D-MATH Algebra I HS17
Prof. Emmanuel Kowalski

Assignment 11

Field extensions

1. Let $f = X^4 - X - 1 \in \mathbb{Q}[X]$ and $\alpha \in \mathbb{C}$ a root of f. Let $K := \mathbb{Q}(\alpha)$.

   (a) Prove that the polynomial $\overline{f} = X^4 - X - 1 \in \mathbb{F}_2[X]$ is irreducible in $\mathbb{F}_2[X]$.

   (b) Deduce that f is irreducible in $\mathbb{Q}[X]$. Recall: this implies that $\mathbb{Q}[X]/(f) \cong K$.

   (c) Write down the following elements as linear combinations of the $\mathbb{Q}$-basis elements $1, \alpha, \alpha^2, \alpha^3$:

$$\alpha^{10}, \quad \frac{1}{\alpha}, \quad \frac{1}{\alpha + 1}, \quad \frac{\alpha^5}{\alpha^2 + 2}.$$

2. Let p be a prime number. Recall that the canonical projection $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ induces a surjective ring homomorphism

$$\pi_p : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X].$$

   Let $f = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ be a polynomial such that p divides $a_0, a_1, \ldots, a_{n-1}$, p does not divide a_n and p^2 does not divide a_0.

   (a) Prove that $\pi_p(f)$ is monomial of degree n in $\mathbb{F}_p[X]$.

   (b) Prove that f is irreducible in $\mathbb{Q}[X]$ [This result is referred to as *Eisenstein's criterion*]

3. Let $a \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$ be a *square-free* integer, that is, an integer which is not divisible by any perfect square except 1. Prove that, for each $n \in \mathbb{Z}_{>0}$, the polynomial $X^n - a \in \mathbb{Q}[X]$ is irreducible. Conclude that there are irreducible polynomials in $\mathbb{Q}[X]$ of any degree $n \geqslant 1$.

4. Let p be a prime number. Let $\zeta := e^{\frac{2\pi i}{p}} \in \mathbb{C}$ and consider the polynomial

$$f := \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1 \in \mathbb{Q}[X].$$

   (a) Prove that f is irreducible [*Hint:* $g(X) := f(X + 1)$. Use Exercise 2]

   (b) Deduce that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. The field $\mathbb{Q}(\zeta)$ is called the *p-th cyclotomic field.*

5. Let $f = \sum_i a_i X^i \in \mathbb{Z}[X]$. Suppose that $\alpha \in \mathbb{Q}$ is a root of f and write $\alpha = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$.

(a) Prove that $a|a_0$ and $b|a_n$.

(b) Deduce that $2X^4+X+3 \in \mathbb{Q}[X]$ has no roots in $\mathbb{Q}$. Is it irreducible in $\mathbb{Q}[X]$?

6. Let $x \in \mathbb{R} \smallsetminus \mathbb{Q}$ be algebraic over $\mathbb{Q}$. Let $f = \operatorname{irr}(x, \mathbb{Q})$ and $n = \deg(f)$.

   (a) Show that there exists $c \in \mathbb{R}_{>0}$ such that, for any $\frac{a}{b} \in \mathbb{Q}$ with coprime $a, b \in \mathbb{Z}$, $b > 0$, we have

   $$\left| x - \frac{a}{b} \right| > \frac{c}{b^n}.$$

   [*Hint:* Write $f(\frac{a}{b}) = f(\frac{a}{b}) - f(x) = (\frac{a}{b} - x)f'(y)$ for some y]

   (b) Show that $\alpha := \sum_{n=1}^{\infty} 10^{-n!}$ is an irrational number.

   (c) Show that α is transcendental over $\mathbb{Q}$. [*Hint:* Consider $\frac{a_m}{b_m} = \sum_{n=1}^{m} 10^{-n!}$ and estimate $|\alpha - \frac{a_m}{b_m}|$]

7. [Transcendence of e] Let $f \in \mathbb{R}[X]$ be a polynomial of degree m. For $t \in \mathbb{R}$, define

   $$I_f(t) := \int_0^t e^{t-u} f(u) du.$$

   (a) Show that $I_f(t) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t)$. [*Hint:* Induction and integration by parts]

   (b) Show that $|I_f(t)| \leqslant |t| e^{|t|} \tilde{f}(|t|)$, where $\tilde{f} = \sum_{i=0}^{m} |a_i| X^i$ if $f = \sum_{i=0}^{m} a_i X^i$.

   (c) From now on, we assume by contradiction that e is algebraic over $\mathbb{Q}$. Show that there exist $n \in \mathbb{Z}_{>0}$ and $q_0, \ldots, q_n \in \mathbb{Z}$ with $q_n \neq 0$, such that

   $$q_0 + q_1 e + \cdots + q_n e^n = 0.$$

   (d) Let p be a prime number and $f_p = X^{p-1}(X-1)^p \cdots (X-n)^p$. Define

   $$J_p = \sum_{k=0}^{n} q_k I_{f_p}(k).$$

   Show that there exists a constant $c \in \mathbb{R}_{>0}$ independent of p such that

   $$|J_p| \leqslant c^p.$$

   [*Hint:* Prove that $\tilde{f}_p(k) \leqslant (2n)^m$, where $m = \deg(f_p)$, for $k = 0, \ldots, n$.]

   (e) Prove that

   $$J_p = -\sum_{j=0}^{m} \sum_{k=0}^{n} q_k f_p^{(j)}(k), \quad \text{where } m = (n+1)p - 1.$$

   (f) Using part (e), show that if $p > n$ and $p > |q_0|$, then J_p is an integer divisible by $(p-1)!$ but not by $p!$

   (g) Conclude by contradiction that e is transcendental over $\mathbb{Q}$.