Теория Галуа 1: алгебраические числа

Правила: Зачеты по листкам бывают двух типов: когда сданы все (или 1/3, или 2/3) задачи со звездочками, либо все (или 1/3, или 2/3) 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.

Если сдана 1/3 задач с (*) и (!), студент получает $2t$ баллов, если 2/3 задач, $6t$ баллов, если все, кроме (максимум) двух – $10t$ баллов.

Если сдана 1/3 задач без звездочек и с (!), студент получает $2t$ баллов, если 2/3 задач, студент получает $6t$ баллов, если все, кроме (максимум) трех – $10t$ баллов.

Эти виды оценок не складываются, то есть больше $10t$ за листочек получить нельзя.

Коэффициент t равен 1.5, если задачи сданы не позже, чем через 20 дней после выдачи, 1, если между 20 и 35 днями, и 0.7, если позже.

Результаты сдачи записываются на листке ведомости, которая выдается студенту, и ее надо хранить до получения окончательных оценок по курсу.

1.1. Алгебраические числа

Определение 1.1. 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 1.1. 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.

Замечание 1.1. Если $k \subset K$ подполе K, а V, W - линейные пространства над K, мы можем рассмотреть V, W как линейные пространства V_k, W_k над k. В такой ситуации, линейное отображение $V_k \longrightarrow W_k$ называется **k-линейным отображением пространства V в W.** Линейные отображения векторных пространств над полем k часто называют **k-линейными**, чтобы обозначить зависимость от k.

Задача 1.2. Пусть $k \subset K$ - подполе K. Приведите пример отображения K-векторных пространств $V \longrightarrow W$, которое k-линейно, но не K-линейно.

Задача 1.3. 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 1.4. В условиях предыдущей задачи, докажите, что ограничение гомоморфизма m_v на $K_x \subset K$ обратимо.

Задача 1.5 (!). Выведите из этого, что K_x – подполе в K.

Определение 1.2. Конечное расширение поля k – это поле $K \supset k$, которое конечномерно как векторное пространство над k.

Задача 1.6. 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 1.7 (!). Выведите из этого следующее: сумма, произведение, частное алгебраических над k элементов снова алгебраично над k.

Задача 1.8. 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, где p простое).

Задача 1.9 (*). Докажите, что существует неалгебраическое комплексное число.

Задача 1.10 (**). а. Докажите, что вещественное число $0,0100010000000000000001...$ (число нулей после i-й единицы равно 2^{2^i}) неалгебраично.

б. Докажите, что вещественное число число $0,0100100001000...$ (число нулей после i-й единицы равно 2^i) неалгебраично.

Задача 1.11 (*). Пусть комплексное число x алгебраично. Докажите, что его комплексно-сопряженное $\bar{x}$ тоже алгебраично.

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

Задача 1.12 (*). Пусть комплексное число $x = a + b\sqrt{-1}$ алгебраично. Докажите, что вещественные числа a и b алгебраичны.

Задача 1.13 (*). Докажите, что $\alpha := \sin(\frac{n\pi}{m})$ алгебраично (над $\mathbb{Q}$) для всех целых n, m.

Алгоритм Евклида и его применения

Задача 1.14. 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 1.15. 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 1.16. 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 1.17. Докажите, что умножение на полином $Q(t)$ действует на $k[t]/Pk[t]$ как эндоморфизм (эндоморфизм это гомоморфизм из пространства в себя).

Задача 1.18. Пусть умножение на полином $Q(t)$ действует на $k[t]/Pk[t]$ нулем. Докажите, что Q делится на P в кольце $k[t]$.

Задача 1.19. 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 1.20 (*). Пусть $A: \ V \longrightarrow V$ - линейный оператор на конечномерном векторном пространстве. 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 1.21 (!). 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 1.3. Пусть $P(t)$ – неприводимый полином. Говорится, что поле $k[t]/Pk[t]$ есть **расширение, полученное добавлением корня** $P(t)$.

Определение 1.4. Алгебраическое расширение поля k – это такое поле $K \supset k$, что все элементы K алгебраичны над k.

Задача 1.22. Докажите, что любое конечное расширение алгебраично.

Задача 1.23 (*). Докажите, что не любое алгебраическое расширение конечно.