Георгий Потошин, 2024

Алгебра II, листочек 1

1. **Пусть $f(x), g(x) \in K[x]$. Пусть $h(x) \in \overline{K}[x]$ – НОД многочленов $f(x), g(x)$, рассмотренных как многочлены над алгебраическим замыканием $\overline{K}$. Докажите, что $h(x) \in K[x]$.**

   Пусть $\tilde{h}(x) \in K[x]$ – НОД многочленов $f(x), g(x)$ в $K[x]$. Тогда $\tilde{h}(x) \mid f(x), g(x)$, тогда $\tilde{h}(x) \mid h(x)$ в $\overline{K}[x]$ по свойству НОДа. С другой стороны есть соотношение Безу в $K[x]$, а именно мы найдём $u(x)$ и $v(x)$ в $K[x]$, что $\tilde{h}(x) = u(x)f(x) + v(x)g(x)$, и так как $h(x) \mid f(x), g(x)$ в $\overline{K}$, то $h(x) \mid \tilde{h}(x)$ в $\overline{K}[x]$. У нас есть делимость в обе стороны в $\overline{K}[x]$ и так как оба многочлена приведены, то они совпадают и $h(x) = \tilde{h}(x) \in K[x]$.

2. **Докажите, что если расширение L/K сепарабельно и чисто несепаребельно, то $L = K$.**

   Так как L/K сепарабельно, то каждый элемент $\alpha \in L$ имеет сепарабельный неприводимый минимальный многочлен $\mathrm{Irr}_\alpha^K(x)$. С другой стороны $\alpha^{p^n} \in K$ для $p = \mathrm{char}\, K > 0$ и для $n \geq 0$. Возьмём такое наименьшее n. Тогда $x^{p^n} - \alpha^{p^n} \in (\mathrm{Irr}_\alpha^K(x))_{K[x]}$, а значит $\mathrm{Irr}_\alpha^K(x) \mid x^{p^n} - \alpha^{p^n} = (x-\alpha)^{p^n}$. Это означает, что $\mathrm{Irr}_\alpha^K(x) = (x-\alpha)^m$, но так как это многочлен неприводим и сепарабелен, то $m = 1$. А значит $x - \alpha \in K[x]$ и $\alpha \in K$, откуда получаем, что $L = K$.

3. **Докажите, что любое конечное поле совершенно, то есть любое его алгебраическое расширение сепарабельно.**

   Пусть K – конечное поле характеристики p, а $\overline{K}$ его алгебраическое замыкание. Пусть $\alpha \in \overline{K}$, тогда $K(\alpha)$ конечное поле порядка q. Тогда полином $x^q - x$ очевидно зануляется на всех элементах $K(\alpha)$ и раскладывается в произведение различных мономов вида $x - a$, где $a \in K(\alpha)$ и коих ровно q штук. Тогда этот полином не имеет кратных корней и зануляет α, а тогда сепарабелен α. Это верно для всех элементов $\overline{K}$, а значит $\overline{K}/K$ сепарабельно и K идеально.

4. **Докажите, что если расширение L/K нормально, то расширение L^{sep}/K нормально.**

   Пусть $K < L < L^{\mathrm{sep}} < \overline{L} = \overline{K}$ – башня полей. Оба замыкания совпадают, так как $K < L$ в частности алгебраично. Пусть $\sigma : L^{\mathrm{sep}} \to \overline{K} = \overline{L}$ гомоморфизм над K. Тогда по нормальности $K < L$, $\sigma[L] = L$. Тогда для $\alpha \in L^{\mathrm{sep}}$ будет неприводимый сепарабельный многочлен $f(x)$. Тогда $f(x) = (x - \alpha_1) \dots (x - \alpha_n)$ не имеет кратных корней, тогда по инъективности σ, $f^\sigma(x) = (x - \alpha_1^\sigma) \dots (x - \alpha_n^\sigma)$ тоже и так как $f^\sigma(x) \in L[x]$ и $f^\sigma(\alpha^\sigma) = 0$, то α^σ сепарабелен над L и $\sigma[L^{\mathrm{sep}}] \subseteq L^{\mathrm{sep}}$.

   Для включения в обратную сторону заметим, что $f^{\sigma^{-1}}(x) \in L[x]$, так как $\sigma[L] = L$ и он однозначно определен, так как σ инъективен. Тогда мы знаем, что существуют $u, v \in L[x]$, что $fu + f'v = 1$. Тогда верно и $f^{\sigma^{-1}}u^{\sigma^{-1}} + (f^{\sigma^{-1}})'v^{\sigma^{-1}} = 1$, а значит $f^{\sigma^{-1}}$ не имеет кратных корней в $\overline{L}$, а тогда $f^{\sigma^{-1}} = (x - \alpha_1) \dots (x - \alpha_n)$, где очевидно $\alpha_i \in L^{\mathrm{sep}}$, так как они корни многочлена без кратных корней. Тогда по предыдущему наблюдению $\alpha_i^\sigma \in L^{\mathrm{sep}}$ тоже. Но так как α один из корней $f(x)$, то $\alpha = \alpha_i^\sigma$ для какого-то сигма, а тогда $L \subseteq \sigma[L]$, а значит $L^{\mathrm{sep}} = \sigma[L^{\mathrm{sep}}]$ и $K < L^{\mathrm{sep}}$ нормально.

5. **Докажите, что расширение $\mathbb{F}_p(x,y)/\mathbb{F}_p(x^p,y^p)$ чисто несепарабельно; проверьте, что $[F_p(x,y) : F_p(x^p,y^p)] = p^2$; убедитесь, что существует бесконечное количество промежуточных полей K таких, что**

   $$\mathbb{F}_p(x^p,y^p) < K < \mathbb{F}_p(x,y)$$

   Пусть $Q \in \mathbb{F}_p(x,y)$, тогда очевидно, что $Q^p \in \mathbb{F}_p(x^p,y^p)$, так как гомоморфизм фробениуса и каждое слагаемое будет возведено в степень p.

   Заметим, что в башне $\mathbb{F}_p(x^p,y^p) < \mathbb{F}_p(x,y^p) < \mathbb{F}_p(x,y)$ первый этаж является расширением по многочлену $t^p - x^p = (t-x)^p$, у которого единственный корень x и очевидно, что $(t-x)^i \notin \mathbb{F}_p(x^p,y^p)[t]$ для $0 < i < p$, так как свободным коэффициентом будет $x^i \notin \mathbb{F}_p(x^p,y^p)$. Тогда $t^p - x^p$ неприводим и $\mathbb{F}_p(x,y^p)$ – расширение по $t^p - x^p$ над $\mathbb{F}_p(x^p,y^p)$. И его степень расширения – p. Аналогично получим, что степень расширения второго этажа также p. Тогда степень $[F_p(x,y) : F_p(x^p,y^p)] = p^2$ равна произведению степеней.

Заметим, что для любого $\alpha \in \mathbb{F}_p(x, y) \setminus \mathbb{F}_p(x^p, y^p)$. Мы можем аналогично построить расширение по неприводимому многочлену $t^p - \alpha^p$, будем называть такое расширение K_α. Теперь осталось сделать правильный выбор таких α. Положим $\alpha_i = x^{ip+1} + y$. Пусть для краткости $K_{\alpha_i} = K_i$. Если $K_i = K_j$ для разных i и j, то

$$(x^{ip+1} + y) - x^{jp+1} + y = x^{ip+1} - x^{jp+1} \in K_i$$

тогда $x(x^{ip} - x^{jp}) \in K_i$, и так как $0 \neq x^{ip} - x^{jp} \in K_i$, то $x \in K_i$. Но тогда $y \in K_i$, а значит $K_i = \mathbb{F}_p(x, y)$, чего не может быть, так как тогда расширение будет степени p^2, а оно степени p.

6. **(Теорема о примитивном элементе) Пусть K – бесконечное поле, и $K(\alpha, \beta)/K$ – сепарабельное расширение, причем $[K(\alpha, \beta) : K] = n$ и $\mathrm{Aut}(K(\alpha, \beta)/K) = G$. Докажите, что**

   (a) **существует элемент $c \in K$ такой, что $|G(\alpha + c\beta)| = n$, то есть G-орбита $G(\alpha + c\beta)$ элемента $\alpha + c\beta$ содержит ровно n элементов**

   Как мне кажется в этом задании есть ошибка, так как вообще не факт, что в группе G найдется n различных элементов, так как каждый автоморфизм переставляет корни минимальных многочленов элементов α и β и этой перестановкой определен. Но у нас могут быть не все корни, и тогда элементов не хватит на n перестановок. Например есть расширение $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2})/\mathbb{Q}$. Поэтому нужно заменить автоморфизмы на вложения в поле разложения $\mathrm{Irr}^K_\alpha(x)$ и $\mathrm{Irr}^K_\beta(x)$, назовём это поле F.

   Так как расшерение сепарабельно, то существует ровно n вложений. Вообще вложения обычно рассматриваются в алгебраическое замыкание, но так как корни можно отправить только в корни того-же многочлена, то достаточно рассмотреть поле разложения. Если бы расширение было к тому же нормальным, то вложения были бы автоморфизмами, как в задаче и спрашивается. Назовем эти вложения σ_i для $1 \leq i \leq n$. Теперь пусть $c \in K$ такое, что $\sigma_i(\alpha) + c\sigma_i(\beta) = \sigma_j(\alpha) + c\sigma_j(\beta)$ для $i \neq j$. Тогда $c = (\sigma_i(\alpha) - \sigma_j(\alpha))/(\sigma_j(\beta) - \sigma_i(\beta))$. Выкинем все такие элементы, коих не больше n. Тогда возьмём какой-нибудь оставшийся ненулевой. Он всегда будет, так как поле K бесконечно. Тогда для такого c, вложения σ_i дадут нам n различных образов элемента $\alpha + c\beta$.

   (b) **если $|G(\alpha + c\beta)| = n$, то $[K(\alpha + c\beta) : K]_{sep} \geq n$**

   Так как мы получили n различных образов $\alpha + c\beta$, то у $\mathrm{Irr}^K_{\alpha+c\beta}(x)$ есть как минимум n корней и они различны. Тогда степень расширения равна степени полином, которая больше или равна n, в сепрабельном случае степень расширения совпадает с сепарабельной степенью.

   (c) **если $|G(\alpha + c\beta)| = n$, то $K(\alpha + c\beta) = K(\alpha, \beta)$**

   Но $K < K(\alpha + c\beta) \leq K(\alpha, \beta)$, а значит $[K(\alpha + c\beta) : K] \leq n$, но тогда там равенство и по мультипликативности степени будет $[K(\alpha + c\beta) : K(\alpha, \beta)] = 1$, то есть $K(\alpha + c\beta) = K(\alpha, \beta)$.

   (d) **если L/K конечно и сепарабельно, то $L = K(\alpha)$.**

   Как обычно построим башню.

   $$K < K(\alpha_1) < \ldots < K(\alpha_1, \ldots, \alpha_m) = L$$

   Пусть гипотезой индукции будет $K(\alpha_1, \ldots, \alpha_i) = K(\alpha)$ для некоторого α. Тогда для $i = 1$ она очевидно верна. Пусть она верна для $i = k$, тогда $K(\alpha_1, \ldots, \alpha_k, \alpha_{k+1}) = K(\alpha_1, \ldots, \alpha_k)(\alpha_{k+1}) = K(\alpha, \alpha_{k+1})$. Тогда по предыдущему пункту мы получим $K(\alpha, \alpha_{k+1}) = K(\alpha')$. По индукции это будет верно и для L.