Алгебра — I

Листок 9′ (дополнительный)

Расширения полей.

1. (a) Пусть p — простое, $q = p^k$. Докажите, что поле $\mathbb{F}_q$ порождено над $\mathbb{F}_p$ одним элементом.

   (b) Докажите, что для любого натурального k существует неприводимый многочлен степени k над $\mathbb{F}_p$.

2. Докажите, что группа автоморфизмов конечного поля $\mathbb{F}_q$ порождена автоморфизмом Фробениуса $a \mapsto a^p$, где p — простое число и $q = p^k$. Каков порядок этой группы?

3. Докажите, что любой неприводимый многочлен $f(x) \in \mathbb{F}_p[x]$, имеющий корень в $\mathbb{F}_{p^k}$, разлагается в $\mathbb{F}_{p^k}[x]$ на линейные множители.

4. Пусть $\Bbbk \subset \mathbb{F}$ — расширение полей. Элемент $a \in \mathbb{F}$ называется *алгебраическим* над $\Bbbk$, если он является корнем некоторого ненулевого многочлена $f(x) \in \Bbbk[x]$, и *трансцендентным* над $\Bbbk$ в противном случае.

   (a) Докажите, что элемент $a \in \mathbb{F}$ является алгебраическим над $\Bbbk$ тогда и только тогда, когда $\Bbbk(a)$ (наименьшее подполе поля $\mathbb{F}$, содержащее $\Bbbk$ и a) конечномерно, как векторное пространство над $\Bbbk$.

   (b) Докажите, что если элемент $a \in \mathbb{F}$ является алгебраическим над $\Bbbk$, то $\Bbbk(a)$ изоморфно $\Bbbk[x]/(g_a)$, где $g_a \in \Bbbk[x]$ — минимальный многочлен элемента a, а если элемент $a \in \mathbb{F}$ трансцендентен над $\Bbbk$, то $\Bbbk(a)$ изоморфно полю рациональных функций $\Bbbk(x)$.

5. Расширение полей $\Bbbk \subset \mathbb{F}$ называется *алгебраическим*, если все элементы поля $\mathbb{F}$ алгебраические над $\Bbbk$. Поле называется *алгебраически замкнутым*, если любой многочлен над ним имеет в нем корень.

   (a) Пусть имеются три поля $\Bbbk \subset \mathbb{F} \subset \mathbb{L}$. Докажите, что если два из расширений $\Bbbk \subset \mathbb{F}$, $\mathbb{F} \subset \mathbb{L}$, $\Bbbk \subset \mathbb{L}$ являются алгебраическими, то и третье тоже является алгебраическим.

   (b) Докажите, что алгебраически замкнутое поле не имеет нетривиальных алгебраических расширений (то есть алгебраических расширений степени, большей 1).

   (c) * Докажите, что у каждого поля $\Bbbk$ есть *алгебраическое замыкание* $\overline{\Bbbk}$ — алгебраически замкнутое поле, являющееся алгебраическим расширением $\Bbbk$.

6. Пусть $\Bbbk \subset \mathbb{F}$ — расширение полей. Элементы $a_1, \dots, a_n \in \mathbb{F}$ называются *алгебраически независимыми* над $\Bbbk$, если для любого ненулевого многочлена $f(x_1, \dots, x_n) \in \Bbbk[x_1, \dots, x_n]$ его значение $f(a_1, \dots, a_n)$ не равно 0 в поле $\mathbb{F}$, и *алгебраически зависимыми* в противном случае. Рассмотрим множество $\mathcal{C}$ минимальных (по включению) подмножеств множества $\mathbb{F}$, алгебраически зависимых над $\Bbbk$, множество $\mathcal{I}$ подмножеств множества $\mathbb{F}$, алгебраически независимых над $\Bbbk$, и множество $\mathcal{B}$ максимальных (по включению) подмножеств множества $\mathbb{F}$, алгебраически независимых над $\Bbbk$.

   (a) Докажите, что если $C_1, C_2 \in \mathcal{C}$, причем $C_1 \neq C_2$, и $e \in C_1 \cap C_2$, то существует $C_3 \in \mathcal{C}$, $C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$.

   (b) Докажите, что если $I_1, I_2 \in \mathcal{I}$, причем $|I_1| < |I_2| < \infty$, то существует $e \in I_2 \setminus I_1$, для которого $I_1 \cup \{e\} \in \mathcal{I}$.

   (c) Докажите, что если множество $\mathcal{B}$ содержит конечное подмножество $B \subset \mathbb{F}$, $|B| = n$, то все элементы $\mathcal{B}$ являются конечными множествами с одинаковым числом элементов n. (В этом случае n называется степенью трансцендентности $\mathbb{F}$ над $\Bbbk$; в противном случае говорят, что степень трансцендентности бесконечна.)

   (d) * Докажите, что множество $\mathcal{B}$ непусто, причем для любых $B_1, B_2 \in \mathcal{B}$ и любого $a \in B_1 \setminus B_2$ существует $b \in B_2 \setminus B_1$ такой, что $(B_1 \setminus \{a\}) \cup \{b\} \in \mathcal{B}$.

   (e) * Пусть все элементы $\mathcal{B}$ — бесконечные множества (то есть степень трансцендентности $\mathbb{F}$ над $\Bbbk$ бесконечна). Докажите, что все они равномощны.

7. (a) Докажите, что степень трансцендентности $\mathbb{C}$ над $\mathbb{Q}$ бесконечна.

   (b) Докажите, что любое поле характеристики ноль, чья степень трансцендентности над $\mathbb{Q}$ конечна (или даже счетна), можно вложить в $\mathbb{C}$.

   (c) Докажите теорему Гамильтона–Кэли (для произвольного поля), используя только то, что матрица любого комплексного линейного оператора приводится к верхнетреугольному виду, и то, что $n \times n$ матрица, характеристический многочлен которой имеет n разных корней, диагонализуема.

   (Указания: теорема Гамильтона–Кэли состоит в том, что некоторый определенный набор из n^2 многочленов с целыми коэффициентами от коэффициентов матрицы $A = (a_{ij})$ (а именно, коэффициенты матрицы $\chi_A(A)$) обращается в ноль тождественно на элементах поля. Для диагональных и, следовательно, для диагонализуемых матриц это верно. Проверьте, что диагонализуемые матрицы плотны в пространстве всех комплексных $n \times n$ матриц, и что полином, обращающийся в ноль на всюду плотном подмножестве пространства $\mathbb{C}^N$, тождественно равен нулю. Воспользуйтесь вложением поля частных кольца многочленов $\mathbb{Z}[a_{11}, \dots, a_{nn}]$ в поле комплексных чисел, чтобы установить, что упомянутые целочисленные многочлены — нулевые и, следовательно, обращаются в нуль на элементах любого поля.)