полем $\mathbb{F}$, $\lambda_1, \dots, \lambda_n \in \mathbb{F}$, то сумма

$$\lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n$$

называется *линейной комбинацией* векторов $v_1, \dots, v_n$.

Задача 4. Пусть $\mathbf{V}$ — линейное пространство над полем $\mathbb{F}$, $X \subset \mathbf{V}$ — некоторое множество векторов из $\mathbf{V}$ (возможно, бесконечное). Докажите, что множество $\mathbf{U}$ всех возможных комбинаций векторов их X образует линейное пространство (*подпространство* в $\mathbf{V}$, минимальное из всех, содержащих множество X). Подпространство $\mathbf{U}$ называется *линейной оболочкой* множества векторов X.

Задача 5. Найдите линейную оболочку множества квадратных трехчленов в пространстве многочленов с действительными коэффициентами.

Определение 3. Множество векторов $\{v_i \mid i \in I\}$ линейного пространства $\mathbf{V}$ над полем $\mathbb{F}$ называется *линейно зависимым*, если существуют индексы $i_1, \dots, i_k \in I$ и ненулевые элементы $\lambda_1, \dots, \lambda_k \in \mathbb{F}$ такие, что

$$\lambda_1 v_{i_1} + \dots + \lambda_k v_{i_k} = 0.$$

В противоположном случае множество векторов называется *линейно независимым.*

Задача 6. Докажите, что множество векторов линейно зависимо тогда и только тогда, когда один из векторов является линейной комбинацией остальных.

Задача 7. Как должны быть расположены два вектора на плоскости, чтобы быть линейно независимыми? А три вектора?

Определение 4. Множество векторов линейного пространства $\mathbf{V}$ называется его *базисом*, если оно линейно независимо и его линейная оболочка совпадает с $\mathbf{V}$. Если у линейного пространства существует конечный базис, то оно называется *конечномерным.*

Задача 8. Для каждого линейного пространства из задачи 3 приведите пример какого-то его базиса. Приведите пример поля, которое не является конечномерным линейным пространством над своим подполем.

Задача 9. Пусть $X = \{v_1, v_2, \dots, v_n\}$ и $Y = \{u_1, \dots, u_k, \dots\}$ — два базиса одного и того же линейного пространства $\mathbf{V}$. Докажите, что тогда существует $u_l \in Y$ такой, что множество $X' = \{u_l, v_2, \dots, v_n\}$ также является базисом.

Задача 10. Выведите из предыдущей задачи, что в конечномерном пространстве все базисы содержат одинаковое количество элементов. Это количество называется *размерностью* линейного пространства (обозначение: $\dim_{\mathbb{F}} \mathbf{V}$).

Задача 11. Сколько векторов в линейном пространстве размерности n над полем из q элементов?

Определение 5. Поле $\mathbb{L}$ называется *расширением* поля $\mathbb{K}$, если $\mathbb{K}$ является подполем в $\mathbb{L}$. Расширение $\mathbb{L}$ поля $\mathbb{K}$ называется *конечным*, если $\dim_{\mathbb{K}} \mathbb{L} < \infty$. Число $\dim_{\mathbb{K}} \mathbb{L}$ в этом случае называется *степенью* расширения $\mathbb{L}$.

Элемент $x \in \mathbb{L}$ называется *алгебраическим* над $\mathbb{K}$, если он удовлетворяет некоторому нетривиальному алгебраическому уравнению с коэффициентами из $\mathbb{K}$, и *трансцендентным* в противном случае. Расширение $\mathbb{L}$ поля $\mathbb{K}$ называется *алгебраическим*, если всякий его элемент алгебраичен над $\mathbb{K}$.

Задача 12. Докажите, что любое конечное расширение поля является алгебраическим. Является ли алгебраическим расширением $\mathbb{R}$ над $\mathbb{Q}$?

Задача 13. Пусть $\mathbb{K}$ — поле, $\mathbb{K}[x]$ — многочлены над этим полем, $f(x) \in \mathbb{K}[x]$ — произвольный многочлен степени n. Докажите, что множество $\mathbb{L}$ остатков от деления многочленов из $\mathbb{K}[x]$ на многочлен $f(x)$ с операциями сложения и умножения остатков по модулю этого многочлена является полем тогда и только тогда, когда многочлен $f(x)$ неприводим над $\mathbb{K}$. Докажите, что в этом случае $\mathbb{L}$ является конечным расширением поля $\mathbb{K}$ степени n (*простое расширение*).

Задача 14. Как с помощью предыдущей задачи построить поле комплексных чисел из поля действительных чисел; поля из 4, 8, 9 элементов?

Задача 15 (Теорема о башне полей). Если $\mathbb{L}$ — конечное расширение поля $\mathbb{K}$, а $\mathbb{M}$ — конечное расширение поля $\mathbb{L}$, то $\mathbb{M}$ — конечное расширение поля $\mathbb{K}$, причем

$$\dim_{\mathbb{K}} \mathbb{M} = \dim_{\mathbb{K}} \mathbb{L} \cdot \dim_{\mathbb{L}} \mathbb{M}.$$

Определение 6. Расширение $\mathbb{L}$ поля $\mathbb{K}$ называется *полем разложения* многочлена $f \in \mathbb{K}[x]$ (не обязательно неприводимого), если f разлагается в $\mathbb{L}[x]$ на линейные множители и поле $\mathbb{L}$ порождается над $\mathbb{K}$ его корнями.

Гомоморфизмы (в частности, изоморфизмы) расширений поля $\mathbb{K}$, тождественные на $\mathbb{K}$, называются *гомоморфизмами* (*изоморфизмами*) *над* $\mathbb{K}$.

Задача 16. Поле разложения любого многочлена $f \in \mathbb{K}[x]$ существует.

Задача 17. Пусть $\mathbb{K}(\alpha)$ — расширение поля $\mathbb{K}$, полученное присоединением корня α неприводимого многочлена $h \in \mathbb{K}[x]$, и φ — гомоморфизм поля $\mathbb{K}$ в некоторое поле $\mathbb{F}$. Гомоморфизм φ продолжается до гомоморфизма $\psi : \mathbb{K}(\alpha) \to \mathbb{F}$ ровно столькими способами, сколько различных корней имеет в $\mathbb{F}$ многочлен $\varphi(h)$, полученный из h применением к его коэффициентам гомоморфизма φ.

Задача 18. Поле разложения любого многочлена $f \in K[x]$ единственно с точностью до изоморфизма над K.

Задача 19. Какая степень может быть у поля разложения кубического многочлена над полем K, $\operatorname{char} K \neq 2$?