KFUPM/ Department of Mathematics/T211/MATH 423/Final Exam

Name: ID#:

---

1. [8pts] Let G be the group $\mathbb{Z}_4 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{50}$.

(a) Find the elementary divisors of G.

(b) Find the invariant factors of G.

---

2. [12pts] (a) Let R be UFD and let $a, b \in R$ with $ab \neq 0$. Prove that $\gcd(a,b) \operatorname{lcm}(a,b) \sim ab$.

(b) Let D be a Euclidean domain with valuation v and let a, b be nonzero elements of D. Show that

(i) $v(1) \leq v(a)$.

(ii) If $a \sim b$, then $v(a) = v(b)$.

(iii) $v(ab) = v(b)$ if and only if a is a unit.

(c) Is it true that subrings of Euclidean domains are Euclidean domains? Justify.

---

3. [12pts] (a) Let F be a field and a be an element in some extension E of F. Let $g(x)$ be a nonconstant polynomial in $F[x]$.

(i) Show that $g(a) \in F(a)$.

(ii) Suppose $g(a)$ is algebraic over F. Prove that a is algebraic over F.

(b) Let K be an extension of a field F such that $[K : F]$ is prime. Show that $\forall a \in K$, either $F(a) = F$ or $F(a) = K$.

---

4. [12pts] Consider the polynomial $f(x) = x^4 + 2x^2 - 8$.

(a) Find a splitting field E for $f(x)$ over $\mathbb{Q}$.

(b) Find a $\mathbb{Q}$-basis for E.

---

5. [12pts] Let a be a root of the polynomial $p(x) = x^2 + 1$ over $\mathbb{Z}_3$ in some splitting field E for $p(x)$ over $\mathbb{Z}_3$ and let $F = \mathbb{Z}_3(a)$.

(a) List the elements of F.

(b) Is $a + 1$ is a generator for the group of units F^* of F? Justify.

(c) Are E and F isomorphic? Justify.

---

6. [12pts] (a) Find $\operatorname{Gal}\left(\mathbb{Q}\left(\sqrt{3}\right)/\mathbb{Q}\right)$.

(b) Let p be a prime number. Prove that $\operatorname{Gal}\left(\mathbb{Q}\left(\sqrt[3]{p}\right)/\mathbb{Q}\right)$ consists of one automorphism only.

---

7. [12pts] Let $G = \operatorname{Gal}\left(\mathbb{Q}\left(\sqrt{2}, i\right)/\mathbb{Q}\right)$.

(a) Show that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) Draw the subgroup lattice of G and the corresponding subfield lattice of $\mathbb{Q}\left(\sqrt{2}, i\right)$.