MATH 422: MISSION 2: FIELD EXTENSIONS AND ELEMENTARY GALOIS THEORY

Show **your** work carefully. 3pts per problem.

Problem 36: Find the splitting field of $x^3 - 1$ over $\mathbb{Q}$. Express your answer in form $\mathbb{Q}(a)$.

Problem 37: Let $a, b \in \mathbb{R}$ with $b \neq 0$. Show that $\mathbb{R}(a + bi) = \mathbb{C}$.

Problem 38: Let $F = \mathbb{Q}(\pi^3)$. Find a basis for $F(\pi)$ over F.

Problem 39: Let $f(x) \in F[x]$ and $a \in F$. Show that $f(x)$ and $f(x + a)$ have the same splitting field over F.

Problem 40: If β is a zero of $x^2 + x + 2$ over $\mathbb{Z}_5$ then find the other zero.

Problem 41: Show that $x^{21} + 2x^8 + 1$ does not have multiple zeros in any extension of $\mathbb{Z}_3$.

Problem 42: Let E be the algebraic closure of a field F. Show that every polynomial in $F[x]$ splits in E.

Problem 43: Suppose F is a field and every irreducible polynomial in $F[x]$ is linear. Show F is algebraically closed.

Problem 44: Suppose E is an extension of F and $a, b \in E$. If a is algebraic over F of degree m, and b is algebraic over F of degree n, where m and n are relatively prime, show that $[F(a, b) : F] = mn$.

Problem 45: Let K be a field extension of F and $a \in K$. Show $[F(a) : F(a^3)] \leq 3$. Find examples to illustrate $[F(a) : F(a^3)]$ can take on the values 1,2 or 3.

Problem 46: Find the minimal polynomial for $\sqrt{-3} + \sqrt{2}$ over $\mathbb{Q}$.

Problem 47: Let E b a finite extension of $\mathbb{R}$. Use the fact that $\mathbb{C}$ is algebraically closed to prove either $E = \mathbb{C}$ or $E = \mathbb{R}$.

Problem 48: Suppose $p(x) \in F[x]$ and E is a finite extension of F. If $p(x)$ is irreducible over F and $\deg(p(x))$ and $[E : F]$ are relatively prime, show that $p(x)$ is irreducible over E.

Problem 49: If α and β are transcendental over $\mathbb{Q}$, show that either $\alpha\beta$ or $\alpha + \beta$ is also transcendental over $\mathbb{Q}$.

Problem 50: Find the splitting field for $x^4 - x^2 - 2$ over $\mathbb{Z}_3$.

Problem 51: If F is a field and the multiplicative group of nonzero elements of F is cyclic, prove F is finite.

Problem 52: Let $a, b \in \mathbb{Q}$. Show that $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$.

Problem 53: Show that it is impossible to construct, with a compass and straightedge, a square whose area equals that of a circle of radius 1. You may use the fact that π is transcendental over $\mathbb{Q}$.

Problem 54: If $[F(a) : F] = 5$, find $[F(a^3) : F]$.

Problem 55: If $a \neq 0$ belongs to a field F and $x^n - a$ splits in some extension E of F, prove that E contains all the n-th roots of unity.

Problem 56: Let $E = \mathbb{Q}[\sqrt{2}, \sqrt[3]{5}]$. Prove $[E : \mathbb{Q}] = 6$.

Problem 57: Let K be a field, and F and extension field of K. Let $\phi : F \to F$ be an automorphism of F such that $\phi(a) = a$ for all $a \in K$. Show that any polynomial $f(x) \in K[x]$, and any root $u \in F$ of $f(x)$, the image $\phi(u)$ must be a root of $f(x)$.

Problem 58: Use the previous exercise to show there are at most four distinct automorphisms of the field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Problem 59: Prove there are only two automorphisms of $\mathbb{Q}(i)$.

Problem 60: Show the splitting field of $x^4 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[4]{2}, i)$. Also, show $x^4 + 2$ over $\mathbb{Q}$ likewise takes $\mathbb{Q}(\sqrt[4]{2}, i)$ as its splitting field.

Problem 61: Show there are at most eight distinct automorphisms of the splitting field $\mathbb{Q}(\sqrt[4]{2}, i)$ over $\mathbb{Q}$.

Problem 62: Let F be a finite field with p^n elements. Then F is the splitting field of the polynomial $x^{p^n} - x$ over the prime subfield of F.

Problem 63: Let F be a field of prime characteristic p and let $n \in \mathbb{N}$. Show:

a. $(a + b)^{p^n} = a^{p^n} + b^{p^n}$

b. $\{a \in F \mid a^{p^n} = a\}$ is a subfield of F.

Problem 64: Let F be a field of characteristic p. If n is a positive integer not divisible by p then the polynomial $x^n - 1$ has no repeated roots in any extension field of F.

Problem 65: For each prime p and each positive integer n, there exists a field with p^n elements.

Remark: the field whose existence is proved above is known as the Galois field of order p^n which we denote by $GF(p^n)$

Problem 66: Any finite subgroup of the multiplicative group of a field is cyclic.

Problem 67: Let F be an extension field of K, and let $f(x) \in K[x]$. Then any element of $Gal(F/K)$ defines a permutation of the roots of $f(x)$ that lie in F.

Problem 68: Show $Gal(Q(\sqrt[3]{2})/\mathbb{Q})$ is trivial.

Problem 69: Exhibit the Fundamental Theorem of Galois Theory for the Galois group of $x^3 - 2$ over $\mathbb{Q}$. In particular, provide the subgroup and subfield lattice diagrams.

Problem 70: Find the Galois group of $x^4 - x^2 - 6$ over $\mathbb{Q}$.