MA251 - Algebra I

Assignment 5 **Autumn 2013**

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 2 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 $x_1, \ldots, x_r \in \mathbb{Z}^n$ 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 $\alpha_1, \ldots, \alpha_r$, 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 $\mathbb{Z}^{n\times n}$. Prove that the index of H in $\mathbb{Z}^3$ is equal to $|\det(A)|$.

Compute the index of $< (2, 1, 1)^T, (1, 2, 1)^T, (1, 1, 2)^T >$ 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 $f\colon G \to G$ defined by $f(x) = 2x$ is a group homomorphism.

(ii) Prove that if a group G satisfies the property that $2g = 1$ for all $g \in G$ then G is abelian.

The following problems are test problems for you to submit for marking. 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. [3 marks]

2. 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) $\langle x_1, x_2, x_3 \mid x_1 - 2x_2, x_1 + 6x_2 + 8x_3, x_1 + 3x_3 \rangle$; [2 marks]

(ii) $\langle x_1, x_2 \mid 6x_1 - 6x_2, -6x_1 - 12x_2, 4x_1 - 8x_2 \rangle$. [2 marks]

3. 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 $m \mid n$. [2 marks]

(ii) Let us assume that $|g|$ and $|h|$ are both finite, with $\text{hcf}(|g|, |h|) = 1$. 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]

4. We consider finite dimensional vector spaces U and V over complex numbers $\mathbb{C}$, their bases $\mathbf{e}_i \in U$, $i = 1, 2, \ldots, n$ and $\mathbf{f}_i \in V$, $i = 1, 2, \ldots, m$, 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

$$T^\star(\alpha)\ (\mathbf{u}) = \alpha(T(\mathbf{u})) \text{ for all } \mathbf{u} \in U.$$

Prove that $T^\star$ is a linear map. [2 marks]

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 $B = A^T$. [2 marks]

(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

$$T_U(\mathbf{w})(\mathbf{u}) = <\mathbf{w}, \mathbf{u}> \text{ for all } \mathbf{w}, \mathbf{u} \in U.$$

Prove that if the basis $\mathbf{e}_i$ is orthonormal them $T_U(\mathbf{e}_i) = \mathbf{e}^i$. [1 marks]

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

(iv) Two linear maps $T: U \to V$ and $S: V \to U$ are *formally dual* if

$$< T(\mathbf{u}), \mathbf{v} > = < \mathbf{u}, S(\mathbf{v}) > \text{ for all } \mathbf{v} \in V,\ \mathbf{u} \in U.$$

Prove that the linear[2] maps T and $T_U^{-1} T^\star T_V$ are formally dual. [2 marks]

(*Hint*: Compute the matrices of both sesquilinear maps $U \times V \to \mathbb{C}$ in a pair of orthonormal bases.)

---

[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