

MA251 - Algebra I

Assignment 4

November 2009

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 30 NOVEMBER** (Monday of the ninth 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. Let A be a symmetric $n \times n$ real matrix. We consider a function $f : S \rightarrow \mathbb{R}$ where $f(\mathbf{v}) = \mathbf{v}^T A \mathbf{v}$ and $S = \{\mathbf{v} \in \mathbb{R}^n \mid \mathbf{v}^T \mathbf{v} = 1\}$ is the unit sphere. The set S is compact and the function f is continuous. It is known in Analysis (Extreme Value Theorem or Weierstrass' Theorem) that there exists a point $\mathbf{v}_0 \in S$ such that $f(\mathbf{v})$ achieves its maximum at $\mathbf{v} = \mathbf{v}_0$. Prove that \mathbf{v}_0 is an eigenvector of A .

(Note: This is another proof of the fact that a symmetric matrix admits a real eigenvector, using methods of Analysis)

P3. 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 .

P4. 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) $\langle x_1, x_2, x_3 \mid x_1 - 2x_2, x_1 + 6x_2 + 8x_3 \rangle$;

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

P5. Write down the possible isomorphism types of abelian groups of orders 74, 147, 666, 800 and 1221.

P6. 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.

P7. Find all subgroups of the group $\mathbb{Z}_2 \oplus \mathbb{Z}_4$. (There are eight altogether.) Express each subgroup as a direct sum of cyclic groups.

P8. 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 $1 \leq i \leq \min(m, n)$, 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

$$\gamma_i(A) = \gcd(\{|\det(S)| \mid S \text{ is an } i \times i \text{-submatrix of } A\}).$$

(The convention here is that $\gcd(0, n) = n$ for any $n \geq 0$.)

(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 $1 \leq i \leq \min(m, n)$. (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 $\gamma_i(B) = \alpha_1 \alpha_2 \dots \alpha_i$ for $1 \leq i \leq r$ and $\gamma_i(B) = 0$ for all $i > r$.

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

P9. 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 $f : G \rightarrow G$ 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. (i) Find the orders of all elements in the group \mathbb{Z}_{12} . [1 mark]

(ii) Write down and prove a formula for the order of an element $k \in \mathbb{Z}_n$ for general n and k . [2 marks]

2. 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 $\text{hcf}(|g|, |h|) = 1$. Prove that $|g + h| = |g||h|$. [2 marks]

(iv) 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]

3. We are working with a finite dimensional Euclidean space (V, \langle, \rangle) . Given vectors $\mathbf{v}_1, \dots, \mathbf{v}_n \in V$, one defines the parallelepiped

$$P(\mathbf{v}_1, \dots, \mathbf{v}_n) = \left\{ \sum \alpha_i \mathbf{v}_i \in V \mid \alpha_i \in [0, 1] \right\}.$$

The n -dimensional volume of this parallelepiped is defined inductively:

$$\text{Vol}_1(P(\mathbf{v}_1)) = \|\mathbf{v}_1\| = \sqrt{\langle \mathbf{v}_1, \mathbf{v}_1 \rangle}, \quad \text{Vol}_n(P(\mathbf{v}_1, \dots, \mathbf{v}_n)) = \text{Vol}_{n-1}(P(\mathbf{v}_1, \dots, \mathbf{v}_{n-1})) \|\mathbf{w}\|$$

where $\mathbf{w} = \mathbf{v}_n + \alpha_1 \mathbf{v}_1 + \dots + \alpha_{n-1} \mathbf{v}_{n-1}$ is the unique¹ vector of this form orthogonal to all \mathbf{v}_i for $i \leq n - 1$. Intuitively, we define the n -dimensional volume as a product of the $n - 1$ -dimensional volume of a base and the height. There is nothing to prove at this point.

(i) Using the Gram matrix from HW-3, prove that

$$\det(G(\mathbf{v}_1, \dots, \mathbf{v}_n)) = \text{Vol}_n(P(\mathbf{v}_1, \dots, \mathbf{v}_n))^2.$$

[2 marks]

(ii) Now let n be the dimension of V . Let A be a square matrix whose columns are $\underline{\mathbf{v}}_i$, the coordinate vectors of \mathbf{v}_i in some orthonormal basis. Using part (i), prove that

$$|\det(A)| = \text{Vol}_n(P(\mathbf{v}_1, \dots, \mathbf{v}_n)).$$

[2 marks]

¹This follows from the direct sum decomposition $V = W \oplus W^\perp$ where W is the span of the first $n - 1$ vectors. Then $\mathbf{w} = \pi(\mathbf{v}_n)$ where $\pi : V \rightarrow W^\perp$ is the projection map along W .

4. We consider finite dimensional vector spaces U and V over complex numbers \mathbb{C} , their bases $\mathbf{e}_i \in U, i = 1, 2 \dots n$ 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 $T : U \rightarrow V$ be a linear map. We consider a function $T^* : V^* \rightarrow U^*$ so that for each $\alpha \in V^*, T^*(\alpha)$ is an element of U^* defined by

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

Prove that T^* is a linear map. [2 marks]

The linear map T^* 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^* 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 2, HW-1 we consider $T_U : U \rightarrow U^*$ defined by

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

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

It follows from (iii) that T_U is an anti-linear² bijection between U and U^* . Hence, we can write its inverse in the following part (iv).

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

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

Prove that the linear³ maps T and $T_U^{-1}T^*T_V$ are formally dual. [2 marks]

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

² $T_U(\alpha\mathbf{v}) = \bar{\alpha}T_U(\mathbf{v})$ rather than $\alpha T_U(\mathbf{v})$

³Composition of anti-linear maps is linear - you don't have to show that the maps are linear or well-defined