Math 101 Fall 2013
MidTerm
Due Friday, October 25, 2013

INSTRUCTIONS: You are allowed to use your lecture notes and a textbook of your choice (either Lang or one of the other texts on reserve). No other resources are allowed — animate or inanimate — with the one exception that you can ask me for clarification. Monitor the web page for corrections and typos.

If you are not using LaTeX, then use one side of the paper only and start each problem on a separate page.

Unless stated otherwise, R denotes a (possibly noncommutative) ring with identity. Ideal always means two-sided ideal.

1. (12) Let R be a PID. Let $\{r_1, \dots, r_k\} \subset R \setminus \{0\}$. We say that d is a $\gcd\{r_1, \dots, r_k\}$ if $d \mid r_i$ for all i and if $c \mid r_i$ for all i, then $c \mid d$. Similarly, we say m is a $\operatorname{lcm}\{r_1, \dots, r_k\}$ if $r_i \mid m$ for all i and if $r_i \mid c$ for all i then $m \mid c$. (When it exists, we call d "the" greatest common divisor and m "the" least common multiple. We'll assume it is clear that if d and m exist, then they are unique up to associates.)

(a) Show that $(r_1, \dots, r_k) = \gcd\{r_1, \dots, r_k\}$. In particular, gcd's always exist in PIDs.

(b) Similarly, show that $\operatorname{lcm}\{r_1, \dots, r_k\}$ exists.

(c) Prove that if $(a, b) = 1$ and if $a \mid bc$, then $a \mid c$.

(d) Let M be a torsion module over R such that $M = M_1 \oplus \cdots \oplus M_k$. Let the exponent of M_i be r_i. Show that the exponent of M is $\operatorname{lcm}\{r_1, \dots, r_k\}$.

ANS: (a) Let d be the generator of the ideal $(r_1, \dots, r_k)$. Then each r_i is a multiple of d and $d \mid r_i$ for all i. Moreover, there are elements s_i such that

$$d = s_1 r_1 + \cdots s_k r_k. \tag{1}$$

Therefore if $c \mid r_i$ for all i, then it follows from (1) that $c \mid d$. Hence d is the gcd as required.

(b) Let m be the generator of the ideal $(r_1) \cap \cdots \cap (r_k)$. Then $m \in (r_i)$, so $r_i \mid m$ for all i. Now suppose that $r_i \mid c$ for all i. Then $c \in (r_i)$ for all i. Hence $c \in (r_1) \cap \cdots \cap (r_k)$ and $m \mid c$ as required. Thus m is the lcm.

(c) Since a and b are relatively prime, there are $x, y \in R$ such that $xa + yb = 1$. But then $xac + ybc = c$. Since a divides both xac and ybc, it must divide c.

(d) Let $m = \operatorname{lcm}\{r_1, \dots, r_k\}$. Since $m \mid r_i$, $m \cdot M_i = \{0\}$. Hence $m \cdot M = \{0\}$. On the other hand, if $r \cdot M = \{0\}$, then $r \cdot M_i = \{0\}$ and $r \mid r_i$ for all i. Hence $m \mid r$ and m is the exponent of M.

2. (10) List the possible isomorphism classes of abelian groups of order $144 = 9 \times 16$. Show both the invariant factor decomposition and the elementary divisor decomposition for each class.

ANS: Viewed as a $\mathbf{Z}$-module, G is a torsion module who's exponent must divide $3^2 2^4$. I find it easier to start with the elementary divisors: there are two possibilities for the 3-primary bit and five for the 2-primary summand. Hence ten isomorphism classes. I'll list the elementary divisor decomposition on the left and its corresponding invariant factor decomposition on the right.

$$\begin{aligned}
\mathbf{Z}_9 \times \mathbf{Z}_{16} &\cong \mathbf{Z}_{144} \\
\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_{16} &\cong \mathbf{Z}_{48} \times \mathbf{Z}_3 \\
\mathbf{Z}_9 \times \mathbf{Z}_8 \times \mathbf{Z}_2 &\cong \mathbf{Z}_{72} \times \mathbf{Z}_2 \\
\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_8 \times \mathbf{Z}_2 &\cong \mathbf{Z}_{24} \times \mathbf{Z}_6 \\
\mathbf{Z}_9 \times \mathbf{Z}_4 \times \mathbf{Z}_4 &\cong \mathbf{Z}_{36} \times \mathbf{Z}_4 \\
\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_4 \times \mathbf{Z}_4 &\cong \mathbf{Z}_{12} \times \mathbf{Z}_{12} \\
\mathbf{Z}_9 \times \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_2 &\cong \mathbf{Z}_{36} \times \mathbf{Z}_2 \times \mathbf{Z}_2 \\
\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_2 &\cong \mathbf{Z}_{12} \times \mathbf{Z}_6 \times \mathbf{Z}_2 \\
\mathbf{Z}_9 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 &\cong \mathbf{Z}_{18} \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \\
\mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 &\cong \mathbf{Z}_6 \times \mathbf{Z}_6 \times \mathbf{Z}_2 \times \mathbf{Z}_2.
\end{aligned}$$

3. (10) Let $V = V_1 \oplus \cdots \oplus V_r$ be a decomposition of a vector space over a field F into a direct sum of subspaces. Let β_i be a basis for each V_i. Show that $\beta = \bigcup_i \beta_i$ is a basis for V.

ANS: First, I claim that if $v_i \in V_i$ and $0 = v_1 + \cdots + v_r$, then each $v_i = 0$. But if $0 = v_1 + \cdots + v_r$, then $v_i = \sum_{j \neq i} v_j$. Then $v_i \in V_i \cap \bigcap_{j \neq i} V_j = \{0\}$. Hence $v_i = 0$. This proves the claim.

Since every element if v is a sum $v_1 + \cdots + v_k$ with $v_i \in V_i$ and β_i spans V_i, it is clear that β spans V. We just have to show that β is linearly independent. Let $\{w_1, \dots, w_r\}$ be a finite subset of β such that there are scalars r_i such that $r_1 \cdot w_1 + \cdots + r_s \cdot w_s = 0$. But then

$$0 = \sum_{i=1}^{r} \Bigl(\sum_{w_k \in \beta_i} r_k \cdot w_k \Bigr).$$

Since $\sum_{w_k \in \beta_i} r_k \cdot w_k \in V_i$ and since β_i is a basis V_i, we must have $\sum_{w_k \in \beta_i} r_k \cdot w_k = 0$ by the claim. But then $r_k = 0$ for all r_k such that $w_k \in \beta_i$. But then all the r_k are zero. This shows that β is linearly independent as required.

4. (20) Find all rational and Jordan canonical forms of a matrix A in $M_5(\mathbf{C})$ with minimal polynomial $m_A(x) = x^2(x-2)$. Be sure to give the corresponding invariants and the characteristic polynomial $c_A(x)$.

ANS: Since $c_A(x)$ must have degree 5, be divisible by $m_A(x)$ and must factor into linear factors consisting of both x and $x-2$, there are three possibilities for the characteristic polynomial: (I) $x^4(x-2)$, (II) $x^3(x+1)^2$ and (III) $x^2(x-2)^3$.

Case (I): Here the possible invariant factor decompositions are $\{x^2(x-2), x^2\}$ and $\{x^2(x-2), x, x\}$. Since $x^2(x-2) = x^3 - 2x^2$, the companion matrix of m_A is

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}.$$

The companion matrix of x^2 is

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Hence corresponding rational canonical forms, R_A, rational Jordan forms, J_A are given, respectively, by the 5×5 matrices

$$R_A = \begin{bmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix} & 0 \\ 0 & \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \end{bmatrix} \qquad J_A = \begin{bmatrix} (2) & 0 & 0 \\ 0 & \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} & 0 \\ 0 & 0 & \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \end{bmatrix}$$

in the case the invariant factors are $\{x^2(x-2), x^2\}$ and the elementary divisors by $\{x-2, x^2, x^2\}$. In the case the invariant factors are $\{x^2(x+1), x, x\}$, then elementary divisors are $\{x-2, x^2, x, x\}$. In the case,

$$R_A = \begin{bmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix} & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad J_A = \begin{bmatrix} 2 & 0 & 0 \\ 0 & \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Case II: Here the invariant factors must be $\{x^2(x-2), x(x-2)\} = \{x^3 - 2x^2, x^2 - 2x\}$ with elementary divisors $\{(x-2), (x-2), x^2, x\}$. Then

$$R_A = \begin{bmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix} & 0 \\ 0 & \begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix} \end{bmatrix} \quad \text{and} \quad J_A = \begin{bmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} & \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix} \\ \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{matrix} \end{bmatrix}$$

Case III: In this case, the invariant factors must be $\{x^2(x-2), x-2, x-2\}$ with elementary divisors $\{\, x-2, x-2, x-2, x^2 \,\}$. Hence

$$R_A = \begin{bmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix} & \begin{matrix} 0 & 0 \end{matrix} \\ \begin{matrix} 0 \\ 0 \end{matrix} & \begin{matrix} 2 & 0 \\ 0 & 2 \end{matrix} \end{bmatrix} \quad \text{and} \quad J_A = \begin{bmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} & \begin{matrix} 0 & 0 & 0 \end{matrix} \\ \begin{matrix} 0 \\ 0 \\ 0 \end{matrix} & \begin{matrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{matrix} \end{bmatrix}$$

5. (20) Let $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{\pi} M'' \longrightarrow 0$ be a short exact sequence of R-modules.

(a) If M' and M'' are finitely generated, must M be finitely generated?

(b) If M is finitely generated, must M' or M'' be finitely generated?

(c) If M' and M'' are free, must M be free?

(d) If M is free, must M' or M'' be free? What if R is a PID?

ANS: (a) Yes. Let $\{m''_1, \dots, m''_k\}$ be generators for M'' and $\{m'_1, \dots, m'_l\}$ be generators for M'. Let m_i be such that $\pi(m_i) = m''_i$. Then I claim $\{i(m'_1), \dots, i(m'_l), m_1, \dots, m_k\}$ generate M. Let $m \in M$. There are r_i such that $\pi(m) = r_1 \cdot m''_1 + \cdots + r_k \cdot m''_k$. Them $m - (r_1 \cdot m_1 + \cdots r_k \cdot m_k)$ is in the kernel of π. Hence there are s_i such that $i(s_1 \cdot m'_1 + \cdots + s_l \cdot m'_l) = m - (r_1 \cdot m_1 + \cdots r_k \cdot m_k)$. But then $m = r_1 \cdot m_1 + \cdots r_k \cdot m_k + s_1 \cdot i(m'_1) + \cdots s_l \cdot i(m_l)$.

(b) As we saw on homework, submodules of finitely generated modules need not be finitely generated. So M' need not be finitely generated. However the image of any generating set in M is clearly a generating set for M'', so M'' must be finitely generated.

(c) Yes. If M'' is free then it is projective and the identity map $\mathrm{id}_{M''} : M'' \to M''$ must lift to a map $s : M'' \to M$ such that $\pi \circ s = \mathrm{id}_{M''}$. That is, π must have a section and $M \cong M' \oplus M''$. It is simple matter to see that the direct sum of free modules is free: for example, let B' be a basis for M' and B'' a basis for M''. Then as in problem 3, $B = B' \oplus B''$ is a basis for M (with an appropriate interpretation of $B' \oplus B''$).

(d) Every module is the surjective image of a free module, so M'' need not be free — whether or not R is a PID. If R is not a PID, then we saw in lecture that submodules of finitely generated modules need not be finitely generated. Hence M' need not be finitely generated in general. (Examples include $\mathbf{Z}_2$ viewed as a ideal (and hence a submodule) of $\mathbf{Z}_4$ over itself. Also we saw that the ideal $(s, x) \subset \mathbf{Z}[x]$ was not free over $\mathbf{Z}[x]$.) But if R is a PID, then we proved that submodules of free modules are always free. So in this case, M' would be finitely generated too.

6. (16) Let V be a finite-dimensional real vector space and $T \in \hom_{\mathbf{R}}(V, V)$ a linear transformation such that $T^2 = -I$. Show that the dimension of V must be even, say equal to $2r$, and that there is a basis β for V such that

$$[T]_\beta^\beta = \begin{pmatrix} 0 & -I_r \\ I_r & 0 \end{pmatrix}$$

where, of course, I_r is the $r \times r$-identity matrix.

ANS: Clearly $p(x) = x^2 + 1$ annihilates T. Since $p(x)$ is irreducible over $\mathbf{R}$, it must be the minimal polynomial. Hence the characteristic polynomial must be of the form $c_T(x) = (x^2 + 1)^r$ for $r \geq 1$. Then $\dim V = 2r$ and $\dim V$ is even as claimed. Furthermore the only possible invariant factor decomposition of V_T is $\{x^2+1,\dots,x^2+1\}$. Hence there is a basis $\alpha = \{v_1, w_1, v_2, w_2, \dots, v_r, w_r\}$ such that

$$[T]^\alpha_\alpha = \begin{bmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} & 0 & 0 & 0 \\ 0 & \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \end{bmatrix}$$

is the rational canonical form of T. Let $\beta = \{v_1, \dots, v_r, w_1, \dots w_r\}$. Then since $T(v_i) = w_i$ and $T(w_i) = -v_i$, $[T]^\beta_\beta$ has the required form.

7. (12) An ideal I in a ring R is called nilpotent if $I^n = \{0\}$ for some n. (For example, consider $p\mathbf{Z}/p^k\mathbf{Z}$ in $\mathbf{Z}/p^k\mathbf{Z}$.) Show that if I is a nilpotent ideal in R and if $\phi : M \to N$ is an R-module map such that the induced map $\bar{\phi} : M/(I \cdot M) \to N/(I \cdot N)$ is surjective, then ϕ is surjective.

ANS: We start with a little lemma (which does not require I to be nilpotent). Note that if J is any ideal in R, then $\phi(J \cdot M) \subset J \cdot N$ and we get an induced map $\bar{\phi}_J : M/J \cdot M \to N/J \cdot N$.

Lemma. *Suppose that M and N are R modules and I an ideal in R. Let $\phi : M \to N$ be a module map such that the induced map $\bar{\phi}_{I^k} : M/I^k \cdot M \to N/I^k \cdot N$ is surjective. Then the induced map $\bar{\phi}_{I^{k+1}} : M/I^{k+1} \cdot M \to I^{k+1} \cdot N$ is surjective.*

Proof of Lemma. Let $n \in N$. Then by assumption there is a $m \in M$ such that $\phi(m) + I^k \cdot N = n + I^k \cdot N$. Hence we have $r_i \in I^k$ and $n_i \in N$ such that

$$\phi(m) - n = r_1 \cdot n_1 + \cdots r_l \cdot n_l.$$

Similarly, there are $m_i \in M$ such that $\phi(m_i) - n_i \in I^k \cdot N$. But then $\phi(r_i \cdot m_i) - r_i \cdot n_i \in I^{k+1} \cdot N$. Then

$$\phi(m + r_1 \cdot m_1 + \cdots + r_l \cdot m_l) - n = \sum_i \phi(r_i \cdot m_i) - r_i \cdot n_i \in I^{k+1} \cdot N.$$

Thus $\bar{\phi}_{I^{k+1}}(m + \sum_i r_i \cdot m_i + I^{k+1} \cdot M) = n + I^{k+1} \cdot N$, and $\bar{\phi}_{I^{k+1}}$ is surjective. $\square$

Since we are given that $\bar{\phi}_I$ is surjective, and induction argument implies that $\bar{\phi}_{I^k}$ is surjective for all k. But if I is nilpotent, then $\bar{\phi}_{I^n} = \phi$ for large n. This completes the proof.