1 Определения

Определение 1.1. Пусть F – факториальное кольцо, $f(x) \in F[x]$. Тогда содержание $c(f)$ многочлена $f(x)$ – это наибольший общий делитель его коэффициентов.

Определение 1.2. Пусть F – факториальное кольцо, $f(x) \in F[x]$. Тогда $f(x)$ – примитивный, если его содержание тривиально: $c(f) \sim 1$

Определение 1.3. Характеристика поля F – $charF$ – это минимальное количество единиц, сумма которых равна нулю. Если никакя сумма единиц не дает нуля, то говорят, что $charF = 0$, иначе F – поле конечное характеристики.

Определение 1.4. Пусть F – поле. Тогда K называется расширением F, если K – поле, и $F \subset K$

Определение 1.5. Пусть K – расширение F. Элемент $\alpha \in K$ называется алгебраическим над F, если $\exists f(x) \in F[x] : f(\alpha) = 0$

Определение 1.6. Пусть K – расширение F. Элемент $\alpha \in K$ называется трансцендентным над F, если $\forall f(x) \in F[x] : f(\alpha) \neq 0$

Определение 1.7. Расширение K называется алгебраическим, если все его элементы алгебраические.

Пример. $\mathbb{C}$ – алгебраическое расширение $\mathbb{R}$, так как любой его элемент $z = a + ib$ является корнем многочлена $\left(\frac{x-a}{b}\right)^2 + 1 = 0$.

Пример. $\mathbb{R}$ – не алгебраическое расширение $\mathbb{Q}$, так как π не является корнем ни какого многочлена над $\mathbb{Q}$.

Определение 1.8. Пусть K – расширение над F. $\alpha \in K$ – алгебраический элемент. Тогда $m_\alpha(x)$ – это минимальный (по степени) многочлен со старшим коэфициентом, равным единице, который обнуляет α.

Определение 1.9. Пусть $K \supset F$ – расширение, $\gamma \in K$. $F(\gamma)$ – минимальное по включению поле, содержащее F и γ.

Определение 1.10. Пусть F – поле, $f(x) \in F[x]$. Тогда поле разложения многочлена $f(x)$ – это такое минимальное по включению расширение $K \supset F$, что f раскладывается на множители над K.

Определение 1.11. Поле K, удовлетворяющее любому из следующих эквивалентных условий, называется алгебраически замкнутым:

1. Любой многочлен $f(x) \in K[x]$ ненулевой степени имеет корень в K.
2. Полем разложения любого многочлена $f(x) \in K[x]$ является K
3. Любой неприводимый многочлен $f(x) \in K[x]$ имеет степень 1.

4. Любое алгебраическое расширение $L \supset K$ тривиально, то есть $L = K$.

Определение 1.12. Пусть F – поле, тогда его алгебраическим замыканием $\overline{F}$ называется такое его алгебраическое расширение, которое является алгебраически замкнутым.

Определение 1.13. Расширение $K \supset F$ называется сепарабельным, если все его элементы $\alpha \in K$ сепарабельны над F.

Определение 1.14. Элемент α расширения $K \supset F$ называется сепарабельным, если его минимальный многочлен m_α не содержит кратных корней.

Определение 1.15. Назовём расширение $K \supset F$ радикальным, если существует башня расширений $K \supset K_n \supset K_{n-1} \supset \cdots \supset K_1 \supset F$, где $K_1 = F(\alpha_0), K_2 = K_1(\alpha_1), \cdots, K_n = K_{n-1}(\alpha_{n-1}), K = K_n(\alpha_n)$, α_i – корень многочлена $x^{n_i} - a_i = 0$, $a_i \in K_i$.

Многочлен $f(x) \in F[x]$ называется разрешимым в радикалах, если его поле разложения является радикальным расширением F.

Определение 1.16. ξ_n – примитивный корень n-ной степени из единицы – это такой элемент F, что $\xi_n^n = 1$, а степени ξ_n – это всевозможные корни n-ной степени из единицы.

Определение 1.17. Два элемента называются сопряженными, если их минимальные многочлены совпадают.

Утверждение 1.1 (критерий неприводимости Эзенштейна)**.** *Для многочлена $f(x) = a_n x^n + \cdots + a_0 \in F[x]$ он является неприводимым, если существует такое простое p, что $p \not| a_n$, $p | a_i$, $i \in \{n-1, \cdots, 0\}$, $p^2 \not| a_0$*

Определение 1.18. Конечное расширение $K \supset F$ называется нормальным, если оно удовлетворяет одному из следующих равносильных условий:

1. $\forall \alpha \in K : \forall \beta$ – сопряженный к α, $\beta \in K$
2. K – поле разложения некоторого семейства многочленов.
3. $\forall \varphi : K \mapsto \overline{F}$ – изоморфизм, сохраняющий F, также является автоморфизмом K.

Определение 1.19. Пусть $G = Aut_F K$ – группа автоморфизмов конечного расширения $K \supset F$, сохраняющих F. $\forall H < G$ рассмотрим $K^H = \{x \in K : \forall h \in H : hx = x\}$. Тогда конечное сепарабельное расширение $K \supset F$ называется расширением Галуа, если для него выполнено одно из следующих эквивалентных условий:

1. K – нормальное расширение
2. $[K : F] = |G|$
3. $K^G = F$

Определение 1.20. Группа Галуа расширения $K \supset F$ – это группа автоморфизмов этого расширения K, сохраняющих F.

2 Вопросы

Утверждение 2.1. *Пусть $f(x) = a_n x^n + \cdots + a_0$ – многочлен над $\mathbb{Z}[x]$. Пусть также $\exists p$ – простое, что p делит все a_i, кроме первого, а a_0 не делится на p^2. Тогда $f(x)$ – неприводимый.*

Доказательство. Пусть не так, тогда $\exists g(x) = b_m x^m + \cdots + b_0, h(x) = c^l x^l + \cdots + c_0 \in \mathbb{Z}[x]$, причем $f = gh$, $m < n, l < n$. Тогда $a_i = \sum_{(j,k):j+k=i} b_j c_k$. Известно, что $p|a_0 = b_0 \cdot c_0$. Тогда либо $p|b_0$, либо $p|c_0$. Причем, поскольку $\neg p^2|a_0$, то c_0 либо b_0 соответсвенно не делится на p. Пусть без ограничения общности $p|b_0, \neg p|c_0$. Тогда из того, что $p|a_1 = b_1 a_0 + b_0 a_1$. Тогда b_1 делится на p. Аналогично для всех остальных b_i. Тогда $p|b_m$, следовательно $a_n = b_m c_k$ также делится на p. Противоречие. □

Утверждение 2.2. *Многочлен $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, где p – простое число, неприводим.*

Доказательство. $\Phi_p(x) = \frac{x^p-1}{x-1}$. Сделаем замену $t = x - 1$. Тогда $\Phi_p = \frac{(t+1)^p-1}{t} = \sum_{i=1}^{p} \binom{p}{i} t^{i-1} = t^{p-1} + \sum_{i=2}^{p-1} \binom{p}{i} t^{i-1} + p$ – неприводим по критерию Эйзенштейна. □

Утверждение 2.3. *Пусть F – факториальное кольцо. Тогда неразложимые многочлены $F[x]$ степени 0 – это в точности простые элементы F.*

Доказательство. Пусть p – неразложимый в $F[x]$. Тогда $\forall a, b, p = ab$: без ограничения общности $a \in F[x]^*$. Но a, b – тоже многочлены степени 0, то есть константы. Но тогда $a \in F^*$. Значит, p – неразложимый, а следовательно, простой в F.

Пусть наоборот, p – простой элемент F. Пусть он разложим над $F[x]$, то есть $\exists f, g \notin F[x]^* : fg = p$. Тогда степень f и g – ноль. Тогда $p = fg$ над F. То есть p – не простой. □

Утверждение 2.4. *Для произвольных многочленов $f, g \in F[x]$ над факториальным кольцом F выполнено равенство $c(fg) = c(f)c(g)$.*

Доказательство. Пусть $fg = c(f)\hat{f}c(g)\hat{g}$, где $\hat{f}, \hat{g}$ – примитивные. Докажем, что $\hat{f}\hat{g}$ – тоже примитивный. Пусть $\hat{f}\hat{g} = a^n x^n + \cdots + a_0, \hat{f} = b_m x^m + \cdots + b_0, \hat{g} = c_l x^l + \cdots + c_0$. Тогда $a_k = \sum_{i=0}^{k} b_i c_{l-i}$. Предположим, что $\hat{f}\hat{g}$ – не примитивный. Тогда $\exists p : p|c(\hat{f}\hat{g})$, p – простое. □