Matematiikan ja tilastotieteen laitos
Transformation Groups
Spring 2012
Exercise 2
Solutions

1. Suppose $A = (a_{ij})$ is a real $n \times m$ matrix. Recall that its **transpose** A^T is defined as an $m \times n$ matrix with $(A^T)_{ij} = a_{ji}$. Also recall that the standard inner product $\cdot$ in $\mathbb{R}^n$ is defined by

$$x \cdot y = \sum_{i=1}^{n} x_i y_i,$$

$x, y \in \mathbb{R}^n$.
a) Suppose A is an $n \times m$ matrix as above. Prove that

$$Ax \cdot y = x \cdot A^T y$$

for all $x \in \mathbb{R}^m, y \in \mathbb{R}^n$.
b) Prove that the equation above characterises A^T uniquely, i.e. if B is an $m \times n$ matrix such that

$$Ax \cdot y = x \cdot By$$

for all $x \in \mathbb{R}^m, y \in \mathbb{R}^n$, then $B = A^T$.

Solution: a) If A is $n \times m$ matrix and $x = (x_1, \ldots, x_m) \in \mathbb{R}^m$, then $Ax = (y_1, \ldots y_n) \in \mathbb{R}^n$, where

$$y_i = \sum_{j=1}^{m} a_{ij} x_j.$$

Hence it follows also that $A^T y = (z_1, \ldots, z_m)$, where

$$z_j = \sum_{i=1}^{n} a_{ij} y_i.$$

Now

$$Ax \cdot y = \sum_{i=1}^{n} (Ax)_i y_i = \sum_{i=1}^{n} (\sum_{j=1}^{m} a_{ij} x_j) y_i = \sum_{j=1}^{m} (\sum_{i=1}^{n} a_{ij} y_i) x_j = x \cdot A^T(y).$$

b) Let us first the following general observations, that we will also use later. Suppose $z \in \mathbb{R}^n$ an element with the property

$$x \cdot z = 0 \text{ for all } x \in \mathbb{R}^n.$$

Then $z = 0$. Indeed for $x = z$ we then have $|z|^2 = z \cdot z = 0$, so $z = 0$.

Now suppose B is an $m \times n$ matrix such that

$$Ax \cdot y = x \cdot By$$

for all $x \in \mathbb{R}^m, y \in \mathbb{R}^n$. By a) This implies that

$$x \cdot By = x \cdot A^T y$$

for all $x \in \mathbb{R}^m, y \in \mathbb{R}^n$, which can also be written as

$$x \cdot (By - A^T y)$$

for all $x \in \mathbb{R}^m, y \in \mathbb{R}^n$. Fix $y \in \mathbb{R}^n$ and let $z = By - A^T y$. Then $x \cdot z = 0$ for all $x \in \mathbb{R}^m$. By the observation above it follows that $z = 0$ i.e. $By = A^T y$. Since this is true for any $y \in \mathbb{R}^n$ it follows that $B = A^T$.

2. Suppose A is an $n \times n$ matrix. Prove that the following conditions are equivalent:
1) A is orthogonal i.e. $A^T A = I = AA^T$.
2) A preserves standard inner product in $\mathbb{R}^n$ i.e.

$$Ax \cdot Ay = x \cdot y$$

for all $x, y \in \mathbb{R}^n$.
3) A preserves standard norm in $\mathbb{R}^n$ i.e.

$$|Ax| = |x|$$

for all $x \in \mathbb{R}^n$. (Recall that $|x| = \sqrt{x \cdot x}$).
Also prove that if A is orthogonal, then $\det A = \pm 1$.

Solution: Suppose A is an arbitrary $n \times n$ matrix. Then by exercise 1)

$$Ax \cdot Ay = x \cdot A^T Ay$$

for all $x, y \in \mathbb{R}^n$. In particular

$$Ax \cdot Ay = x \cdot y$$

for all $x, y \in \mathbb{R}^n$ if and only if

$$x \cdot A^T Ay = x \cdot y$$

for all $x, y \in \mathbb{R}^n$. This is true if and only if

$$x \cdot (A^T Ay - y)$$

for all $x, y \in \mathbb{R}^n$. By the observations made above this is equivalent to $A^T Ay - y = 0$ for all $y \in \mathbb{R}^n$, which in turn is equivalent to $A^T A = I$.
Hence we have proved that the condition 2) is equivalent to condition $A^T A = I$. On the other hand in Linear Algebra it is proved that for square matrices A, B condition $AB = I$ implies $BA = I$ (for dimensional reasons). Hence condition 1) is equivalent to condition $A^T A = I$. We have shown the equivalences of conditions 1) and 2).

Let us prove that 2) and 3) are equivalent. Suppose A preserves inner product. Then for every $x \in \mathbb{R}^n$ we have

$$|Ax|^2 = Ax \cdot Ax = x \cdot x = |x|^2,$$

so $|Ax| = |x|$, since both are non-negative real numbers. Conversely suppose A preserves norms. Then

$$Ax \cdot Ax = x \cdot x$$

for all $x \in \mathbb{R}^n$. Apply this to the vector $x + y$, to obtain

$$Ax \cdot Ax + 2Ax \cdot Ay + Ay \cdot Ay = A(x+y) \cdot A(x+y) = (x+y) \cdot (x+y) = x \cdot x + 2x \cdot y + y \cdot y.$$

Since $Ax \cdot Ax = x \cdot x$ and $Ay \cdot Ay = y \cdot y$, these cancel out, to leave us with

$$2Ax \cdot Ay = 2x \cdot y, \text{ i.e.}$$

$$Ax \cdot Ay = x \cdot y.$$

Suppose A is orthogonal. Then $A^T A = I$, and using properties of integral we get

$$(\det A)^2 = \det A \det A = \det A^T \det A = \det(A^T A) = \det I = 1.$$

Hence $\det A = \pm 1$.

3. a) Prove that

$$O(n) = \{A \in M(n \times n, \mathbb{R}) \mid A^T A = I = AA^T\}$$

considered as a subgroup of $GL(n, \mathbb{R})$ is a compact topological group (Hint: a subset of $\mathbb{R}^m$ is compact if and only if it is closed and bounded).
b) We have proved in the lectures that

$$SL(n) = \{A \in M(n \times n, \mathbb{R}) \mid \det A = 1\}$$

is a closed subgroup of $GL(n, \mathbb{R})$. Is it compact?

Solution: a)Since $O(n)$ is a subspace of $M(n; \mathbb{R})$, which is homeomorphic to Euclidean space $\mathbb{R}^{n^2}$, it is enough to show $O(n)$ is closed and bounded in $M(n; \mathbb{R})$.
Consider the mapping $\phi \colon M(n; \mathbb{R}) \to M(n; \mathbb{R})$ defined by $\phi(A) = A^T A$. This mapping is clearly continuous, since taking transpose and multiplication of matrices are continuous operations. $>$We have

$$O(n) = \phi^{-1}(\{I\}).$$

Since singleton $\{I\}$ is closed in $M(n; \mathbb{R})$, $O(n)$ is closed in $M(n; \mathbb{R})$.

By the previous exercise orthogonal matrix A preserves norm, so in particular $|Ae_j| = 1$, where e_j is the j-th vector in the standard orthonormal basis of $\mathbb{R}^n$. But the coordinates of Ae_j are exactly the entries a_{ij} on the j-th column of A. Hence

$$|Ae_j|^2 = \sum_{i=1}^{n} a_{ij}^2 \leq 1,$$

which implies that $|a_{ij}| \leq 1$. This works for any pair of indices i, j. Hence $O(n)$ is bounded subset of $M(n; \mathbb{R}) \approx \mathbb{R}^{n^2}$.

b) If $n = 1$ $SL(1; \mathbb{R}) = \{1\}$ is certainly compact.
Suppose $n \geq 2$. Recall that $n \times n$-matrix A is called diagonal matrix, if all its entries outside diagonal are zero. In other words $A = (a_{ij})$ is diagonal if and only if $a_{ij} = 0$ whenever $i \neq j$. It is known from the linear algebra that for a diagonal matrix A we have

$$\det A = a_{11} a_{22} \dots a_{nn}.$$

Now let $> 0a$ be an arbitrary positive real number$A$ be a diagonal $n \times n$-matrix with $a_{11} = a, a_{22} = 1/a, a_{ii} = 1$ for $i > 2$. Then $\det A = 1$, so $A \in SL(n; \mathbb{R})$. Also the Euclidean norm of A (thought of as an element of $\mathbb{R}^{n^2}$) is at least a.

Hence $SL(n;\mathbb{R})$ is not bounded in $\mathbb{R}^{n^2}$, so in particular it cannot be compact).

Hence $SL(n;\mathbb{R})$ is compact if and only if $n = 1$.

4. Suppose H is a closed subgroup of $(\mathbb{R}, +)$, $H \neq \mathbb{R}$. Prove that there exists $a \in \mathbb{R}$ such that $H = a\mathbb{Z}$, hence H is discrete and isomorphic to $\mathbb{Z}$. (Hint: prove that $a = \min(H \cap \{x \in \mathbb{R} \mid x > 0\})$ exists.)
Conclude that every non-trivial subgroup of $(\mathbb{R}, +)$ is either discrete group isomorphic to $\mathbb{Z}$ or dense in $\mathbb{R}$.
Solution: If $H = \{0\}$ is trivial, we clearly have $H = 0\mathbb{Z}$. Suppose H is not trivial. 'Consider the set

$$A = H \cap \{x \in \mathbb{R} \mid x > 0\}.$$

If H is non-trivial, then H contains an element $h \neq 0$. Since H is a group, it also contains $-h$. One of the numbers h or $-h$ are strictly positive. Hence A is non-empty. It is clearly bounded from below, so

$$a = \inf A$$

exists and $a \geq 0$. Suppose $a = 0$. Then (by the definition of infimum) A, hence also H, contains a sequence $(h_n)_{n\in\mathbb{N}}$, where $h_n \in A$ (i.e. $h_n > 0$ for all $n \in \mathbb{N}$) and

$$\lim_{n\to\infty} h_n = 0.$$

Suppose $x \in \mathbb{R}$ is arbitrary. Fix $n \in \mathbb{N}$. Then there exists (unique) integer $m \in \mathbb{Z}$ such that

$$m \leq (x/h_n < m + 1\text{i.e.}$$
$$mh_n \leq x < (m + 1)h_n.$$

This implies that

$$0 \leq x - mh_n < h_n,$$

hence

$$|x - mh_n| < h_n \to 0, \text{ when } n \to \infty.$$

Since H is a group and $m \in \mathbb{Z}$, $mh_n \in H$. We see that we can find an element of H arbitrary close to x. This means that $x \in \overline{H} = H$, since H is closed. We have thus shown that if $a = 0$, $H = \mathbb{R}$. This contradicts the assumptions.

Hence $a > 0$. Since H is closed $a \in H$, in other words

$$a = \min H \cap \{x \in \mathbb{R} \mid x > 0\}.$$

Since H is group it certainly then contains a subgroup $a\mathbb{Z}$ generated by a. Let us show conversely that $H \subset a\mathbb{Z}$.
Suppose $h \in H, h > 0$. Then there exists (unique) integer $n \in \mathbb{N}$ such that

$$na \leq h < (n + 1)a.$$

Then $0 \leq h - na < a$. Since H is a group $h - na \in H$. Now if $h - na > 0$, then $h - na$ is a positive element of H, which is smaller than a, which contradicts the definition of a. Hence $h - na = 0$, i.e. $h = na$. If $h < 0$, $-h > 0$, so $-h \in a\mathbb{Z}$ and hence $h \in a\mathbb{Z}$. Certainly $0 \in a\mathbb{Z}$. Thus $H = a\mathbb{Z}$.

Finally let H be an arbitrary non-trivial subgroup of $\mathbb{R}$. Then $\overline{H}$ is non-trivial closed subgroup of G (Lemma 2.2). Thus either $\overline{H} = \mathbb{R}$, in which case H is dense in $\mathbb{R}$ or $\overline{H} = a\mathbb{Z}$ for some $a > 0$. Now $a\mathbb{Z}$ is discrete, so its only dense subset is $\overline{H}$ itself, hence $H = \overline{H} = a\mathbb{Z}$.

5. Suppose α is an irrational number. Prove that the set
$$\{n + m\alpha \mid n, m \in \mathbb{Z}\}$$
is dense in $\mathbb{R}$.
Solution: The set $H = \{n + m\alpha \mid n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{R}$, so by the previous exercise either H is dense in $\mathbb{R}$ or there exists $c \in \mathbb{R}$ such that $H = c\mathbb{Z}$. Let us show that the second option leads to contradiction.
Now $1, \alpha \in H$, so there exist $n_1, n_2 \in \mathbb{Z}$ such that $1 = n_1 c, \alpha = n_2 c$. Then we have
$$\alpha = \alpha/1 = \frac{n_2 c}{n_1 c} = \frac{n_2}{n_1} \in \mathbb{Q}.$$
This contradicts the assumption.

Remark: In the similar fashion one can show the following.
Suppose $a, b \in \mathbb{R}$. Then the set $a\mathbb{Z} + b\mathbb{Z}$ is dense in $\mathbb{R}$ if and only if a and b are independent over integers, i.e. $na + mb = 0$ if and only if $n = m = 0$.

6. Suppose H is a normal (in algebraic sence) subgroup of a topological group G. Prove that $\overline{H}$ is also normal.
(Reminder: subgroup H is normal if $xH = Hx$ for all $x \in G$.)

Solution: Fix $x \in G$ and consider the mapping $f\colon G \to G$, $f(g) = xgx^{-1}$. This mapping is continuous and $f(H) = xHx^{-1} \subset H$, since H is normal. From the properties of continuous mappings it follows that
$$f(\overline{H}) \subset \overline{f(H)} \subset \overline{H}.$$
Hence $x\overline{H}x^{-1} \subset \overline{H}$. This is true for every $x \in G$. Hence $\overline{H}$ is normal.

Bonus points for the exercises: 25% - 1 point, 40% - 2 points, 50% - 3 points, 60% - 4 points, 75% - 5 points.