Георгий Потошин, 2024

Алгебра I, листочек 10

1. **Положим $q = p^n$. Докажите, что поле $\mathbb{F}_q$ имеет единственное расширение степени k. Докажите, что $\overline{\mathbb{F}_p} = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$**

   Расширение степени k поля $\mathbb{F}_q$ будет иметь q^k, так как оно векторное пространство размерности k над $\mathbb{F}_q$. Точно также как на лекции заметим, что для $q' = q^k$, $x^{q'} - x$ имеет корнем любой элемент поля, так как для $x \in \mathbb{F}_{q'}$ либо $x = 0$, либо порядок ненулевого элемента делит порядок мультипликавной группы, а тогда $x^{q'-1} = 1$. При этом других коней у полинома нет, так как мы уже нашли их в количестве, равном его степени. Тогда $\mathbb{F}_{q'}$ является полем разложения многочлена $x^{q'} - x \in \mathbb{F}_q[x]$, как мы видели на лекции оно единственно и сущесвует.

   Пусть $L = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$. Покажем, что это поле. Пусть $\alpha, \beta \in L$, тогда можно предположить, что $\alpha \in \mathbb{F}_{p^m}$ и $\beta \in \mathbb{F}_{p^k}$, тогда на самом деле по предыдущему утверждению $\alpha, \beta \in \mathbb{F}_{p^{\mathrm{lcm}(k,m)}}$, значит определены их обратные, противоположные, сумма и произведение. Расширение $L/\mathbb{F}_q$ алгебраичено, так каждый элемент из L лежит в конечном алгебраическом расширении. Теперь проверим алгебраическую замкнутость L. Пусть $P = a_0 + a_1 x + \ldots + a_n x^n \in L[x]$, тогда каждые коэффициент лежит в каком-то конечном расширении $a_i \in \mathbb{F}_{p^{n_i}}$. Положим $m = \mathrm{lcm}(n_0, \ldots, n_n)$, тогда на самом деле $P \in \mathbb{F}_{p^m}$, если у P есть корень $\mathbb{F}_{p^m}$, то победа. Если нет, то P неприводим, а значит $\mathbb{F}_{p^m}[x]/(P) = \mathbb{F}_{p^{m(n-1)}}$, по единственности расширения. И найдется корень в $\mathbb{F}_{p^{m(n-1)}}$. А тогда поле L агебраически замкнуто и $L = \overline{\mathbb{F}_p}$ – алгебраическое замыкание.

2. **Опишите все автоморфизмы поля $\mathbb{C}$ над $\mathbb{R}$. Опишите все автоморфизмы поля $\mathbb{F}_{q^n}$ над $\mathbb{F}_q$, где $q = p^k$.**

   Заметим, что $\mathbb{C} = \mathbb{R}(i)$ расширяет $\mathbb{R}$ со степенью 2, а тогда у нас не может быть больше автоморфизмов над $\mathbb{R}$, чем 2 по следствию с лекции. Мы можем предъявить эти 2, а именно тождественный и сопряжение.

   Мы знаем, что $\mathbb{F}_{p^{nk}}$ обладает nk автоморфизмами над $\mathbb{F}_p$, тогда $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ образуют подгруппу в $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{q^n})$, так как если автоморфизм переводит тождественно $\mathbb{F}_q$ в себя, то он тем более переводит тождественно $\mathbb{F}_p$ в себя. Давайте возьмём какой-нибудь автоморфизм f над простым подполем. Пусть $f = x \mapsto x^{p^l}$, так как они все имеют такой вид. Если мы хотим $f(a) = a$ для любого $a \in \mathbb{F}_q$, то нам необходимо и достаточно, чтобы это было верно для элемента ζ, порождающего мультипликативную группу. $\zeta^{p^l-1} = 1$ означает, что $p^n - 1 \mid p^l - 1$, это возможно если $n \mid l$, так как тогда $l = mn$ и $q - 1 \mid q^m - 1$ верно. Покажем, что если $n \nmid l$, то $p^n - 1 \nmid p^l - 1$. Для этого заметим, что $p^n - 1 = p^{n-l}(p^l - 1) + p^{n-l}$ и продолжив так полинмиально делить с остатком, мы получим $p^n - 1 = g(p)(p^l - 1) + p^r - 1$, где r – остаток при делении n на l. Если мы хотим, чтобы $p^r - 1 = 0$, то необходимо, чтобы $r = 0$, а это ровно то, что нам нужно. Тогда все автоморфизмы $\mathbb{F}_{q^n}$ над $\mathbb{F}_q$ имеют вид $x \mapsto x^{q^m}$, и они порождены $x \mapsto x^{q^m}$. Так как $x \mapsto x^{q^n}$ тождественен, то их не более n штук. С другой стороны как мы видели на лекции все автоморфизмы $x \mapsto x^{p^{km}}$ различны для $0 < m \leq n$, а значит они и будут всеми автоморфизмами и они образуют циклическую группу.

3. **Опишите все автоморфизмы поля $\mathbb{R}$. Конечно ли множество автоморфизмов поля $\mathbb{C}$?**

   Пусть f – автоморфизм поля $\mathbb{R}$. Тогда f отправляет простое подполе в простое подполе, так как оно образовано единицей. То есть для любого рационального q верно $f(q) = q$. Пусть теперь a, b – действительные числа и пусть $a > b$. Заметим, что мы найдём число x, что $x^2 = (a - b)$, а тогда $f(a) - f(b) = f(a - b) = f(x^2) = f(x)^2 > 0$, а тогда f строго возрастает. Пусть $s \in \mathbb{R}$ обозначим за $S_- = \{q \in \mathbb{Q} \mid q < s\}$ и за $S_+ = \{q \in \mathbb{Q} \mid q > s\}$ из курса анализа известно, что такое сечение однозначно определяет число s. После автоморфизма сечения перейдут в сечения, а так как f строго возрастает, то $f(s)$ окажется зажат между S_- и S_+, а значит $f(s) = s$, тогда у $\mathbb{R}$ есть единственный автоморфизм – тождественный.

   Множество автоморфизмов $\mathbb{C}$ не конечно. Пусть $a \in \mathbb{C}$ трансцедентное число над $\mathbb{Q}$, такое есть из соображения о кардиналах. Тогда $\mathbb{Q}(a)$ – счетно, так как изморфно $\mathbb{Q}(x)$, тогда вновь по соображению о кардиналах есть бесконечность трансцендентных комплексных чисел над $\mathbb{Q}(a)$. Давайте покажем, что по каждому такому выбору числа b можно построить автоморфизм $\mathbb{C}$, что переставляет a и b, причем каждый такой выбор даст нам новый автоморфизм $\mathbb{C}$.

Покажем, что есть автоморфизм $\mathbb{Q}(a,b)$, что переставляет a и b. Для этого заметим, что если для $f(x,y) \in \mathbb{Q}(x,y)$ верно, что $f(a,b) = 0$, то в частности левую часть можно переписать как $g(b) = 0$ для некоторого $g(y) \in \mathbb{Q}(a)(y)$, а тогда $g(y) = 0$, но тогда $f(x,y) = 0$, так как каждый коэффициент $g(y)$ является вычислением некого $h(x) \in \mathbb{Q}$ в a, и так как вычисление нулевое и a трансцендентное, то $h(x) = 0$. Более того вычисление $f(a,b)$ можно всегда произвести, так как a и b по выбору алгебраически независимы и знаменатель не зануляется. Тогда зададим авитоморфизм $f(a,b) \mapsto f(b,a)$ для любого $f(x,y) \in \mathbb{Q}(x,y)$. Если $f \neq g$ для некоторых $f(x,y), g(x,y) \in \mathbb{Q}(x,y)$, то $f(a,b) \neq g(a,b)$ и $f(b,a) \neq g(b,a)$, так как $f - g \neq 0$ и по предыдущему наблюдению $(f-g)(a,b) \neq 0$ например. Тогда у нас есть автоморфизм и мы его назовём ϕ. Покажем, что его можно продлить до $\mathbb{C} \to \mathbb{C}$. Мы будем продлевать именно автоморфизмы, а не морфизмы, чтобы не получим случаем подполя $\mathbb{C}$ изоморфного $\mathbb{C}$.

Устроим частично упорядоченное множество автоморфизмов подполей комплексных чисел $K \to K$, таких что они продолжают ϕ с порядком $(f : K \to K) \leq (g : L \to L)$, если $K \leq L$ и $g|_K = f$. Покжем, что есть максимальный элемент. Пусть $\{f_i : K_i \to K_i\}$ возрастающая цепь, тогда её точная верхняя грань – автоморфизм $f : \bigcup_i K_i \to \bigcup_i K_i$, отправляющий $a \in K_i$ в $f_i(a)$, как нетрудно видеть, он корректен и является автоморфимом поля. Тогда применив лемму Цорна мы получим, что есть максимальный элемент $m : M \to M$.

Если $M = \mathbb{C}$, то победа, иначе мы можем взять $a \in \mathbb{C} \setminus M$, и продолжить $m : M \to M$ до $m' : M(a) \to M(a)$, просто отправив $a \mapsto a$ в случае, когда a трансцендентно, так как разные $f(x) \in M(x)$ имеют разные значения в точке a. Для алгебраического a мы можем продлить $m : M \to M$ до $m'' : \overline{M} \to \overline{M}$, так как расширение $\overline{M}/M$ алгебраично, а значит есть продолжение $\widetilde{m} : M \to \overline{M}$ до m''. В обоих случая мы прийдем к противоречию, а значит $M = \mathbb{C}$ и мы построили новый автоморфизм $\mathbb{C}$.

4. **Докажите, что расширение полей степени 2 нормально. Докажите, что расширение полей $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$ не нормально.**

   Пусть L/K расширение степени 2, тогда на самом деле $L = K[\alpha]$ для некого $\alpha \in L$. Пусть $p(x) = \mathrm{Irr}^K_\alpha(x)$, его степень 2. В L многочле $p(x)$ имеет один корень α, а тогда поделив $p(x)$ на $x - \alpha$ мы найдем и второй корень. А значит L – поле разложения $p(x)$ на K, а тогда расширение нормально.

   Расширение $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$ не нормально, так как например у неприводимого $x^4 - 2$ есть корень $\sqrt[4]{2}$, но в $x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$ правый множитель не раскладывается на линейные множители, так как у него нет корней, потому как квадрат действительного числа всегда положителен.

5. **Пусть $F \leq K \leq L$ – башня полей, и L/F нормально. Докажите, что L/K нормально. Приведите пример башни полей $F \leq K \leq L$, в которой K/F и L/K нормальны, но L/F не нормально.**

   Пусть $f(x) \in K[x]$ неприводим и у него есть корень $\alpha \in L$, тогда положим $p(x) = \mathrm{Irr}^K_\alpha(x) \in L[x]$. Устроим морфизм $\theta : K(x) \to L = f(x) \mapsto f(\alpha)$, его ядро максимальный идеал, в котором лежат $f(x)$ и $p(x)$. Так как $f(x)$ неприводим, то $\mathrm{Ker}(\theta) = (f(x))$, а значит $f(x) \mid p(x)$. С другой стороны, так как $p(x) \in F(x)$ и L/F нормально и у $p(x)$ есть корень α в L, то $p(x)$ раскладывается на линейные множители, а значит $f(x)$ тоже.

   Начнем с $\mathbb{Q}$, нормально расширим его до $\mathbb{Q}(i)$. Далеьше нормально расширим, добавив корень полинома $x^2 + (1+i)x + (1+i)$. Найдем его корень $D = (1+i)^2 - 4(1+i) = -2i - 4$, и $\alpha = (-(1+i) + i\sqrt{2}\sqrt{i+2})/2$. Покжем, что $\alpha \notin \mathbb{Q}(i)$. Пусть это не так, тогда есть $a, b \in \mathbb{Q}$, что $\sqrt{2}\sqrt{i+2} = a + ib$. Покажем, что такого быть не может, так как

$$
\begin{aligned}
a + ib &= \sqrt{2}\sqrt{i+2} \\
a^2 - b^2 + 2abi &= 4 + 2i \\
a^2 - b^2 = 4 \;&\&\; ab = 1 \\
a^2 - 1/a^2 &= 4 \\
a^4 + 4a^2 - 1 &= 0 \\
a^2 &= -2 \pm \sqrt{5}
\end{aligned}
$$

Тогда $\mathbb{Q}(i,\alpha)/\mathbb{Q}(i)$ вновь расширение степени 2, а значит нормально. Теперь покажем, что $\mathbb{Q}(i,\alpha)/\mathbb{Q}$ не нормально. Для начала построим неприводимый над $\mathbb{Q}$ многочлен. У нас уже был $x^2+(1+i)x+1+i$, возьмём сопряженный к нему и перемножим их

$$\begin{aligned}
&(x^2+(1+i)x+1+i)(x^2+(1-i)x+1-i)\\
&=x^4+(1-i)x^3+(1-i)x^2+(1+i)x^3+2x^2+2x+(1+i)x^2+2x+2\\
&=x^4+2x^3+4x^2+4x+2
\end{aligned}$$

Покажем, что у него не корней в $\mathbb{Q}$. Из школьного курса алгебры известно, что все возможные рациональные корни можно получить, посмотрев на делители старшего и младшего члена. Возможные рациональные корни $\pm1,\pm2$. Но очевидно, что ни один не зануляет многочлен

$$\begin{aligned}
1^4+2\cdot1^3+4\cdot1^2+4\cdot1+2&>0\\
2^4+2\cdot2^3+4\cdot2^2+4\cdot2+2&>0\\
(-1)^4+2(-1)^3+4(-1)^2+4(-1)+2&=1\\
(-2)^4+2(-2)^3+4(-2)^2+4(-2)+2&=10
\end{aligned}$$

Покажем, что $x^4+2x^3+4x^2+4x+2$ не раскладывается в произведение 2х полиномов степени 2. Пусть он разложился, тогда найдутся $a,b,p,q\in\mathbb{Q}$, что

$$\begin{aligned}
&x^4+2x^3+4x^2+4x+2\\
&=(x^2+ax+b)(x^2+px+q)\\
&=x^4+(a+p)x^3+(ap+q+b)x^2+(aq+bp)x+bq
\end{aligned}$$

Тогда мы получим следующую систему уравнений

$$\begin{cases}a+p=2\\ap+q+b=4\\aq+bp=4\\bq=2\end{cases}$$

Заменим везде p на $2-a$

$$\begin{cases}a(2-a)+q+b=4\\aq+b(2-a)=4\\bq=2\end{cases}$$

А теперь заменим везде q на $2/b$, так как b не ноль

$$\begin{cases}a(2-a)+2/b+b=4\\2a/b+b(2-a)=4\end{cases}$$

Домножим оба равенства на $b\neq0$.

$$\begin{cases}ba(2-a)+2+b^2=4b\\2a+b^2(2-a)=4b\end{cases}$$

Заметим, что второе раветнство можно переписать

$$\begin{aligned}
&2a+b^2(2-a)=4b\\
&(b^2-2)(2-a)+4=4b\\
&2-a=(4b-4)/(b^2-2)\quad\text{можем поделить, так как }\sqrt{2}\notin\mathbb{Q}\\
&a=2-\frac{4b-4}{b^2-2}=\frac{2b^2-4b}{b^2-2}
\end{aligned}$$

Подствив выражения для a и $2-a$ от b в первое уравнение системы, мы получим уравнение на b

$$\begin{aligned}
b\frac{2b^2-4b}{b^2-2}\frac{4b-4}{b^2-2}+2+b^2&=4b\\
b(2b^2-4b)(4b-4)+(b^2-4b+2)(b^2-2)^2&=0
\end{aligned}$$

У нас вновь получилось полиномиальное уравнение со старшим коэффициентом 1 и младшим 8, тогда возможные рациональные корни только $\pm 1, \pm 2, \pm 4, \pm 8$. Проверим, что ни один не подходит

$$
\begin{aligned}
b(2b^2 - 4b)(4b - 4) + (b^2 - 4b + 2)(b^2 - 2)^2 \\
1(2 \cdot 1^2 - 4 \cdot 1)(4 \cdot 1 - 4) + (1^2 - 4 \cdot 1 + 2)(1^2 - 2)^2 &= -1 \\
(-1)(2 \cdot (-1)^2 - 4 \cdot (-1))(4 \cdot (-1) - 4) + ((-1)^2 - 4 \cdot (-1) + 2)((-1)^2 - 2)^2 &= 55 \\
2(2 \cdot 2^2 - 4 \cdot 2)(4 \cdot 2 - 4) + (2^2 - 4 \cdot 2 + 2)(2^2 - 2)^2 &= -8 \\
(-2)(2 \cdot (-2)^2 - 4 \cdot (-2))(4 \cdot (-2) - 4) + ((-2)^2 - 4 \cdot (-2) + 2)((-2)^2 - 2)^2 &= 440 \\
4(2 \cdot 4^2 - 4 \cdot 4)(4 \cdot 4 - 4) + (4^2 - 4 \cdot 4 + 2)(4^2 - 2)^2 &= 1160 \\
(-4)(2 \cdot (-4)^2 - 4 \cdot (-4))(4 \cdot (-4) - 4) + ((-4)^2 - 4 \cdot (-4) + 2)((-4)^2 - 2)^2 &= 10504 \\
8(2 \cdot 8^2 - 4 \cdot 8)(4 \cdot 8 - 4) + (8^2 - 4 \cdot 8 + 2)(8^2 - 2)^2 &= 152200 \\
(-8)(2 \cdot (-8)^2 - 4 \cdot (-8))(4 \cdot (-8) - 4) + ((-8)^2 - 4 \cdot (-8) + 2)((-8)^2 - 2)^2 &= 4222792
\end{aligned}
$$

Тогда наш изначальный многочлен $x^4 + 2x^3 + 4x^2 + 4x + 2$ не раскладывается в произведение квадратов и не имеет рациональных корней, а значит он неприводим над $\mathbb{Q}$. С другой стороны, в $\mathbb{Q}(i, \alpha)$ он раскладывается в $(x^2 + (1+i)x + 1 + i)(x^2 + (1-i)x + 1 - i)$ и левый множитель раскладывается на линейные. Давайте убедися, что у правого множителя нет корней в $\mathbb{Q}(i, \alpha)$. В $\mathbb{C}$ у правого множителя корни следующие

$$
\begin{aligned}
D &= (1 - i)^2 - 4(1 - i) = 2i - 4 \\
x_{1,2} &= (-(1 - i) \pm \sqrt{2i - 4})/2
\end{aligned}
$$

И то что они лежат в $\mathbb{Q}(i, \alpha)$ эквивалентно тому, что $\sqrt{2i - 4}$ $\mathbb{Q}(i)$-линейно выражается через $1, \sqrt{2i + 4}$, так как расширение $\mathbb{Q}(i, \alpha)/\mathbb{Q}(i)$ – степени 2. Пусть $a, b, c, d \in \mathbb{Q}$ такие, что

$$
\begin{aligned}
&\sqrt{2i - 4} + (ai + b)\sqrt{2i + 4} = ci + d \\
&(\sqrt{2i - 4} + (ai + b)\sqrt{2i + 4})^2 = (ci + d)^2 \\
&2i - 4 + (b^2 - a^2 + 2iab)(2i + 4) + 2(ai + b)\sqrt{(2i - 4)(2i + 4)} = (ci + d)^2 \\
&2i - 4 + (b^2 - a^2 + 2iab)(2i + 4) + 2(ai + b)\sqrt{-20} = (ci + d)^2
\end{aligned}
$$

Но так как $\sqrt{-20} \notin \mathbb{Q}(i)$, $ai + b = 0$, а тогда

$$
\begin{aligned}
&2i - 4 = d^2 - c^2 + 2icd \\
&cd = 1 \quad \& \quad c^2 - d^2 = 4
\end{aligned}
$$

Но как мы уже видели у такой системы нет рациональных решений, а значит мы получили неприводимый многочлен, что не раскладывается на линейные множители в $\mathbb{Q}(i, \alpha)$, а значит расширение $\mathbb{Q}(i, \alpha)/\mathbb{Q}$ не нормально и контр-пример построен.