Упражнение 2.1. Круговые расширения $\mathbb{Q}$.

Пусть $\zeta_m = \sqrt[m]{1}$ — первообразный корень степени m из 1 над $\mathbb{Q}$. Поле $\mathbb{Q}(\zeta_m)$ имеет важный арифметический смысл.

(а) В случае, когда $m = p^r$, а p простое, доказать, что $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m) = (p-1)p^{r-1}$, а $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ (Указание: заметим, что ζ_m является корнем многочлена $f(x) = \frac{x^m-1}{x^{m/p}-1}$. Из леммы Гаусса следует, что f неприводим над $\mathbb{Q}$ тогда и только тогда, когда он неприводим над $\mathbb{Z}$. Пусть $f(x) = g(x)h(x)$, $g, h \in \mathbb{Z}[x]$. Рассматривая редукцию по модулю p, доказать, что $g(1)$ и $h(1)$ должны делится на p, и получить противоречие с тем, что $f(1) = p$.)

(б) Доказать, что для взаимно простых чисел m и n композит полей $\mathbb{Q}(\zeta_m)$ и $\mathbb{Q}(\zeta_n)$ в поле $\overline{\mathbb{Q}}$ равен $\mathbb{Q}(\zeta_{mn})$.

(в) В дальнейшем мы докажем, что $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ для взаимно простых m и n. Вывести из этого и из упражнения 2.2, что для любого натурального m $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$, а $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$, где φ — функция Эйлера.

(г) Каждое простое число, взаимно простое с m, определяет элемент группы Галуа $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$, равный $p(\mathrm{mod} m)$. Найти явный вид действия этого автоморфизма поля $\mathbb{Q}(\zeta_m)$ на ζ_m. Что он напоминает? Мы еще встретимся с подобной ситуацией, она занимает центральное место в алгебраической теории чисел. (Ответ: $\zeta_m \mapsto \zeta_m^p$.)

Упражнение 2.2. Композит расширений.

Пусть L_1/K и L_1/K два расширения поля K, $L_1, L_2 \subset F$. Рассмотрим их композит $L_1 \cdot L_2$ В поле F.

(а) Доказать, что $\mathrm{Gal}(L_1 \cdot L_2/L_2) \cong \mathrm{Gal}(L_1/(L_1 \cap L_2))$. (Указание: пусть H — образ $\mathrm{Gal}(L_1 \cdot L_2/L_2)$ в $\mathrm{Gal}(L_1/(L_1 \cap L_2))$ при гомоморфизме ограничения. Показать, что $L_1^H = L_1 \cap L_2$.)

(б) Вывести из (а), что $\mathrm{Gal}(L_1 \cdot L_2/L_1 \cap L_2) \cong \mathrm{Gal}(L_1/L_1 \cap L_2) \times \mathrm{Gal}(L_2/L_1 \cap L_2)$.

Упражнение 2.3. Норма и след.

Пусть L/K расширение Галуа, $\alpha \in L$. Тогда *нормой* α называется

$$N_{L/K}(\alpha) = \prod_{g \in \mathrm{Gal}(L/K)} g(\alpha),$$

а *следом*

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{g \in \mathrm{Gal}(L/K)} g(\alpha).$$

(а) Доказать, что $N_{L/K}$ является гомоморфизмом мультипликативных групп $L^* \to K^*$, а $\mathrm{Tr}_{L/K}$ является гомоморфизмом аддитивных групп $L^+ \to K^+$. Вывести из этого, что если натуральные числа m и n являются суммой двух квадратов, то и mn тоже является суммой двух квадратов. (Указание: рассмотреть расширение $\mathbb{Q} \subset \mathbb{Q}(i)$.)

(б) Пусть минимальный многочлен для α над K равен $x^n + a_{n-1}x^{n-1} + \ldots + a_0$. Показать, что норма $N_{L/K}(\alpha)$ равна $a_0^{[L:K(\alpha)]}$, а след $\mathrm{Tr}_{L/K}(\alpha)$ равен $[L : K(\alpha)]a_{n-1}$.

(в) Используя теорему Артина о характерах, доказать, что $\mathrm{Tr}_{L/K}$ не является тождественно нулевым отображением.

(г) (для знакомых с линейной алгеброй) Доказать, что на линейном пространстве L над K билинейная форма $\mathrm{Tr}_{L/K}(ab) : L \times L \to K$ невырождена. Вывести отсюда, что $\sqrt{p_1}, \ldots, \sqrt{p_n}$ линейно независимы над где $\mathbb{Q}$, $p_1 \ldots, p_n$ различные простые числа.

(д) (для знакомых с линейной алгеброй) Любому элементу $\alpha \in L$ можно сопоставить оператор A_α умножения на α в линейном пространстве L над K. Доказать, что это гомоморфизм $L \to GL_K(L)$, и что определитель и след оператора M_α равны $N_{L/K}(\alpha)$ и $\mathrm{Tr}_{L/K}(\alpha)$ соответственно. (Указание: заметить, что M_α является корнем свего характеристического многочлена, в то время, как α является корнем свего минимального многочлена.)

Упражнение 2.5. Построения циркулем и линейкой.

(а) Пользуясь тем, что π трансцендентно, доказать, что циркулем и линейкой невозможно построить квадрат, имеющий ту же площадь, что и нарисованный на плоскости круг с отмеченным центром (квадратура круга).

(б) Показать, что деление данного угла на три равных части (трисекция угла) равносильно построению числа $\cos(\varphi/3) + i\sin(\varphi/3)$ по числам $\cos(\varphi) + i\sin(\varphi) = \xi$ и 1. Доказать, что данная задача разрешима циркулем и линейкой тогда и только тогда, когда многочлен $x^3 - \xi \in K[x]$ имеет корень в K, где $K = \mathbb{Q}(\xi)$. Привести примеры углов, для которых задача трисекции разрешима и неразрешима. (Указание: рассмотреть углы $\pi/2$, $\pi/3$.)

(в) Постройте циркулем и линейкой правильный 5-угольник. Для энтузиастов предлагается построить правильный 17-угольник.

Упражнение 2.6. Аналог между фундаментальной группой и группой Галуа.

Найти фундаментальную группу окружности $\pi_1(S^1)$, рассмотрев накрытие $\mathbb{R} \to S^1$, являющееся факторизацией по $\mathbb{Z} \subset \mathbb{R}$. Показать, в чем аналог между окружностью и конечными полями.

Упражнение 2.7. Решение кубического уравнения.

Решить кубическое уравнение, пользуясь тем, что группа S_3 разрешима.