Упражнение 1.1. Структура кольца многочленов над полем.

Пусть K поле, $K[x]$ кольцо многочленов с коэффициентами в K.

(а) Доказать, что все идеалы в $K[x]$ главные и показать, что любой простой идеал в $K[x]$ является максимальным (Указание: алгоритм Евклида).

(б) Пусть R ассоциативное коммутативное кольцо с единицей (в дальнейшем будут рассматриваться лишь такие кольца). Доказать, что идеал $\mathfrak{m} \subset R$ максимален тогда и только тогда, когда факторкольцо $R/\mathfrak{m}$ является полем.

(в) Доказать факториальность $K[x]$, то есть то, что любой многочлен однозначно с точностью до умножения на элементы из K раскладывается в произведение неприводимых многочленов (для этого вспомнить аналогичное доказательство для кольца целых чисел).

Упражнение 1.2. Присоединение корней многочленов.

Рассмотрим алгебраическое замыкание $\overline{K}$ поля K. Пусть $\alpha \in \overline{K}$. Тогда $K(\alpha)$ обозначает минимальное подполе в $\overline{K}$, содержащее K и α, то есть

$$K(\alpha) = \{\frac{P(\alpha)}{Q(\alpha)} | P, Q \in K[x]\}$$

(а) Показать, что $I = \{P \in K[x] | P(\alpha) = 0\}$ является простым иделом в $K[x]$.

(б) Доказать, что $K[x]/I \cong K(\alpha)$ (Указание: рассмотреть гомоморфизм $K[x] \to \overline{K}, x \mapsto \alpha$).

Такие расширения полей называются *простыми.*

(в) Из вышесказанного следует, что поля $K(\alpha)$ и $K(\beta)$ изоморфны для разных корней α и β одного и того же неприводимого многочлена P. Однако при этом они могут быть разными подполями в $\overline{K}$. Привести соответствующий пример. (Указание: рассмотреть $K = \mathbb{Q}$, $P(x) = x^3 - 2$)

В дальнейшем будет часто использовано следующее важное и простое утверждение:

(г) Пусть задан гомоморфизм полей $\varphi : K \to F$. Тогда он может быть продолжен до гомоморфизма $\overline{\varphi} : K(\alpha) \to F$ ровно столькими способами, сколько корней у P в поле F. (Указание: рассмотреть, куда может перейти α при гомоморфизме $\overline{\varphi}$.)

Упражнение 1.3. Поле разложения.

Пусть α корень некоторого неприводимого многочлена $P \in K[x]$. Тогда над полем $K(\alpha)$ возможно разложение $P(x) = (x - \alpha)Q(x)$.

(а) Привести пример того, что многочлен P не разлагается целиком на линейные сомножители над полем $K(\alpha)$.

(б) Доказать, что существует такое поле L, содержащее K, что многочлен P разлагается над ним на линейные сомножители, и никакое строго содержащееся в нем поле не обладает таким свойством. Показать единственность такого поля, как K-алгебры.

(в) Доказать, что в $\overline{K}$ есть лишь одно подполе, изоморфное полю разложения L.

L называется *полем разложения* многочлена P.

Упражнение 1.4. Степень расширения полей.

Пусть $K \subset L$ расширение полей. Тогда L можно рассматривать, как векторное пространство над K. По определению, *степень расширения* равна $[L : K] = \dim_K L$.

(а) Показать, что для башни полей $K \subset L \subset E$ выполнено $[E : K] = [E : L][L : K]$.

Если $[L : K] < \infty$, то такое расширение полей называется *конечным*.

(б) Доказать, что конечное расширение является алгебраическим.

(в) Пусть $L = K(\alpha)$, где α корень неприводимого многочлена P. Тогда $[L : K] = \deg(P)$.

(г) Используя (б) и (в), доказать, что сумма и произведение алгебраических чисел алгебраические числа.

(д) Показать, что любое конечное расширение может быть представлено, как композиция простых.

(е) Используя понятие степени расширения, доказать, что любое конечное поле состоит из p^r элементов, где p простое число, равное характеристике нашего поля, а r некоторое натуральное число.

Упражнение 1.5. Квадратичные расширения.

Пусть $K \subset L$, $[L : K] = 2$, $\mathrm{char} K \neq 2$.

(а) Показать, что L можно представить в виде $K(\alpha)$, где α корень некоторого квадратичного многочлена вида $P(x) = x^2 - D$.

(б) Показать, что L является полем разложения P.

Упражнение 1.6. Кубические многочлены.

Пусть $\mathrm{char} K \neq 2, 3$.

(а) Любой кубический многочлен $P(x)$ над K может быть приведен к виду $P(x) = x^3 + px + q$ с помощью линейной замены переменной x.

(б) Пусть α_1, α_2 и α_3 корни P, $D = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2$ — *дискриминант* многочлена P. Доказать, что $D \in K$. (Аналогичная формула для дискриминанта верна и в квадратичном случае!)

(в) Обозначим через L поле разложения многочлена P. Доказать, что если D не является квадратом в K, то $L = K(\sqrt{D}, \alpha)$, где α произвольный корень P. (Указание: $[L : K] \leq 6$)

(г) Предположим теперь, что $D \in K^2$. Проверить, что $\alpha_2 + \alpha_3, \alpha_2 - \alpha_3 \in K(\alpha_1)$ и вывести отсюда, что $L = K(\alpha_1)$.

(д) Напомним, что если $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ — некоторый многочлен, то его результант со своей производной равен $\prod_{i<j}(\alpha_i - \alpha_j)^2$, где $P(x) = \prod_{i=1}^n (x - \alpha_i)$. Выразить с помощью этого дискриминант в нашем случае через коэффициенты p и q. (Ответ: $D = -4p^3 - 27q^2$)

(е) Найти поле разложения F многочлена $x^3 - 7$ над $\mathbb{Q}$ используя то, что $\sqrt[3]{1} \in F$. Найти F другим способом, опираясь на (в), (г) и (д).

Упражнение 1.7. Структура конечных полей.

Пусть K — конечное поле, $\mathrm{char} K = p$. Мы уже видели, что число элементов в K должно иметь вид p^n.

(а) Доказать, что для любого натурального n существует и единственно поле из p^n элементов, и что в $\overline{\mathbb{F}_p}$ есть лишь одно подполе, изоморфное ему. Поле из p^n элементов обозначается $\mathbb{F}_{p^n}$. (Указание: любой $x \in \mathbb{F}_{p^n}$ является корнем многочлена $x^{p^n} - x = 0$)

(б) Пусть K поле, $G \subset K^*$ конечная подгруппа мультипликативной группы поля. Доказать, что G циклическая. (Указание: использовать структурную теорему о конечно порожденных абелевых группах, а также то, что у многочлена $x^m - 1$ не более, чем m корней.)

(в) Доказать, что над конечным полем существует неприводимый многочлен любой степени, используя (а) и (б).

Следующее очевидное замечание носит фундаментальный характер:

(г) Пусть K поле, $\mathrm{char} K = p > 0$. Тогда для любых $a, b \in K$ и натурального n $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

Упражнение 1.8. Сепарабельные расширения.

Многочлен $P \in K[x]$ *сепарабельный*, если он не имеет кратных корней в $\overline{K}$.

(а) Многочлен сепарабельный тогда и только тогда, когда он взаимно прост со своей производной. (Напоминание: не забыть разобрать тот случай, когда у многочлена положительной степени нулевая производная.)

(б) Если многочлен P неприводим и несепарабелен, то $\mathrm{char} K = p > 0$, и $P(x) = Q(x^p)$ для некоторого многочлена Q.

Пусть $K \subset L$ расширение полей. Элемент $\alpha \in L$ называется *сепарабельным* над K, если сепарабелен его минимальный многочлен. Само расширение $K \subset L$ *сепарабельно*, если любой элемент $\alpha \in L$ сепарабелен. Поле K *совершенно*, если любое его алгебраическое расширение сепарабельно.

(в) Показать, что сумма и произведение сепарабельных элементов сепарабельны. (Указание: явно построить минимальный многочлен для суммы и для произведения.)

(г) Доказать, что поле K характеристики p совершенно тогда и только тогда, когда для любого натурального n из любого его элемента $\alpha \in K$ извлекается корень степени p^n (в самом K).

(д) Доказать, что все конечные поля, поля нулевой характеристики и алгебраически замкнутые поля совершенны.

(е) Показать, что для башни полей $K \subset L \subset F$ из того, что расширение $K \subset F$ сепарабельно, следует, что расширение $L \subset F$ тоже сепарабельно.

(ж) Пусть L/K конечное сепарабельное расширение полей. Тогда число вложений $L \to \overline{K}$ над K равно $[L : K]$. (Указание: достаточно доказать для простого расширения, а для него можно использовать упражнение 1.2(г).)

(з) Вывести из (ж) то, что композиция сепарабельных расширений сепарабельное расширение.

Упражнение 1.9. Вычисление группы Галуа в простейших случаях.

(а) Показать, что если $\mathrm{char} K \neq 2$, то любое его квадратичное расширение является расширением Галуа с группой $\mathbb{Z}/2\mathbb{Z}$.

(б) Пусть L поле разложения неприводимого кубического многочлена над полем K, $\mathrm{char}K \neq 2, 3$. Покажите, что если дискримининт D не является квадратом в K, то $\mathrm{Gal}(L/K) \cong S_3$. Какое промежуточное поле соответствует подгруппе $A_3 \subset S_3$? Чему изоморфна группа Галуа $\mathrm{Gal}(L/K)$ в том случае, когда D является квадратом в поле K?

(в) Доказать, что $\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q) \cong \mathbb{Z}/k\mathbb{Z}$, где $q = p^r$, p простое число. Описать явно биекцию, устанавливаемую в основной теореме теории Галуа в данном случае. (Указание: рассмотрите автоморфизм Фробениуса:$x \mapsto x^q$)

(г) Пусть k некоторое поле, $K = k(a_1, \ldots, a_n)$, L поле разложение многочлена $x^n + a_1 x^{n-1} + \ldots + a_n \in K[x]$. Доказать, что $\mathrm{Gal}(L/K) \cong S_n$. (Указание: рассмотреть расширение $k(\sigma_1, \ldots, \sigma_n) \subset k(x_1, \ldots, x_n)$, где $\sigma_1, \ldots, \sigma_n$ — симметрические многочлены от $x_1, \ldots, x_n$).

Группой Галуа неприводимого многочлена над полем K называется группа Галуа $\mathrm{Gal}(L/K)$ его поля разложения L.

(д) Найти группу Галуа многочлена $x^4 - 3$ над полем $\mathbb{Q}$. (Указание: данное поле разложения содержит два подполя $\mathbb{Q}(i)$ и $\mathbb{Q}(\sqrt[4]{3})$, пересекающихся по $\mathbb{Q}$.)

Упражнение 1.10. Бесконечные расширения Галуа.

Заметим, что в формулировке условий (ii) и (iii) в теореме 1.3 не присутствует конечность расширения L/K.

(а) Доказать, что (ii) равносильно (iii) в случае бесконечного расширения.

Такие бесконечные расширения тоже называются *расширениями Галуа.*

(б) Доказать основную теорему теории Галуа для подгрупп конечного индекса в группе $\mathrm{Gal}(L/K)$ в случае бесконечного расширения.