Георгий Потошин, 2024

Алгебра I, листочек 9

1. **Докажите, что $F \in \mathbb{k}[x]$, $F(\alpha) = 0,\ \alpha \in \mathbb{k}$ влечет $(x-\alpha)|F$ (теорема Безу). Докажите, что многочлен степени n над полем имеет не более n различных корней. Докажите, что группа**

$$\mu_n(\mathbb{k}) = \{\alpha \in \mathbb{k} | \alpha^n = 1\}$$

содержит не больше, чем n элементов.

Многочлены над полем можно делить с остатком. Поделим F на $(x-\alpha)$, мы получим следующее равенство $F = Q \cdot (x-\alpha) + \beta$. Если подставить в это равенство α, то занулится все, кроме β, тогда $0 = \beta$, что в точности означает, что F делится на $(x-a)$.

С другой стороны как мы видели ранее $\mathbb{k}[x]$ целостное кольцо главных идеалов, а значит в нём единственно разложение на неприводимые, которыми в частности являются многочлены степени 1, так как они просты в кольце. Тогда в единственном разложении будет только конечное число множителей степени 1, и так как степень многочлена равна сумме степеней его фактора, то у нас не может быть больше факторов, чем степень многочлена, в частности это касается факторов степени 1, а корней не меньше, чем типов факторов степени 1, так как каждому корню потенциально соответствует 1 или несколько факторов, как мы показали в предыдущем параграфе.

В частности в группе $\mu_n(\mathbb{k})$ лежат все корни $x^n - 1$, а их не больше n.

2. **Докажите, что конечная подгруппа мультипликативной группы поля циклична.**

Пусть G – конечная подгруппа мультипликативной группы поля порядка n, она абелева. Обозначим за $\psi(d) = \#\{a \in G | a^d = 1\}$. Так как $x^d = 1$ имеет решений в $\mathbb{k}$ не больше, чем n, то $\psi(d) \leq d$. Пусть для некого d есть элемент a этого порядка, обозначим за G_d множество элементов G порядка d, тогда очевидно, что $\langle a \rangle \subseteq \{a \in G | a^d = 1\}$, но $\#\langle a \rangle = d$, а $\#\{a \in G | a^d = 1\} \leq d$, тогда включение превратится в равенство. $\langle a \rangle$ циклическая группа порядка d, содержащая все корни $x^d - 1$. Тогда все элементы порядка d лежат в $\langle a \rangle$ и количество таких элементов $\phi(d)$. Тогда

$$n = \#G = \sum_{d|n} \#G_d \leq \sum_{d|n} \phi(d) = n$$

А значит $\#G_d = \phi(d)$, в частности это верно для n, а значит мы находим элемент порядка n. Он порождает всю группу G, тогда эта группа циклическая.

3. **Докажите, что если $[\mathbb{L} : \mathbb{K}] = 2$, то $\mathbb{L} = \mathbb{K}[\sqrt{\alpha}]$, где $\alpha \in \mathbb{K}$.**

Это не верно в случае, когда $\operatorname{char} K = 2$, так как мы можем положить $K = \mathbb{F}_2$ и $L = \mathbb{F}_2[x]/(1 + x + x^2)$. Для этого нужно проверить неприводимость $f(x) = 1 + x + x^2$, заметим, что никакой элемент K не является корнем $f(x)$, так как $f(0) = 1$ и $f(1) = 1$ и если бы $f(x)$ раскладывался в произведение многочленов меньшей степени, то они были бы степени 1 и были бы корни. Это означает, что $(f(x))$ максимальный идеал, так как кольцо $K[x]$ кольцо главных идеалов, а значит нет большего идеала, так как тогда бы $f(x)$ равнялся бы произведению двух многочленов меньшей степени и не был бы неприводимым. Тогда L поле, как фактор кольца по максимальному идеалу. При этом если бы $L = K[\sqrt{\alpha}]$, то $\sqrt{\alpha} \in L \setminus K$, а это только x и $1 + x$, но их квадраты $x^2 = x + 1$ и $(x+1)^2 = x$ не лежат в K, а значит такая конструкция невозможна.

Тем не менее если характеристика K не равна 2, то для некоторого $a \in L \setminus K$ $\{1, a, a^2\}$ линейно зависимы, а значит найдутся $b_0, b_1, b_2 \in K$, что $b_0 + b_1 a + b_2 x^2 = 0$. b_2 не может равняться нулю, так как иначе бы $a \in K$, но это не так. Тогда поделив на b_2 мы получим $a^2 + pa + q = 0$, так как характеристика не равна нулю, то $a^2 + pa + q = (a + p/2)^2 + q - p^2/4 = 0$, тогда можно положить $\alpha = p^2/4 - q \in K$, а $\sqrt{\alpha} = a + p/2 \in L$. Так как расширение имеет степень 2, а $\sqrt{\alpha}$ и 1 линейно независимы, то они образуют базис, а тогда они порождают L и утверждение доказано.

4.

5.

6.

7.

8. **Пусть $\mathbb{F}$ – конечное поле. Докажите, что любая функция $f : \mathbb{F} \to \mathbb{F}$ является многочленом. Приведите пример двух различных многочленов, задающих одинаковую функцию.**

   Это так, как можно для каждой функции записать интерполяционный многочлен Лагранжа. Пусть $\mathbb{F} = \{a_1, \dots, a_q\}$, тогда для любой $f : \mathbb{F} \to \mathbb{F}$ мы найдем $\phi : 1..q \to 1..q$, что $f(a_i) = a_{\phi(i)}$. Запишем многочлен, моделирующий эту функцию

   $$F = \sum_{i \in 1..q} a_{\phi(i)} \prod_{j \neq i, j \in 1..q} \frac{x - a_j}{a_i - a_j}$$

   Для поля $\mathbb{F}_2$ два многочлена 1, $1 + x + x^2$, как мы уже видели, моделируют одинаковые функции.

9. **Пусть $\mathbb{F}$ – произвольное поле ненулевой характеристики p и $\phi : \mathbb{F} \to \mathbb{F} = x \mapsto x^p$ – отображение. Докажите, что это гомоморфизм (гомоморфизм Фробениуса). Приведите два примера бесконечных полей характеристики p таких, что в первом случае ϕ биективен, а во втором – нет.**

   То что ϕ переводит произведение в произведение и единицу в единицу достаточно очевидно и не требует проверки, убедимся, что ϕ переводит сумму в сумму. Известно, что $(a + b)^p = a^p + b^p + \sum_{i=1}^{p-1} C_p^i a^i b^{p-i}$, но так как p просто и $C_p^i = p \cdot \ldots \cdot (p - i + 1)/i!$, то для $i \neq 0, p$ верно, что $p \mid C_p^i$, а тогда в биноме Ньютона все члены, кроме первого и последнего занулятся, а значит $\phi(a + b) = a^p + b^p$ и ϕ – гомоморфизм. Так как он гомоморфизм из поля, то он инъективен.

   Приведем теперь два примера. $F = \mathbb{F}_2(x)$ является полем, пусть $f(x) \in \operatorname{Im}\phi$, тогда $f(x) = (p(x)/q(x))^2$, где $p(x)/q(x)$ несократима, тогда в несократимом виде у $f(x)$ в числителе и знаменателе будут стоять многочлены четной степени, это означает, что мы не сможем получить например x возведением в квадрат, а значит ϕ не биекция.

   Пусть теперь $F = \mathbb{F}_2(\mathbb{Q}^+) = \operatorname{Frac}\mathbb{F}_2[\mathbb{Q}^+]$ Поле частных группового кольца, проверим, что это кольцо целостно. По определению $K = \mathbb{F}_2[\mathbb{Q}^+] = \{f : \mathbb{Q}^+ \to \mathbb{F}_2 \mid f \text{ почти всюду } 0\}$. Сложение устроено по точечно, а для $f, g \in K$ и $q \in \mathbb{Q}$ $(f \cdot g)(q) = \sum_{l \in \mathbb{Q}} f(l) g(q - l)$. Сумма корректна, так как ненулевые значения встречаются только конечное число раз, а произведение элементов равно нулю почти повсюду по тому же аргументу. Проверим, что произведение ненулевых элементов f, g не нуль. Пусть $a \in \mathbb{Q}$ – максимальное по условию $f(a) \neq 0$, аналогично $b \in \mathbb{Q}$ максимально по условию $g(b) \neq 0$, тогда очевидно, что $(g \cdot f)(a + b) = f(a)g(b) \neq 0$, а значит кольцо целостно и по нему можно брать поле частных. Теперь пусть $f = p/q \in F$, тогда положим $f' = p'/q'$ таким, что $p'(x) = p(2x)$, а $q'(x) = q(2x)$. Заметим, что характеристические функции $\{\chi_q\}_{q \in \mathbb{Q}}$ образуют базис K на $\mathbb{F}_2$, а значит например $p' = \chi_{q_1} + \ldots + \chi_{q_n}$, где q_i попарно различны, тогда $(p')^2 = (\chi_{q_1} + \ldots + \chi_{q_n})^2 = \chi_{q_1}^2 + \ldots + \chi_{q_n}^2 = \chi_{2q_1} + \ldots + \chi_{2q_n} = p$, а значит $(f')^2 = f$ и возведение в квадрат сюръективно и в купе с инъективностью биективно.