Math 601 – Spring 2026 – Harry Tamvakis
PROBLEM SET 7 – Due April 9, 2026

A1) Let $n \geq 1$ be positive integer and

$$\zeta_n := e^{2\pi i/n} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}).$$

Find the minimal polynomial over $\mathbb{Q}$ of (a) ζ_5 (b) ζ_6 (c) ζ_8 (d) ζ_{10}.

A2) Let K_1 and K_2 be two finite extensions of a field F which are contained in the field L. Assume that both K_1 and K_2 are splitting fields (of some polynomials) over F. Prove that the composite field K_1K_2 and the intersection $K_1 \cap K_2$ are both splitting fields over F.

A3) Let K_1 and K_2 be two finite extensions of a field F which are both contained in the field L. Prove that the F-algebra $K_1 \otimes_F K_2$ is a field if and only if $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.

A4) Show that if F is an infinite field, then the multiplicative group $(F^*, \cdot)$ is not cyclic.

A5) (a) Let p be a prime and $f(x)$ be an irreducible polynomial of degree n over the finite field $\mathbb{F}_p$. Show that $\mathbb{F}_p[x]/(f(x))$ is a field with p^n elements, which is isomorphic to a splitting field of the polynomial $x^{p^n} - x$ and $f(x)$ divides $x^{p^n} - x$.

(b) Let $g(x)$ be an irreducible polynomial in $\mathbb{F}_p[x]$. Show that $g(x)$ divides $x^{p^n} - x$ if and only if $\deg(g(x))$ divides n.

A6) (a) Prove that $x^3 + x^2 + 1$ and $x^3 + x + 1$ are irreducible over the finite field $\mathbb{F}_2$.

(b) Give an explicit isomorphism between the quotients $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$ and $\mathbb{F}_2[x]/(x^3 + x + 1)$.

A7) For any prime p and non-zero $a \in \mathbb{F}_p$, prove that the polynomial $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$. [Hint: Prove that if α is root then $\alpha + 1$ is also a root.]

B1) A complex number z is called an *algebraic integer* if z is a root of a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with integer coefficients a_i, for some $n \geq 1$.

(a) Prove that if $\alpha_1, \ldots, \alpha_k$ are algebraic integers, then $\mathbb{Z}[\alpha_1, \ldots, \alpha_k]$ is a finitely generated abelian group.

(b) Prove that the set $\mathcal{O}$ of all algebraic integers is a *subring* of $\mathbb{C}$.

(c) Suppose that z is a root of a monic polynomial $g(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$ with coefficients $\alpha_i \in \mathcal{O}$. Prove that $z \in \mathcal{O}$.

B2) Let F be any field.

(a) Suppose that the additive group $(F, +)$ is a finitely generated abelian group. Prove that F must be a finite field.

(b) Suppose that F is a finite field. Classify the additive subgroup $(F, +)$ up to group isomorphism.

B3) Let F be a field and $F(x)$ be the quotient field of the polynomial ring $F[x]$. Let $t \in F(x)$ be the rational function $t = p(x)/q(x)$, where $p(x), q(x) \in F[x]$ are relatively prime polynomials and $q(x) \neq 0$. Then $F(x)$ is an extension of the field $F(t)$.

(a) Show that the polynomial $p(z) - tq(z)$ in the variable z and coefficients in $F(t)$ is irreducible over $F(t)$ and has x as a root. [Hint: By Gauss' Lemma this polynomial is irreducible in $(F(t))[z]$ if and only if it is irreducible in $(F[t])[z]$. Then note that $(F[t])[z] = (F[z])[t]$.]

(b) Show that $[F(x) : F(t)] = \max(\deg p(x), \deg q(x))$.

(c) Show that $F(t) = F(x)$ if and only if

$$t(x) = \frac{ax + b}{cx + d}$$

for some $a, b, c, d \in F$ such that $ad - bc \neq 0$.

C problem

C1) Let ϕ denote the Frobenius map $x \mapsto x^p$ on the finite field $\mathbb{F}_{p^n}$. Consider ϕ as an $\mathbb{F}_p$-linear transformation of the n-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_{p^n}$.

(a) Determine the rational canonical form over $\mathbb{F}_p$ for ϕ.

(b) Determine the Jordan canonical form for ϕ (over a field which contains all the eigenvalues of ϕ).