Для зачета по каждому листку надо сдать все задачи со звездочками, либо все задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

Алгебра 4: алгебраические числа

Алгебраические числа

Определение 4.1. Пусть $k \subset K$ – поле, содержащееся в поле K (в такой ситуации говорится, что k **подполе** в K, а K **расширение** k). Элемент $x \in K$ называется **алгебраическим над** k, если x – корень ненулевого многочлена с коэффициентами в k.

Довольно часто, когда говорят про алгебраические числа, подразумевают комплексные числа, алгебраические над $\mathbb{Q}$, т.е. корни многочленов с рациональными коэффициентами.

Задача 4.1. Пусть k – подполе в K, а x – элемент в K. Рассмотрим K как линейное пространство над k. Пусть $K_x \subset K$ – линейное подпространство K, порожденное степенями x. Докажите, что K_x конечномерно тогда и только тогда, когда x алгебраично.

Задача 4.2. Пусть k – подполе в K, x – алгебраический элемент в K, а $K_x \subset K$ – линейное подпространство, порожденное степенями x. Для ненулевого вектора $v \in K_x$, рассмотрим операцию m_v домножения на v в K. Докажите, что m_v – k-линейное отображение, которое сохраняет подпространство $K_x \subset K$.

Задача 4.3. В условиях предыдущей задачи, докажите, что ограничение гомоморфизма m_v на $K_x \subset K$ обратимо.

Задача 4.4 (!). Выведите из этого, что K_x – подполе в K.

Определение 4.2. Конечное расширение поля k – это поле $K \supset k$, которое конечномерно как векторное пространство над k.

Задача 4.5. Пусть $K_1 \supset K_2 \supset K_3$ поля, такие, что K_1 конечномерно над K_2, которое конечномерно над K_3. Докажите, что K_1 – конечное расширение K_3.

Задача 4.6 (!). Выведите из этого следующее: сумма, произведение, частное алгебраических над k элементов снова алгебраично над k.

Задача 4.7. Докажите, что любое конечное поле – конечное расширение поля остатков по модулю p для какого-то простого числа p. Выведите из этого, что конечное поле имеет p^n элементов (для каких-то чисел p, n, p простое).

Задача 4.8 (*). Докажите, что существует неалгебраическое комплексное число.

Задача 4.9 (**). Докажите, что вещественное число число $0,0100100001000000001...$ (число нулей после i-й единицы равно 2^i) неалгебраично.

Задача 4.10 (*). Пусть комплексное число x алгебраично. Докажите, что его комплексно-сопряженное $\overline{x}$ тоже алгебраично.

Указание. Воспользуйтесь тем, что комплексное сопряжение есть автоморфизм $\mathbb{C}$, сохраняющий $\mathbb{Q}$.

Задача 4.11 (*). Пусть комплексное число $x = a + b\sqrt{-1}$ алгебраично. Докажите, что вещественные числа a и b алгебраичны.

Алгебраическое замыкание

Задача 4.12. Пусть $P(t), Q(t) \in k[t]$ – полиномы положительной степени над полем k, не имеющие общих делителей. Докажите, что 1 можно выразить как линейную комбинацию P и Q над $k[t]$:

$$1 = Q(t)A(t) + P(t)B(t).$$

Указание. Воспользуйтесь алгоритмом Евклида для полиномов (делением в столбик с остатком и индукцией).

Задача 4.13. Пусть $P(t)$ – неприводимый полином (не раскладывается в произведение многочленов положительной степени с коэффициентами из k), а произведение $Q(t)Q_1(t)$ делится на $P(t)$, где $Q(t)$, $Q_1(t)$ – ненулевые полиномы. Докажите, что $Q(t)$ или $Q_1(t)$ делится на $P(t)$.

Указание. Пусть $Q(t)$ не делится на $P(t)$. Воспользуйтесь предыдущей задачей, чтобы выразить 1 как линейную комбинацию $Q(t)$ и $P(t)$:

$$1 = Q(t)A(t) + P(t)B(t).$$

Тогда $1 \cdot Q_1(t) = Q(t)Q_1(t)A(t) + P(t)B(t)Q_1(t)$ очевидно делится на $P(t)$.

Задача 4.14. Пусть $P(t)$ – многочлен над k. Рассмотрим кольцо $k[t]$ полиномов от t и факторпространство $k[t]/Pk[t]$ всех полиномов по полиномам, которые делятся на P. Докажите, что $k[t]/Pk[t]$ есть кольцо (относительно естественных операций умножения и сложения).

Задача 4.15. Докажите, что умножение на полином $Q(t)$ действует на $k[t]/Pk[t]$ как эндоморфизм (эндоморфизм это гомоморфизм из пространства в себя).

Задача 4.16. Пусть умножение на полином $Q(t)$ действует на $k[t]/Pk[t]$ нулем. Докажите, что Q делится на P в кольце $k[t]$.

Задача 4.17. Пусть $P(t)$ неприводим. Предположим, что $Q(t)$ – полином, который не делится на $P(t)$. Докажите, что оператор умножения m_Q на $Q(t)$ на пространстве $k[t]/Pk[t]$ – мономорфизм.

Указание. Пусть v лежит в ядре m_Q, а $Q_1(t)$ – полином, представляющий v. Тогда QQ_1 делится на P в силу утверждения предыдущей задачи. Воспользуйтесь алгоритмом Евклида для полиномов, чтобы получить, что Q делится на P либо Q_1 делится на P.

Задача 4.18 (*). Пусть $A: V \longrightarrow V$ - линейный оператор. Докажите, что есть такой полином $P(t) = t^n + a_n t^{n-1} + ...$, что $P(A) = 0$. Всегда ли можно найти неприводимый полином $P(t)$ такой, что $P(A) = 0$?

Задача 4.19 (!). Пусть $P(t)$ неприводим. Докажите, что $k[t]/Pk[t]$ – поле.

Указание. Воспользуйтесь предыдущей задачей, чтобы доказать, что если Q не делится на P, то умножение на $Q(t)$ задает на $k[t]/Pk[t]$ обратимый линейный оператор.

Определение 4.3. Пусть $P(t)$ – неприводимый полином. Говорится, что поле $k[t]/Pk[t]$ есть **расширение, полученное добавлением корня** $P(t)$.

Определение 4.4. Алгебраическое расширение поля k – это такое поле $K \supset k$, что все элементы K алгебраичны над k.

Задача 4.20. Докажите, что любое конечное расширение алгебраично.

Задача 4.21 (*). Докажите, что не любое алгебраическое расширение конечно.

Определение 4.5. Пусть k – поле. Поле k называется **алгебраически замкнутым**, если любой полином положительной степени $P \in k[t]$ имеет корень в k.

Определение 4.6. **Алгебраическое замыкание поля** k – это алгебраическое расширение $\overline{k} \supset k$, которое алгебраически замкнуто.

Задача 4.22 (*). Пусть K – расширение поля k, а $z \in K$ – корень ненулевого многочлена $P(t)$, коэффициенты которого алгебраичны над k. Докажите, что z алгебраичен над k.

Задача 4.23 (*). Пусть K – такое алгебраическое расширение поля k, что любой многочлен $P(t) \in k[t]$ имеет корень в K. Докажите, что любой многочлен $P(t) \in k[t]$ разлагается в произведение линейных многочленов из $K[t]$.

Задача 4.24 (*). В условиях предыдущей задачи докажите, что K алгебраически замкнуто.

Указание. Пусть $P \in K[t]$ – неприводимый многочлен с коэффициентами из K. Добавим его корень α к K. Воспользовавшись задачей 4.22, получаем, что α алгебраичен над k. Значит, α – корень многочлена из $k[t]$. Но любой такой многочлен разлагается в произведение $\prod(t-\alpha_i)$, $\alpha_i \in K$, как следует из предыдущей задачи. Выведите из этого, что $\alpha \in K$.

Задача 4.25 (*). Докажите, что у каждого поля k есть алгебраическое замыкание.

Указание. Возьмем любое алгебраическое расширение поля k. Если оно алгебраически замкнуто, мы все доказали. Иначе существует $P(t) \in k[t]$, который не имеет корней в K. Добавим к K его корень, получим поле K_1. Заменим K на K_1. Повторяя эту процедуру столько раз, сколько необходимо, перейдем к объединению всех алгебраических расширений k. Мы получим поле, которое содержит корень любого многочлена из $k[t]$. Воспользовавшись предыдущей задачей, убедитесь, что это поле алгебраически замкнуто.

Задача 4.26 (**). В наброске доказательства, приведенном выше, неявно использовалась лемма Цорна. Придумайте, для счетного поля k, доказательство, не использующее лемму Цорна, и независимое от аксиомы выбора.

Задача 4.27 (**). Можно ли доказать существование алгебраического замыкания для произвольного поля, не используя аксиому выбора?

Задача 4.28 (**). Докажите, что алгебраическое замыкание поля единственно с точностью до изоморфизма.