1 Fields and polynomials

1. Show that in a finite field, every element can be written as a sum of at most two squares.

2. i) For $n \geq 2$, show that for every prime p, $x^{2^n} + 1$ is reducible over $\mathbb{F}_p$ (but irreducible over $\mathbb{Q}$).

   ii) Show that for every prime p, $(x^2 - 2)(x^2 - 3)(x^2 - 6)$ has a root in $\mathbb{F}_p$, the finite field of order p (but has no root in $\mathbb{Q}$).

3. Let K be a field, $\varphi : K \to K$ a ring homomorphism, and $k := \{a \in K \mid \varphi(a) = a\}$ the fixed field of φ. Show that if $\alpha \in K \setminus \varphi(K)$, then α is transcendental over k. Deduce that if F is the prime subfield of K, and K/F is algebraic, then $\mathrm{End}(K) = \mathrm{Aut}(K) = \mathrm{Aut}(K/F)$.

4. Let $n, m, c \in \mathbb{N}$ with n, m not both even, and suppose $c = pr$ with p prime, $p \nmid r$. Show that $x^n + c^m$ is irreducible over $\mathbb{Q}$ iff $(n, m) = 1$.

5. Let ζ_n be a primitive n^{th} root of unity. Show that $\mathrm{Tr}(\zeta_n) = \mu(n)$, where $\mu(n)$ is the Möbius function (recall that if α is algebraic over $\mathbb{Q}$, then $\mathrm{Tr}(\alpha)$ is the sum of Galois conjugates of α).

2 Past exam problems

6. (6.11.18) Let k be a field, and $p_1, \ldots, p_n \in k[x]$. Show that $\gcd(p_1, \ldots, p_n) = 1$ iff there is an $n \times n$ matrix over $k[x]$ of determinant 1 whose first row is $p_1, \ldots, p_n$.

7. (6.11.7) For any $0 \neq f \in \mathbb{Q}[x]$, show that there exists $0 \neq g \in \mathbb{Q}[x]$ such that $f(x)g(x) = a_2x^2 + a_3x^3 + a_5x^5 + \ldots + a_px^p$ has only prime degrees appearing.

8. (6.12.16) Show that for any $n \in \mathbb{N}$, the field $\mathbb{Q}(t_1, \ldots, t_n)$ of rational functions in n variables is isomorphic to a subfield of $\mathbb{R}$.

9. (6.12.5) Show that a finite subgroup of the group of units of a field is cyclic.

10. (6.11.32) Let k be a field, p a prime, and $a \in k$. If a is not a p^{th} power in k, show that $x^p - a$ is irreducible in $k[x]$.