MA251 - Algebra I

Assignment 5 **Autumn 2016**

Answer the questions on your own paper. Write your own name in the top left-hand corner, and your university ID number in the top right-hand corner. Use the problems at the beginning as well as exercises in the lecture notes for a warm up. Solutions to the **FOUR TEST** *problems must be handed in by* **15.00** *on* **MONDAY 5 DECEMBER** *(Monday of the tenth week of term), or they will not be marked. There will be an award of 5 extra marks for clarity, so do a good job.*

These are practice problems for you to sharpen your teeth on.

P1. Prove that elements $x_1, \dots, x_r \in \mathbb{Z}^n$ are linearly independent if and only if they are linearly independent over $\mathbb{Q}$ when regarded as vectors in $\mathbb{Q}^n$.

P2. Write down the possible isomorphism types of abelian groups of orders up to 16.

P3. Let n be a positive integer. Show that there are $2^n - 1$ surjective homomorphisms from $\mathbb{Z}^n$ to $\mathbb{Z}_2$, and use the First Isomorphism Theorem to deduce that there are exactly $2^n - 1$ subgroups of $\mathbb{Z}^n$ of index 2. How many subgroups of index 3 are there?

P4. Show that the Smith Normal Form of a unimodular matrix with entries in $\mathbb{Z}$ is the identity matrix. Deduce that any such unimodular matrix can be expressed as the product of elementary unimodular matrices.

P5. Find all subgroups of the groups $\mathbb{Z}_{15}$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_4$. (The former has 4 and the latter has 8.) Express each subgroup as a direct sum of cyclic groups.

P6. Proof of the uniqueness of the Smith Normal Form. Let $A \in \mathbb{Z}^{m\times n}$ be an $m \times n$ matrix with entries in $\mathbb{Z}$. For $1 \le i \le \min(m, n)$, an $i \times i$-submatrix of A is defined to be a matrix obtained from A by deleting any $m - i$ rows and any $n - i$ columns of A. Define $\gamma_i(A) = \gcd(\{|\det(S)|\ ;\ S \text{ is an } i \times i - \text{submatrix of } A\})$. (The convention here is that $\gcd(0, n) = n$ for any $n \ge 0$.)

(i) Show that, if B is obtained from A by applying elementary unimodular row and column operations, then $\gamma_i(B) = \gamma_i(A)$ for $1 \le i \le \min(m, n)$. (This is easy for (UR2), (UR3), but a little harder for (UR1).)

(ii) Show that, if B is Smith Normal Form with nonzero diagonal entries $\alpha_1, \dots, \alpha_r$, then $\gamma_i(B) = \alpha_1\alpha_2 \cdots \alpha_i$ for $1 \le i \le r$ and $\gamma_i(B) = 0$ for all $i > r$.

(iii) Deduce that the Smith Normal Form is uniquely determined by A.

P7. Let H be the subgroup of $\mathbb{Z}^n$ generated by the columns of a matrix $A \in \mathbb{Z}^{n\times n}$, invertible in $\mathbb{Q}^{n\times n}$. Prove that the index of H in $\mathbb{Z}^n$ is equal to $|\det(A)|$.

Compute the index of $\langle (2, 1, 1)^T, (1, 2, 1)^T, (1, 1, 2)^T \rangle$ in $\mathbb{Z}^3$.

P8. A group is a set with a binary operation that satisfies all axioms of an abelian group except commutativity. Homomorphism between groups is a function f satisfying $f(x+y) = f(x)+f(y)$.

(i) Prove that a group G is abelian if and only if $f : G \to G$ defined by $f(x) = 2x$ is a group homomorphism.

(ii) Prove that if a group G satisfies the property that $2g = 0$ for all $g \in G$ then G is abelian.

P9. Prove that if $x_1, \dots, x_n$ span $\mathbb{Z}^n$ then they are a basis of $\mathbb{Z}^n$.

P10. We consider finite-dimensional complex vector spaces U and V, their bases $\mathbf{e}_i \in U$, $i = 1, 2, \dots, n$ and $\mathbf{f}_i \in V$, $i = 1, 2, \dots, m$, their dual spaces U^* and V^*, and the dual bases $\mathbf{e}^i$ and $\mathbf{f}^i$.

(i) Let $T : U \to V$ be a linear map. We consider a function $T^\star : V^* \to U^*$ so that for each $\alpha \in V^*$, $T^\star(\alpha)$ is an element of U^* defined by $T^\star(\alpha)\ (\mathbf{u}) = \alpha(T(\mathbf{u}))$ for all $\mathbf{u} \in U$. Prove that $T^\star$ is a linear map.

The linear map $T^\star$ in (i) is called *the dual linear map* of T.

(ii) Suppose A is the matrix of T and B is the matrix of $T^\star$ in the bases described above. Prove that $B = A^T$.

(iii) Now we assume that both vector spaces are Hermitian. As in the Problem 4, HW-3 we consider $T_U : U \to U^*$ defined by $T_U(\mathbf{w})(\mathbf{u}) = \langle \mathbf{w}, \mathbf{u} \rangle$ for all $\mathbf{w}, \mathbf{u} \in U$. Prove that if the basis $\mathbf{e}_i$ is orthonormal them $T_U(\mathbf{e}_i) = \mathbf{e}^i$.

It follows from (iii) that T_U is a semilinear[1] bijection between U and U^*. Hence, we can use its inverse in the following part (iv).

(iv) Two linear maps $T\colon U \to V$ and $S\colon V \to U$ are *formally dual* if $\langle T(\mathbf{u}), \mathbf{v}\rangle = \langle \mathbf{u}, S(\mathbf{v})\rangle$ for all $\mathbf{v} \in V,\ \mathbf{u} \in U$. Prove that the linear[2] maps T and $T_U^{-1}T^{\star}T_V$ are formally dual. (*Hint*: Compute the matrices of both sesquilinear maps $U \times V \to \mathbb{C}$ in a pair of orthonormal bases.)

P11. For the following finitely generated abelian groups G, write down their corresponding matrix, reduce it to Smith Normal Form, and hence express G as a direct sum of cyclic groups:

(i) $\langle x_1, x_2, x_3 \mid x_1 - 2x_2, x_1 + 6x_2 + 8x_3, x_1 + 3x_3\rangle$;

(ii) $\langle x_1, x_2 \mid 6x_1 - 6x_2, -6x_1 - 12x_2, 4x_1 - 8x_2\rangle$.

The following problems are test problems for you to submit for marking, unless there's 0 marks for them. Write concise but complete solutions only to the questions asked. Additional 5 marks are awarded for clarity.

1. Write down the possible isomorphism types of abelian groups of orders 74 and 800. You may use any theorems from the lectures if you state them. [3 marks]

2. Recall that a $\mathbb{Z}$-module is an abelian group $(G, +)$ together with a map $\mathbb{Z}\times G \to G\colon (a, x) \mapsto ax$ (called scalar multiplication) such that

(a)	$a(x + y) = ax + ay$	for all $a \in \mathbb{Z},\ x, y \in G$;
(b)	$(a + b)x = ax + bx$	for all $a, b \in \mathbb{Z},\ x \in G$;
(c)	$(ab)x = a(bx)$	for all $a, b \in \mathbb{Z},\ x \in G$;
(d)	$1x = x$	for all $x \in G$.

(i) Let $(G, +)$ be an abelian group. Prove that there is *at most one* scalar multiplication $\mathbb{Z} \times G \to G\colon (a, x) \mapsto ax$ making it into a $\mathbb{Z}$-module. (*At least one* is harder and was partially proved in the lectures.) [1 mark]

(ii) Let $(G, +)$ be an abelian group. Prove that (a),(b),(d) imply (c). Don't use any consequences of (a),(b),(d) unless you prove them. You may use anything about abelian groups. [2 marks]

3. Find the $\mathbb{Z}$-Smith Normal Form of $A = \begin{pmatrix} 4 & 2 & 4 \\ 3 & 3 & 4 \\ 2 & 2 & 2 \end{pmatrix}$. You don't need to give all row or column operations to arrive at the $\mathbb{Z}$SNM but you should give enough calculations to conclude what the $\mathbb{Z}$SNM is. [2 marks]

4. Assume $G \cong H$ are isomorphic abelian groups where

$$G = \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_k, \qquad H = \mathbb{Z}/e_1 \times \cdots \times \mathbb{Z}/e_k$$

and $d_i, e_i \in \mathbb{Z}_{\geq 0}$ for all i, and $d_i | d_{i+1}$ and $e_i | e_{i+1}$ for all i. You will prove that $d_i = e_i$ for all i. For an abelian group $(G, +)$ write $G[m] = \{x \in G \mid mx = 0\}$ and $mG = \{mx \mid x \in G\}$.

(i) Let $m, n \geq 1$ have greatest common divisor d. Prove: $(\mathbb{Z}/n)[m] \cong \mathbb{Z}/d$. [0 marks]

(ii) Assume $d_k \neq 0$ and $e_k \neq 0$. Let $m \geq 1$. Prove that $\#G[m] \leq m^k$ and that equality holds if and only if $m | d_1$. [1 mark]

(iii) [Continued from (ii).] Prove $d_i = e_i$ for all i. Hint: Clearly $G/G[d_1] \cong H/H[d_1]$. [3 marks]

(iv) Let $m, n \geq 0$ be such that $\mathbb{Z}^m \cong \mathbb{Z}^n$. Prove $m = n$. Hint: Write $P = \mathbb{Z}^m$, $Q = \mathbb{Z}^n$ and consider $P/2P$ and $Q/2Q$. [2 mark]

(v) We now drop the assumptions $d_k \neq 0$ and $e_k \neq 0$. Prove $d_i = e_i$ for all i. [0 marks]

5. Let G be an abelian group and let $g, h \in G$.

(i) If $|g| = m$ is finite then prove that, for $n \in \mathbb{Z}, ng = 0$ if and only if $m|n$. [2 marks]

(ii) Let us assume that $|g|$ and $|h|$ are both finite, with $\mathrm{hcf}(|g|, |h|) = 1$. Prove that $|g + h| = |g||h|$. [2 marks]

(iii) Prove that $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if m and n are relatively prime. [2 marks]

---

[1] $T_U(\alpha\mathbf{v}) = \bar{\alpha}T_U(\mathbf{v})$ rather then $\alpha T_U(\mathbf{v})$

[2] Composition of anti-linear maps is linear - you don't have to show that the maps are linear or well-defined.