MAT 612 **Final Exam (take-home)** Name SOLUTIONS

04/30/2010 (due Thursday 05/6/2010, 5 pm)

120 points

1.(15) Let M be the $\mathbb{Z}$-module (i.e., abelian group) generated by three elements a, b, c, subject to the relations $28a + 12b + 4c = 0$ and $32a + 16b + 8c = 0$. Find the invariant factor decomposition of M. Identify the rank and torsion submodule of M.

2.(20) Let $R = \mathbb{Q}[x]$ and $A = \begin{bmatrix} 3 & 3 & 4 \\ 0 & 2 & 4 \\ 0 & 1 & 2 \end{bmatrix}$. Define an R-module structure on $M = \mathbb{Q}^3$ by $p(x) \cdot v = p(A)v$.

(a) Find $x \cdot e_1, x \cdot e_2$, and $x \cdot e_3$ where e_1, e_2, and e_3 are the standard basis vectors in $\mathbb{Q}^3$.

(b) Let $\varphi\colon R^3 \longrightarrow M$ be the unique homomorphism satisfying $\varphi((1,0,0)) = e_1, \varphi((0,1,0)) = e_2$, and $\varphi((0,0,1)) = e_3$. Find $\varphi(2x, 1 + x^2, 2 - x)$.

(c) Find generators for the kernel of φ, and a presentation matrix for M as an R-module.

(d) Find the orders (annihilators) of the cyclic submodules of M generated by e_1, e_2, and e_3.

3.(15) Let $\Bbbk$ be a field and $R = \Bbbk[x, y]$. Find a free resolution of the R-module R/I, where I is the ideal (x^2, xy).

4.(15) Let $Q \subseteq R$ be a primary ideal,and let $P = \sqrt{Q}$. Let A be an ideal of R with $A \not\subseteq Q$, and set $I = (Q : A) = \{r \in R \mid rA \subseteq Q\}$. Show that $\sqrt{I} = P$ and I is primary.

5.(15) Suppose $F \subseteq E$ is a field extension with $|E : F| < \infty$. Prove that $|\mathrm{Gal}(E, F)|$ divides $|E : F|$.

6.(25) Determine the degree of the following field extensions.

(a) $\mathbb{Q} \subseteq \mathbb{Q}[\omega]$ where $\omega = e^{\frac{2\pi i}{3}}$.

(b) $\mathbb{Q} \subseteq E$ where E is a splitting field of the polynomial $f(x) = x^p - q$ over $\mathbb{Q}$, where p and q are prime.

(c) Show that the regular pentagon is constructible with compass and straight-edge.

7.(15) Let $F \subseteq E$ with $|E : F| < \infty$. Suppose $f \in F[X]$ is irreducible and $\deg(f) = p$ is prime. Prove: if f is reducible over E then p divides $|E : F|$.
Hint: Consider $E[\alpha]$ and $F[\alpha]$, where α is a root of f in a splitting field of f over E.

(1) We are given the presentation $\mathbb{Z}^2 \xrightarrow{p} \mathbb{Z}^3 \xrightarrow{q} M \longrightarrow 0$ where $p(e_1) = 28e_1 + 12e_2 + 4e_3$ and $p(e_2) = 32e_1 + 16e_2 + 8e_3$, and $q(e_1) = a$, $q(e_2) = b$, $q(e_3) = c$. We reduce the relation matrix $\begin{bmatrix} 28 & 12 & 4 \\ 32 & 16 & 8 \end{bmatrix}$ to Smith Normal Form and keep track of the steps. For clarity write f_1, f_2, f_3 for the standard basis of $\mathbb{Z}^3$. (over for calculation)

$$\begin{matrix} & f_1 & f_2 & f_3 \\ e_1 \\ e_2 \end{matrix}\begin{bmatrix} 28 & 12 & 4 \\ 32 & 16 & 8 \end{bmatrix} \sim \begin{bmatrix} -4 & -4 & -4 \\ 32 & 16 & 8 \end{bmatrix} \sim \begin{bmatrix} 4 & 4 & 4 \\ 32 & 16 & 8 \end{bmatrix}$$

$e_1 \leftarrow e_1 - e_2$ $\qquad$ $e_1 \leftarrow -e_1$.

$e_2 \leftarrow e_2 - 8e_1$

$$\begin{bmatrix} 4 & 0 & 0 \\ 0 & 8 & -24 \end{bmatrix} \leftarrow \begin{bmatrix} 4 & 0 & 0 \\ 0 & -16 & -24 \end{bmatrix} \leftarrow \begin{bmatrix} 4 & 4 & 4 \\ 0 & -16 & -24 \end{bmatrix}$$

$f_2 \leftarrow f_2 - f_3$ $\qquad$ $f_2 \leftarrow f_2 - f_1$, $f_3 \leftarrow f_3 - f_1$

$f_3 \leftarrow f_3 + 3f_2$

$$\begin{matrix} & f_1' & f_2' & f_3' \\ e_1' \\ e_2' \end{matrix}\begin{bmatrix} 4 & 0 & 0 \\ 0 & 8 & 0 \end{bmatrix}$$

We conclude that M is isomorphic to $\mathbb{Z}^3 / \mathbb{Z}(4,0,0) \oplus \mathbb{Z}(0,8,0)$, which is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}$. Then $\operatorname{rank}(M) = 1$ and $\operatorname{Tor}(M) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. To find the generators of $\operatorname{Tor}(M)$, we must find f_1' and f_2' by following the column operations. In terms of elementary matrices:

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \end{bmatrix} = P \begin{bmatrix} 28 & 12 & 4 \\ 32 & 18 & 8 \end{bmatrix} Q \text{ where } P = \begin{bmatrix} 1 & 0 \\ -8 & 1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$$

and $Q = \begin{bmatrix} 1 & -4 & -4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix}$ $\qquad = \begin{bmatrix} -1 & 1 \\ 8 & -7 \end{bmatrix}$

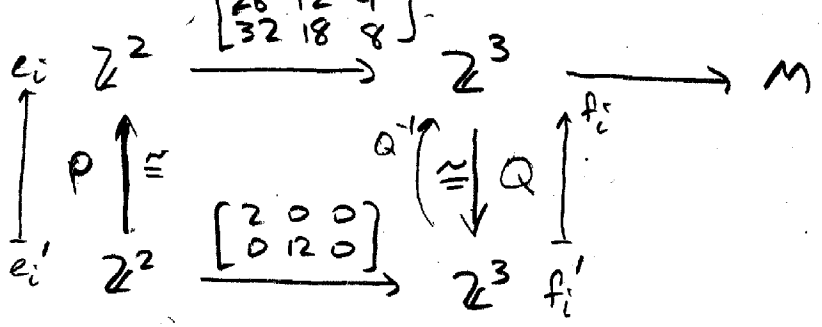
$$= \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 3 \\ 0 & -1 & -2 \end{bmatrix}.$$ Then $Q^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & -2 & -3 \\ 0 & 1 & 1 \end{bmatrix}$. Then

$f_1' = e_1 + e_2 + e_3$ and $f_2' = -2e_2 - 3e_3$.

Then $\boxed{\operatorname{Tor}(M) = \mathbb{Z}(a + b + c) \oplus \mathbb{Z}(-2b + 3c)}$.

Indeed, $4(a + b + c) = 4a + 4b + 4c = -(28a + 12b + 4c) + (32a + 16b + 8c)$, and $8(-2b + 3c) = -16b + 24c = -8(28a + 12b + 4c) + 7(32a + 16b + 8c)$.

Here is a diagram. Elements of $\mathbb{Z}^k$ are represented by row vectors.



② (a) $x \cdot e_1 = Ae_1 = \boxed{3e_1}$, $x \cdot e_2 = Ae_2 = \boxed{3e_1 + 2e_2 + e_3}$,
$x \cdot e_3 = Ae_3 = \boxed{4e_1 + 4e_2 + 2e_3}$.

(b) $\varphi(2x, 1+x^2, 2-x) = \varphi(2x(1,0,0) + (1+x^2)(0,1,0) + (2-x)(0,0,1))$
$= 2x \cdot \varphi(1,0,0) + (1+x^2) \cdot \varphi(0,1,0) + (2-x) \cdot \varphi(0,0,1)$
$= 2x \cdot e_1 + (1+x^2) \cdot e_2 + (2-x) \cdot e_3 = 2Ae_1 + (I + A^2)e_2 + (2-A)e_3$
$= 6e_1 + (19e_1 + 9e_2 + 4e_3) + (-4e_1 - 4e_2) = \boxed{21e_1 + 5e_2 + 4e_3}$

(c) For clarity let us denote the standard basis vectors of R^3 by f_1, f_2, f_3. Since $x \cdot e_1 = 3e_1$, $(x-3)f_1 \in \ker(\varphi)$. Similarly, $xf_2 - (3f_1 + 2f_2 + f_3) = -3f_1 + (x-2)f_2 - f_3 \in \ker(\varphi)$, and $xf_3 - (4e_1 + 4e_2 + 2e_3) = -4f_1 - 4f_2 + (x-2)f_3 \in \ker(\varphi)$. Claim $\ker(\varphi)$ is generated by these three elements. Call them r_1, r_2, r_3, and let $K = Rr_1 + Rr_2 + Rr_3$. In R/K, $x \cdot f_1 = Af_1$, $x \cdot f_2 = Af_2$, and $x \cdot f_3 = Af_3$. Then, if $p(x) = a_n x^n + \cdots + a_1 x + a_0$, $p(x) \cdot f_i = (a_n x^n + \cdots + a_0) \cdot f_i$
$= a_n x^n \cdot f_i + \cdots + a_1 x \cdot f_i + a_0 f_i = a_n A^n f_i + \cdots + a_1 A f_i + a_0 f_i$
$= p(A) f_i \in \mathbb{Q}^3$. (Here $\mathbb{Q}^3$ is identified with $\mathbb{Q}f_1 \oplus \mathbb{Q}f_2 \oplus \mathbb{Q}f_3$ in R^3.) Then $R/K \cong \mathbb{Q}^3 / K \cap \mathbb{Q}^3 = \mathbb{Q}^3$ since $K \cap \mathbb{Q}^3 = 0$. It follows that $K = \ker(\varphi)$.

Thus $\ker(\varphi)$ is generated by r_1, r_2, r_3, and M has presentation matrix $\begin{bmatrix} x-3 & 3 & -4 \\ 0 & x-2 & -4 \\ 0 & -11 & x-2 \end{bmatrix}$. (Here we are writing elements of R^3 as column vectors.)

(d) We calculate: $A^0 e_1 = e_1$, $Ae_1 = 3e_1$, $A^2 e_1 = 9e_1$, etc., so $Re_1 = \mathbb{Q}e_1$. The map $R \longrightarrow Re_1$ has kernel $(x-3)$.
$A^0 e_2 = e_2$, $Ae_2 = 2e_2 + e_3$, $A^2 e_2 = 4e_2 + e_3$, $A^3 e_2 = 8e_2 + e_3$, etc. Then $Re_2 = \mathbb{Q}e_2 \oplus \mathbb{Q}e_3$. The map $R \longrightarrow Re_2$ has kernel $(x^2 - x - 2)$. (since $(A^2 - A^1 - 2A^0)e_2 = 0$).

(3) From the presentation we have $R^2 \xrightarrow{\beta} R \xrightarrow{\alpha} R/I \longrightarrow 0$ where $\alpha(1) = 1 + I$, $\beta(1,0) = x^2$, and $\beta(0,1) = xy$. Then $(p,q) \in \ker\beta \iff px^2 + qxy = 0 \iff px = -qy \iff p = -ry$ and $q = +rx$ for some r (since x and y are primes in R). So $\ker(\beta) = R(-y, x)$. Define $\gamma : R \longrightarrow R^2$ by $\gamma(1) = (-y, x)$. γ is injective because R^2 is torsionfree. Then
$0 \longrightarrow R \xrightarrow{\gamma} R^2 \xrightarrow{\beta} R \xrightarrow{\alpha} R/I \longrightarrow 0$ is a free resolution.

Note: The ring R is <u>graded by degree</u>, meaning $R = \bigoplus_{d \geq 0} R_d$ where R_d is the $\mathbb{k}$-module of polynomials that are homogeneous of degree d, and $R_{d_1} \cdot R_{d_2} \subseteq R_{d_1+d_2}$. The ideal $I = (x^2, xy)$ is generated by homogeneous polynomials, hence $R/I = M$ is a graded R-module ($M = \bigoplus_{d \geq 0} M_d$ with $R_{d_1} \cdot M_{d_2} \subseteq M_{d_1+d_2}$.)
α is homogeneous of degree 0: $\alpha(R_d) \subseteq M_d$.
Each entry of $\beta = [\beta_1 \ \beta_2]$ is homogeneous of degree two: $\beta_i(R_d) \subseteq R_{d+2}$ (e.g. $\beta_1(1) = x^2$, $\beta_2(1) = xy$).
And each component of $\gamma = \begin{bmatrix} -y \\ x \end{bmatrix}$ is homogeneous of degree 1. This is all reflected in the <u>graded</u> free resolution:

$$0 \longrightarrow R(-1) \xrightarrow{\phi} R(-2) \oplus R(-2) \xrightarrow{\beta} R \xrightarrow{\alpha} M \longrightarrow 0$$

Here $R(-2)$ is R with the grading shifted: $R(-2)_d = R_{d-2}$, so $1 \in R(-2)$ has degree 2; and similarly for $R(-1)$. This is done so that all the maps have degree 0.

(4) Suppose $r^n \in I$. Then $r^n A \subseteq Q$. Since $A \not\subseteq Q$, we may choose $a \in A$ with $a \notin Q$. Then $r^n a \in Q$. Since Q is primary, and $a \notin Q$, $r^n \in \sqrt{Q} = P$. Then $r \in \sqrt{P} = P$. Thus $\sqrt{I} \subseteq P$. Conversely, if $r \in P$, then $r^n \in Q$ for some $n \geq 1$. Then $r^n A \subseteq Q$ so $r^n \in I$, hence $r \in \sqrt{I}$. Thus $\sqrt{I} = P$. Suppose $xy \in I$ and $y \notin I$. Then $xyA \subseteq Q$. Since $y \notin I$, there exists $a \in A$ with $ya \notin Q$. Then, since $x(ya) \in Q$, $x \in \sqrt{Q}$. Then $x^n \in Q$ for some $n \geq 1$. Then $x^n A \subseteq Q$, so $x^n \in I$, and then $x \in \sqrt{I}$. This shows I is primary.

(5) Let $K = \mathrm{Fix}(\mathrm{Gal}(E,F))$. By the Galois correspondence, E is Galois over K. ($\mathrm{Fix}(\mathrm{Gal}(E,K)) = F$ $\mathrm{Fix}(\mathrm{Gal}(E, \mathrm{Fix}(\mathrm{Gal}(E,F)))) = \mathrm{Fix}(\mathrm{Gal}(E,F)) = K$)

Also, $\mathrm{Gal}(E,K) = \mathrm{Gal}(E,F)$; $\subseteq$ is automatic, and $\supseteq$ follows immediately from the definition of K. Then $|\mathrm{Gal}(E,F)| = |\mathrm{Gal}(E,K)| = |E:K|$ divides $|E:F|$ since $|E:F| = |E:K|\,|K:F|$.

(6) (a) $x^3 - 1 = (x-1)(x^2+x+1)$, and x^2+x+1 is irreducible by an example done in class. Then $m_\omega^{\mathbb{Q}}(x) = x^2+x+1$, and $|\mathbb{Q}[\omega]:\mathbb{Q}| = 2$.

(b) As in part (a), if $\omega = e^{2\pi i/p}$, then $m_\omega^{\mathbb{Q}}(x) = x^{p-1} + \cdots + x + 1$. Also, $x^p - q$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion and Gauss' Lemma, so, with $\alpha = \sqrt[p]{q}$, $m_\alpha^{\mathbb{Q}}(x) = x^p - q$. Since $\deg m_\omega^{\mathbb{Q}} = p-1$ and $\deg m_\alpha^{\mathbb{Q}} = p$ are relatively prime, $m_\omega^{\mathbb{Q}} = m_\omega^{\mathbb{Q}[\alpha]}$ by HW #6.2 Finally, $E = \mathbb{Q}[\alpha, \omega]$. Then $|E:\mathbb{Q}| = |E:\mathbb{Q}[\alpha]|\,|\mathbb{Q}[\alpha]:\mathbb{Q}|$ $= (p-1)p$.

(c) To construct a regular pentagon, it is enough to construct $\omega = e^{2\pi i/5}$. Since 5 is prime, the minimal polynomial of ω is $f(x) = x^4 + x^3 + x^2 + x + 1$. By HW # 7.2, $E = \mathbb{Q}[\omega]$ is Galois over $\mathbb{Q}$, and $Gal(E, \mathbb{Q}) \cong U(\mathbb{Z}_5)$; since 5 is prime, $U(\mathbb{Z}_5)$ is cyclic, of order 4. Then there are subgroups $1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 = Gal(E, \mathbb{Q})$ with $|H_1 : H_0| = |H_2 : H_1| = 2$. Let $K_i = Fix(H_i)$. Then $\mathbb{Q} = K_2 \subseteq K_1 \subseteq K_0 = E$ and $|K_1 : K_2| = |K_0 : K_1| = 2$. Since $\omega \in E$ it follows that ω is constructible.

(7) Let L be a splitting field for f over E, and let $\alpha \in L$ with $f(\alpha) = 0$. Since f is irreducible, $|F[\alpha] : F| = \deg(f) = p$. Since f is reducible over E, $|E[\alpha] : E| < p$. Then $|E[\alpha] : F| = |E[\alpha] : E|\,|E : F|$ and $|E[\alpha] : F| = |E[\alpha] : F[\alpha]|\,|F[\alpha] : F|$. Then $p = |F[\alpha] : F|$ divides $|E[\alpha] : E|\,|E : F|$. Since p is prime, and $|E[\alpha] : E| < p$, it follows that p divides $|E : F|$.