Двадцать седьмая Летняя многопредметная школа Кировской области
Вишкиль, 3–28 июля 2011 года.
10 класс (профи) • 11 июля

Поля и расширения полей.

Определение. Если поле K содержится в поле L, то будем говорить, что L — *расширение* K.

Упр. 0. Существует ли расширение поля $\mathbb{C}$?

Упр. 1. Докажите, что каждое поле содержит $\mathbb{Q}$ или $\mathbb{Z}_p$ (точнее говоря, поле, изоморфное $\mathbb{Q}$ или $\mathbb{Z}_p$) в качестве подполя, причем ровно одно из этих полей.

Определение. Любое расширение L поля K является векторным пространством над K относительно обычных операций сложения и умножения в поле L. Размерность этого векторного пространства L над полем K называется *степенью* расширения $L \supset K$ и обозначается через $[L : K] = \dim_K L$. Если степень конечна, расширение называется *конечным*.

Упр. 2. Существует ли поле из шести элементов? Для каких m *может существовать* конечное поле из m элементов?

Определение. Пусть имеется расширение $K \subset L$, S — некоторое подмножество в L. Обозначим через $K(S)$ наименьшее (по включению) подполе поля L, содержащее все элементы из K и из S. Мы будем говорить, что $K(S)$ получено *присоединением* элементов S к K.

Упр. 3. Докажите, что $K(S)$ существует.

Упр. 4. Докажите, что $K(S)(M) = K(M)(S)$ – расширение не зависит от порядка присоединения элементов – важнейшее свойство!!!

Определение. Два поля K и L называются *изоморфными*, если существует такая биекция φ между их элементами, при которой сумма переходит в сумму, произведение — в произведение.

Упр. 5. Докажите, что при изоморфизме нулевой элемент переходит в нулевой, единичный — в единичный, разность — в разность, а частное — в частное.

Нас будет интересовать простейший (и одновременно с этим важнейший) случай: как устроено расширение, полученное присоединением одного элемента?

Определение. Пусть $K \subset L$ — расширение полей. Элемент $\alpha \in L$ называется *алгебраичным* над K, если он является корнем некоторого ненулевого многочлена с коэффициентами из K (этот многочлен можно считать неприводимым над K). В противном случае говорят, что α *трансцендентен* над K.

Упр. 6. а) Какие комплексные числа алгебраичны над $\mathbb{R}$, а какие – трансцендентны?

б) Докажите, что существуют вещественные числа, трансцендентные над $\mathbb{Q}$.

Теорема 1. Если элемент α трансцендентен над K, то $K(\alpha)$ изоморфно $K(t)$ – полю рациональных функций над K от одной переменной.

Упр. 7. Пусть $K \subset L$, $\alpha \in L$ – алгебраический над K элемент. Рассмотрим ненулевой неприводимый многочлен $f(x) \in K[x]$, корнем которого является α. Тогда если $g(x) \in K[x]$, то $g(\alpha) = 0 \iff g(x) \vdots f(x)$. То есть этот многочлен определен однозначно с точностью до мультипликативного множителя.

Упр. 8. Избавьтесь от иррациональности в знаменателе: $\frac{1}{\alpha^2+3\alpha+5}$, где α — корень уравнения $\alpha^3 - \alpha + 1 = 0$.

Теорема 2. Если α — корень неприводимого над K многочлена степени n, то расширение $K \subset K(\alpha)$ имеет степень n, причем элементы $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ образуют базис поля $K(\alpha)$ над K.

Упр. 9. Пусть α_1, α_2 — два корня неприводимого многочлена f. Тогда поля $K(\alpha_1)$ и $K(\alpha_2)$ изоморфны. Приведите пример, показывающий, что они могут не совпадать.

Для самостоятельного решения

1. Изоморфны ли $\mathbb{Q}(\sqrt{2})$ и $\mathbb{Q}(\sqrt{3})$?

2. Опишите все конечные расширения а) $\mathbb{C}$; б) $\mathbb{R}$.

3. а) Докажите, что в поле характеристики p выполняется равенство: $(x+y)^p = x^p + y^p$.

б) Разложите на множители над $\mathbb{Z}_p$ многочлен $x^p - x$.

в) Докажите часть *теоремы Вильсона*: $(p-1)! \equiv -1 \pmod{p}$ при простом p.

Теорема о размерности башни

Теорема об алгебраичности конечного расширения. Если $K \subset L$ — конечное расширение степени n, то каждый элемент из L алгебраичен над K степени не выше n.

Теорема о размерности башни (часть I). Пусть $k \subset E \subset L$ — поля, причем расширения $k \subset E$ и $E \subset L$ – конечны. Тогда расширение $k \subset L$ конечно и $[L : k] = [L : E] \cdot [E : k]$.

Следствие. Сумма, разность, произведение и частное алгебраических чисел (в данном поле над данным подполем) является алгебраическим числом. Иначе говоря, множество алгебраических чисел (в данном поле над данным подполем) является полем.

Упр. 1. Найдите размерность и базис расширения $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$.

Упр. 2. Пусть α, β – два различных корня многочлена многочлена $x^3 - 3$. Найдите размерность и базис расширения $\mathbb{Q} \subset \mathbb{Q}(\alpha, \beta)$.

Упр. 3. Докажите, что многочлен $x^5 - 7$ неприводим над полем $\mathbb{Q}(\sqrt[3]{3})$.

Упр. 4. Докажите, что число $a\sqrt[3]{3} + b\sqrt[5]{7/2} + c\sqrt[8]{8}$, $a, b, c \in \mathbb{Q}$ рационально тогда и только тогда, когда оно равно нулю.

Упр. 5. а) Поле $F \subset \mathbb{C}$ получено из $\mathbb{Q}$ присоединением квадратных корней из а) ста; б) всех рациональных чисел. Докажите, что в F нет ни одного кубического корня из а) целого; б) рационального числа, который не являлся бы кубом рационального числа.

б) Изначально дано поле $\mathbb{Q}$. Очередное поле получается из предыдущего присоединением некоторого корня из какого-то элемента этого предыдущего этажа степени 2,3 или 4. Докажите, что ни в каком этаже нет элемента $\sqrt[5]{5}$. ($\sqrt[5]{5}$ *не выражаются через радикалы степеней 2,3 и 4.*)

Упр. 6. Пусть $r = \sqrt[15]{15}$. Рассмотрим число $a_0 + a_1 r + a_2 r^2 + \cdots + a_{14} r^{14}$, $a_i \in \mathbb{Q}$. Пусть число является корнем неприводимого многочлена. Чему может равняться его степень?

Упр. 7. а) Рассмотрим любое комплексное число, которое получается из рациональных чисел при помощи арифметических действий и операций извлечения корней. Докажите, что это число алгебраично.

б) Оцените степень алгебраичности числа $\sqrt[3]{2 - 5\sqrt{3}} - \sqrt{3 + 5\sqrt[3]{7}}$.

НЕТРИВИАЛЬНЫЙ ВОПРОС. Любое ли алгебраическое число получается таким образом?

Для самостоятельного решения

1. Докажите, что $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{6}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Теорема (о размерности башни, часть II). Пусть $k \subset E \subset L$ — поля, причем расширение $k \subset L$ конечно. Тогда расширения $k \subset E$ и $E \subset L$ конечны, причем $[L : k] = [L : E] \cdot [E : k]$.

Теорема об алгебраической замкнутости поля алгебраических чисел. Если некоторое комплесное число является корнем многочлена с алгебраическими (над $\mathbb{Q}$) коэффициентами, то это число алгебраично (над $\mathbb{Q}$).