MAT 612 **Exam 2 (take-home)** Name SOLUTIONS
04/07/2010 (due Wednesday 04/14/2010, 5 pm)
90 points

1.(20) Let $F \subseteq E$ be a field extension.

(a) Suppose $\alpha \in E$ is transcendental over F. Prove that $F[\alpha]$ is isomorphic to $F[x]$. (Hence $F(\alpha)$ is isomorphic to $F(x)$.)

(b) A subset $S = \{\alpha_1, \ldots, \alpha_n\}$ of E is said to be *algebraically dependent* over F if there is a nonzero polynomial $p \in F[x_1, \ldots, x_n]$ such that $p(\alpha_1, \ldots, \alpha_n) = 0$. A set is *algebraically independent* if it is not algebraically dependent.

Suppose $\{\alpha_1, \ldots, \alpha_n\}$ is an algebraically independent subset of E. Prove that $F[\alpha_1, \ldots, \alpha_n]$ is isomorphic to $F[x_1, \ldots, x_n]$. (Hence $F(\alpha_1, \ldots, \alpha_n)$ is isomorphic to $F(x_1, \ldots, x_n)$.)

(c) Suppose $\{\alpha_1, \ldots, \alpha_n\}$ is a *maximal* algebraically independent subset of E. Prove that E is algebraic over $F(\alpha_1, \ldots, \alpha_n)$.

2.(20) Suppose $F \subseteq K \subseteq E$ are field extensions.

(a) Suppose $\alpha \in E$ is algebraic over F. Prove α is algebraic over K and $m_\alpha^K(x)$ divides $m_\alpha^F(x)$ in $E[x]$.

(b) Suppose $\alpha, \beta \in E$ are algebraic over F, and $m_\alpha^F(x)$ and $m_\beta^F(x)$ have relatively prime degrees. Prove that $m_\alpha^F(x) = m_\alpha^{F[\beta]}(x)$.

3.(15) Suppose $E = F[\alpha]$ with α algebraic over F. Prove that $|\operatorname{Gal}(E, F)| \leq |E : F|$.
(Hint: Consider the roots of $m_\alpha^F(x)$ in E.)

4.(15) Suppose $F \subseteq E$ is a field extension.

(a) Let $\alpha, \beta \in E$. Suppose there exist distinct elements $s, t \in F$ such that $F[\alpha + s\beta] = F[\alpha + t\beta]$. Prove that $F[\alpha, \beta] = F[\alpha + s\beta]$.
(Note: The hypothesis will hold if F is infinite and there are only finitely many fields K with $F \subseteq K \subseteq E$.)

(b) Suppose E and F are finite. Show $E = F[\alpha]$ for some $\alpha \in E$.

5.(20) Let $R = \Bbbk[x_1, \ldots, x_n]$, $\Bbbk$ a field. A *monomial* in R is an element of the form $cx_1^{a_1} \cdots x_n^{a_n}$, where $0 \neq c \in \Bbbk$ and each a_i is a non-negative integer. This element is denoted $c\mathbf{x}^{\mathbf{a}}$ where $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$. (For example, $(x, y, z)^{(2,0,3)} = x^2 z^3$.) Then $\mathbf{x}^{\mathbf{a}}\mathbf{x}^{\mathbf{b}} = \mathbf{x}^{\mathbf{a}+\mathbf{b}}$.

A *monomial ideal* in R is an ideal generated by monomials.

(a) Suppose I is a monomial ideal. Show that I is prime if and only if I is generated by a subset $\{x_{i_1}, \ldots, x_{i_k}\}$ of the variables $\{x_1, \ldots, x_n\}$.

(b) Suppose I is a monomial ideal, and $f \in R$. Note that f can be written in the form $\sum_{\mathbf{a} \in S} c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}}$ for some finite set S of vectors in $\mathbb{N}^n$, where $c_{\mathbf{a}} \in \Bbbk$ for $\mathbf{a} \in S$. Suppose $f \in I$. Show that every term of f is in I.
Notational hint: write $I = (\mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_k})$. (Why only finitely many? Why no c's?)

(c) Let I be the ideal generated by $\{ad, ae, bcd, be, ce, de\}$ in $R = \Bbbk[a, b, c, d, e]$. Express I as an intersection of prime ideals, and answer these questions: is I radical? does I have any embedded primes?
Hint: Use ideal quotient.

(over for solutions)

(1)(a) Let $\varphi = ev_\alpha : F[x] \longrightarrow F[x]$, $f \longmapsto f(\alpha)$. Then φ is surjective. If $f \neq 0$ lies in $\ker(\varphi)$, then $f(\alpha) = 0$, implying α is algebraic, a contradiction. Thus $\ker(\varphi) = 0$ and φ is an isomorphism.

(b) As in (a), let $\varphi : F[x_1, \dots, x_n] \longrightarrow F[\alpha_1, \dots, \alpha_n]$ be defined by $\varphi(p) = p(\alpha_1, \dots, \alpha_n)$. Then φ is surjective, and $\ker(\varphi) = 0$ because $\{\alpha_1, \dots, \alpha_n\}$ is algebraically independent. Thus φ is an isomorphism.

(c) Let $\alpha \in E$. Then $\{\alpha_1, \dots, \alpha_n, \alpha\}$ is algebraically dependent, by the maximality assumption. Then $\exists\ p \in F[x_1, \dots, x_n, x]$, $p \neq 0$, such that $p(\alpha_1, \dots, \alpha_n, \alpha) = 0$. Then $p \in F(x_1, \dots, x_n)[x]$ and $p(\alpha) = 0$, so α is algebraic over $F(x_1, \dots, x_n)$.

(2)(a) Let $\varphi : K[x] \longrightarrow E$ be defined by $\varphi(p) = p(\alpha)$. Since $K[x]$ is a PID, $\ker(\varphi)$ is a principal ideal, generated by m_α^K, by definition. Since $F \subseteq K$, $m_\alpha^F \in K[x]$. Since $m_\alpha^F(\alpha) = 0$, α is algebraic over K. Also $m_\alpha^F \in \ker(\varphi)$, hence m_α^F is a multiple of m_α^K.

(b) Note: Since β is algebraic over F, $F[\beta] = F(\beta)$ is a field. By part (a), $m_\alpha^{F[\beta]}$ divides m_α^F; since both are monic it suffices to show they have the same degree. We have $|F[\alpha,\beta] : F| = |F[\alpha,\beta] : F[\beta]|\,|F[\beta] : F| = (\deg m_\alpha^{F[\beta]})(\deg m_\beta^F)$ and $|F[\alpha,\beta] : F| = |F[\alpha,\beta] : F[\alpha]| \cdot |F[\alpha] : F| = |F[\alpha,\beta] : F[\alpha]| \cdot (\deg m_\alpha^F)$. Then $\deg m_\alpha^F$ divides $(\deg m_\alpha^{F[\beta]})(\deg m_\beta^F)$. Since $\deg m_\alpha^F$ and $\deg m_\beta^F$ are relatively prime, $\deg m_\alpha^F$ divides $\deg m_\alpha^{F[\beta]}$. Then $\deg m_\alpha^F \leq \deg m_\alpha^{F[\beta]}$. Since $m_\alpha^{F[\beta]}$ divides m_α^F, $\deg m_\alpha^{F[\beta]} \leq \deg m_\alpha^F$, hence equality holds. □

2(b) (continued) Here is an example: $m^{\mathbb{Q}}_{\sqrt[3]{2}}(x) = x^3 - 2$ and $m^{\mathbb{Q}}_{\sqrt{2}}(x) = x^2 - 2$, so $x^3 - 2$ is irreducible over $\mathbb{Q}[\sqrt{2}]$.

(3) Let $\alpha_1, \ldots, \alpha_p$ be the roots of $m^F_\alpha(x)$ in E. If $\varphi \in Gal(E,F)$, then $\varphi(m^F_\alpha(x)) = m^F_\alpha(x)$, so $m^F_\alpha(\alpha_i) = 0 \Rightarrow m^F_\alpha(\varphi(\alpha_i)) = 0$. Hence $\varphi(\alpha) = \alpha_i$ for some i. Since $E = F[\alpha]$, $\varphi : E \to E$ is uniquely determined by $\varphi(\alpha)$. (since $\varphi|_F = id_F$). There are at most p possibilities for $\varphi(\alpha)$, hence $|Gal(E,F)| \le p$. But $m^F_\alpha(x)$ has at most n roots, where $n = \deg m^F_\alpha = |E:F|$, hence $|Gal(E,F)| \le |E:F|$.

(4) (a) Suppose $F[\alpha + s\beta] = F[\alpha + t\beta] = K$, with $s \neq t$, $s, t \in F$. Then $(\alpha + s\beta) - (\alpha + t\beta) \in K$, so $(s-t)\beta \in K$. Since $s - t \in F \subseteq K$ and $s - t \neq 0$, $\beta = (s-t)^{-1}(s-t)\beta \in K$. Then $\alpha = (\alpha + t\beta) - t\beta \in K$, so $F[\alpha, \beta] \subseteq K$. Obviously $K = F[\alpha + s\beta] \subseteq F[\alpha, \beta]$. Thus $F[\alpha, \beta] = K = F[\alpha + s\beta]$.
Note: if E is infinite and there are only finitely many fields K with $F \subseteq K \subseteq E$, then $\exists\, s \neq t$ in F with $F[\alpha + s\beta] = F[\alpha + t\beta]$ by the pigeonhole principle.

(b) Since E is finite, $E^\times = E - \{0\}$ is cyclic. Let $\alpha \in E$ such that $\langle \alpha \rangle = E^\times$. Then every $\beta \in E - F$ can be written $\beta = p(\alpha)$ where $p(x) = x^k$. Thus $E = F[\alpha]$.

(5) Let $I = \langle \underline{x}^{\underline{a}_1}, \ldots, \underline{x}^{\underline{a}_p} \rangle$ be a monomial ideal. Assume I is prime. Suppose $\underline{a}_j = \underline{b} + \underline{c}$ where $\underline{b}, \underline{c} \in \mathbb{N}^n$ are both nonzero. Then $\underline{x}^{\underline{a}_j} = \underline{x}^{\underline{b}} \cdot \underline{x}^{\underline{c}}$. Since I is prime, $\underline{x}^{\underline{b}} \in I$ or $\underline{x}^{\underline{c}} \in I$. Say $\underline{x}^{\underline{b}} \in I$. Then $\underline{x}^{\underline{a}_j}$ can be replaced by $\underline{x}^{\underline{b}}$ in the generating set,

(over)

since any multiple of x^{a_j} is a multiple of x^b.
Thus, we may assume, for each j, $1 \le j \le k$, a_j cannot be written as a sum of nonzero vectors in $\mathbb{N}^n$. It follows that $a_j = 0$ or 1 for every j, and at most one a_i is nonzero. Then $x^{a_j} = x_{i_j}$ for $1 \le i_1 \le i_2 \le \cdots \le i_k \le n$. Thus I is generated by a subset of the variables. (see below for proof)

(b) Let I be a monomial ideal in $R = k[x_1, \ldots, x_n]$. Since R is noetherian, I is generated by finitely many monomials.* $I = \langle c_1 x^{a_1}, \ldots, c_k x^{a_m} \rangle$ for some $a_i \in \mathbb{N}^n$ and $c_i \in k$. Since k is a field, c_i is a unit (if nonzero), hence may assume without loss that $c_i = 1 \ \forall\, i$. Suppose $f = \sum_{a \in S} c_a x^a \in I$, with $c_a \in k$. Then $\exists$ $f_k \in R$ for $1 \le k \le m$ such that $\sum_{k=1}^{m} f_k x^{a_k} = \sum_{a \in S} c_a x^a$. Write $f_k = \sum_{b \in S_k} c_{b,k} x^b$. Then $\sum_{k=1}^{m} f_k x^{a_k} = \sum_{k=1}^{m} \sum_{b \in S_k} c_{a,k} x^{b + a_k}$ $= \sum_{a \in S} c_a x^a$. Let $a \in S$, with $c_a \neq 0$. Then, for some $1 \le k \le m$ and $b \in S_k$, $b + a_k = a$. Then $c_a x^a = (c_a x^b) x^{a_k}$ is an element of I. Thus every term of f is in I.

* Since R is noetherian, the family of ideals $J \subseteq I$ generated by finitely many monomials has a maximal element, which one can easily show must be equal to I.

(c) Suppose $f \in R$ and $g \in (I : f)$. Then $fg \in I$. By (b) this means that every nonzero term of fg is in I. It follows that $(I : f_1 + f_2) = (I : f_1) \cap (I : f_2)$, so if $(I : f)$ is prime we may assume f is a monomial. Also $g \in (I : x^a)$ iff every term of gx^a is

in I, if and only if every term of g is in $(I : \underline{x}^{\underline{a}})$. Thus $(I : \underline{x}^{\underline{a}})$ is a monomial ideal. Using (a), we need to find subsets S of $\{a,b,c,d,e\}$ and monomials $\underline{x}^{\underline{a}}$ such that $(I : \underline{x}^{\underline{a}}) = (S)$. $I = (ad, ae, bcd, be, ce, de)$. Setting $\underline{a} = (1,0,0,0,0)$, $(I : a) = (d, e)$; $\underline{a} = (0,1,0,0,0)$ $\Rightarrow (I : b) = (cd, e)$, not prime. Continuing, $(I : c) = (bd, e)$, not prime; $(I : d) = (a, bc, e)$, not prime; $(I : e) = (a, b, c, d)$; $(I : ab) = (d, e)$, $(I : ac) = (d, e)$, $(I : ad) = R$, $(I : ae) = R$, $(I : bc) = (d, e)$, $(I : bd) = (a, c, e)$, $(I : be) = R$, $(I : cd) = (a, b, e)$, $(I : ce) = R$, $(I : de) = R$, $(I : abc) = (d, e)$. All other monomials $\underline{x}^{\underline{a}}$ lie in I, so $(I : \underline{x}^{\underline{a}}) = R$. So the associated primes of I are: (d, e), (a, b, c, d), (a, c, e), and (a, b, e). (Note: all equalities are proved using (b).)

$I = (a, b, c, d) \cap (a, c, e) \cap (a, b, e) \cap (d, e)$.

This would follow from a proof that I is radical (using the primary decomposition of I). And I is radical because none of its generators have repeated factors,* as follows: let $f = \sum_{\underline{a} \in S} c_{\underline{a}} \underline{x}^{\underline{a}} \in \sqrt{I}$, so $f^n \in I$. Then, by (b), $\underline{x}^{\underline{a}_1 + \cdots + \underline{a}_n} \in I$ for any $\underline{a}_1, \ldots, \underline{a}_n \in S$. In particular, $(\underline{x}^{\underline{a}})^n \in I$ for every $\underline{a} \in S$. This implies $(\underline{x}^{\underline{a}})^n$ is a multiple of one of the generators. Then $n\underline{a} = k(1,0,0,1,0)$ or $k(1,0,0,0,1)$, etc., for some k, which implies $\underline{a}$ has the same property, hence $\underline{x}^{\underline{a}} \in I$.

* I is called a "squarefree monomial ideal."

But we can prove the claim directly, using (b). We have $I \subseteq (a,b,c,d) \cap (a,c,e) \cap (b,d) \cap (d,e)$ automatically

(over)

Let $f \in (a,b,c,d) \cap (a,c,e) \cap (a,b,e) \cap (d,e)$. Then every term of f lies in the intersection also, so we may assume without loss that f is a monomial. Then f is a multiple of d or e. Case 1: $f = gd$. Then g is a multiple of a, c, or e, so f is a multiple of ad, cd, or de. In the first and last cases, $f \in I$. If $f = hcd$, then h is a multiple of a, b, or e, since $f \in (a,b,e)$. Then f is a multiple of acd, bcd, or cde, hence f is in I.

Case 2: $f = ge$. Then g is a multiple of a, b, c, or d, hence f is a multiple of ae, be, ce, or de, hence $f \in I$. This proves equality.

Since I is an intersection of prime ideals, this is a standard primary decomposition, so there are no embedded primes, and I is radical.