Math 561 H **Fall 2011**
Homework 1 Solutions **Drew Armstrong**

---

1. Let G be a group. Prove that the identity element of G is unique (that is, there is only one element of G satisfying the defining property of an identity element). This justifies our use of the special symbol "e".

Proof. Suppose that there exist $e, f \in G$ such that $ae = ea = a$ for all $a \in G$ and $bf = fb = b$ for all $b \in G$. Letting $a = f$ and $b = e$ yields $e = ef = f$. □

2. Let G be a finite group.

(a) Show that there are an odd number of $x \in G$ such that $x^3 = e$.
(b) Show that there are an even number of $x \in G$ such that $x^2 \neq e$.

(Hint: What is the inverse of x^n?)

Proof. Given $x \in G$ we first note that $(x^n)^{-1} = (x^{-1})^n$ (make sure you know why this is true). To prove part (a) we want to show that the size of the set $S = \{x \in G : x^3 = e\}$ is odd. First note that we have $x \in S \Rightarrow x^{-1} \in S$ because inverting both sides of $x^3 = e$ gives $(x^{-1})^3 = e^{-1} = e$. Then substituting $x \to x^{-1}$ in the same argument gives $x^{-1} \in S \Rightarrow x \in S$. Thus the elements of S come in pairs (x, x^{-1}) with $x \neq x^{-1}$ and possibly some single elements with $x = x^{-1}$. But $x \in S$ and $x = x^{-1}$ together imply that $e = x^2 \Rightarrow x = x^3 \Rightarrow x = e$. Hence $e \in S$ is the only element of S that does not come from a pair (x, x^{-1}). We conclude that $|S|$ is odd.

To prove part (b) let $T = \{x \in G : x^2 \neq e\}$. As above we can see that $x \in T \Leftrightarrow x^{-1} \in T$. Furthermore, by definition no element of T satisfies $x = x^{-1}$. Hence the elements of T come in pairs (x, x^{-1}) and we conclude that $|T|$ is even. □

3. Let G be a finite group. For all $a, b \in G$, show that ab and ba have the same order as elements of G.

Proof. We wish to show that the sets $\langle ab \rangle = \{(ab)^k : k \in \mathbb{Z}\}$ and $\langle ba \rangle = \{(ba)^k : k \in \mathbb{Z}\}$ have the same size. This will be done if we can find a bijection from $\langle ba \rangle$ to $\langle ab \rangle$. We claim that ϕ_a from Problem 4 is such a bijection.

Indeed, note that ϕ_a maps $\langle ba \rangle$ into $\langle ab \rangle$ because $\phi_a((ba)^k) = a(ba)^k a^{-1} = (ab)^k(aa^{-1}) = (ab)^k \in \langle ab \rangle$. The injective (one-to-one) property follows from Problem 4, and the map $\phi_a : \langle ba \rangle \to \langle ab \rangle$ is surjective (onto) because **for any** $(ab)^k \in \langle ab \rangle$ we have $(ab)^k = \phi_a((ba)^k)$. □

4. Let G be a group and fix an element $g \in G$. Define a function $\phi_g : G \to G$ by $\phi_g(h) = ghg^{-1}$ for all $h \in G$.

(a) Prove that ϕ_g is a bijection (one-to-one and onto).
(b) Prove that $\phi_g(ab) = \phi_g(a)\phi_g(b)$ for all $a, b \in G$.

These two properties mean that ϕ_g is an automorphism (a "symmetry") of G.

Proof. We first show part (a). To show that ϕ_g is injective (one-to-one), suppose that $\phi_g(a) = \phi_g(b)$, or $gag^{-1} = gbg^{-1}$, for some $a, b \in G$. Applying the map $\phi_{g^{-1}}$ to both sides shows that $a = g^{-1}gag^{-1}g = g^{-1}gbg^{-1}g = b$. To show that ϕ_g is surjective (onto) consider an arbitrary group element $h \in G$. This element is hit by ϕ_g because $\phi_g(g^{-1}hg) = h$. These two properties show that ϕ_g is a bijection from G to itself, otherwise known as a permutation of G.

To show (b), note that for any $a, b \in G$ we have

$$\phi_g(a)\phi_g(b) = (gag^{-1})(gbg^{-1}) = ga(gg^{-1})bg^{-1} = gabg^{-1} = \phi_g(ab).$$

□

So not only is ϕ_g a permutation of the **set** G, but it also preserves the **group structure** of G. Such a map is called an automorphism of G, and the particular map ϕ_g is called "conjugation by g".

5. Suppose that $1, 9, 16, 22, 53, 74, 79, 81$ are eight members of a nine-element subgroup of $(\mathbb{Z}/91\mathbb{Z})^\times$. Which element has been left out? Recall: $(\mathbb{Z}/91\mathbb{Z})^\times$ is the multiplicative group of invertible elements of $\mathbb{Z}/91\mathbb{Z}$. What is the inverse of 9 in this group?

A subgroup must be closed. By trial-and-error multiplying the given eight numbers together (mod 91) you will find that only one extra number shows up. That is, 29. The following multiplication table shows everything we could possibly want to know about this group.

$\times$	1	9	16	22	29	53	74	79	81
1	1	9	16	22	29	53	74	79	81
9	9	81	53	16	79	22	29	74	1
16	16	53	74	79	9	29	1	81	22
22	22	16	79	29	1	74	81	9	53
29	29	79	9	1	22	81	53	16	74
53	53	22	29	74	81	79	9	1	16
74	74	29	1	81	53	9	16	22	79
79	79	74	81	9	16	1	22	53	29
81	81	1	22	53	74	16	79	29	9

In particular, it is a closed subset of $(\mathbb{Z}/91\mathbb{Z})^\times$ because no extra numbers show up in the table. (It is not everything, because $|(\mathbb{Z}/91\mathbb{Z})^\times| = 90$ and our group only has 9 elements.) We can see that every element of our group has an inverse because 1 shows up (exactly once) in each row and column. In particular note that $9 \times 81 = 1 \bmod 91$, hence $9^{-1} = 81$. Finally, note that our group is abelian (commutative) because the table is symmetric about its main diagonal. [Is our group cyclic? Hint: NO. How can you tell from the table?]

6. Let $M_n(\mathbb{R})$ denote the set of all $n \times n$ matrices with real entries. We define the (real) general linear group, special linear group, orthogonal group, and special orthogonal group as follows:

$$GL_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) : \det A \neq 0\},$$
$$SL_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) : \det A = 1\},$$
$$O_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) : AA^T = I\},$$
$$SO_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) : AA^T = I, \det A = 1\}.$$

Why is $GL_n(\mathbb{R})$ a group? Show that $SL_n(\mathbb{R})$, $O_n(\mathbb{R})$ and $SO_n(\mathbb{R})$ are subgroups of $GL_n(\mathbb{R})$.

Your answer will vary, depending on your background in linear algebra. I'll give my version of an answer.

First note that $GL_n(\mathbb{R})$ is closed under matrix multiplication because if $\det(A) \neq 0$ and $\det(B) \neq 0$, it follows that $\det(AB) = \det(A)\det(B) \neq 0$. The identity matrix I is in $GL_n(\mathbb{R})$ since $\det(I) = 1$ and $GL_n(\mathbb{R})$ is closed under inverses because of the fact that A^{-1} exists if and only if $\det(A) \neq 0$.

Note that $\det(A) = 1$ implies $\det(A) \neq 0$, hence $SL_n(\mathbb{R})$ is a subset of $GL_n(\mathbb{R})$. It is closed because $\det(A) = 1$ and $\det(B) = 1$ imply $\det(AB) = \det(A)\det(B) = 1$. The identity matrix is in $SL_n(\mathbb{R})$ and for $A \in SL_n(\mathbb{R})$ we have $A^{-1} \in SL_n(\mathbb{R})$ because $\det(A^{-1}) = 1/\det(A) = 1$.

Note that $AA^T = I$ implies $\det(A) = \pm 1 \neq 0$ because

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

Hence $O_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$. The identity matrix is in $O_n(\mathbb{R})$ because $II^T = I$, and if $AA^T = I$ then inverting both sides gives

$$I = I^{-1} = (AA^T)^{-1} = (A^T)^{-1}A^{-1} = (A^{-1})^T A^{-1}.$$

A slightly fancy result (which I'll prove in class) then implies that $A^{-1}(A^{-1})^T = I$.

Finally, note that $SO_n(\mathbb{R}) = SL_n(\mathbb{R}) \cap O_n(\mathbb{R})$. It is a general fact (can you prove it?) that the intersection of two subgroups is a subgroup.

7. Given a matrix $A \in M_n(\mathbb{R})$ we can define a function from pairs $u, v \in \mathbb{R}^n$ of column vectors to scalars $\mathbb{R}$ by $(u, v)_A := u^T Av$. (Such a function is called a bilinear form — it is a generalization of the dot product.) If $(u, v)_A = (u, v)_B$ for all vectors u, v, **prove** that the matrices A, B are equal. (Hint: What if u, v are standard basis vectors?)

Proof. Suppose that $(u, v)_A = (u, v)_B$ for all column vectors $u, v \in \mathbb{R}^n$. Let $\mathbf{e}_j \in \mathbb{R}^n$ denote the column vector with a 1 in its j-th position and zeroes elsewhere. Then by definition $A\mathbf{e}_j$ equals is the j-th column of A. Taking the dot product of this with $\mathbf{e}_i$ gives $\mathbf{e}_i^T(A\mathbf{e}_j) = a_{ij}$, which is the entry in the i-th row and j-column of A. Finally, note that $a_{ij} = (\mathbf{e}_i, \mathbf{e}_j)_A = (\mathbf{e}_i, \mathbf{e}_j)_B = b_{ij}$ for all $1 \leq i, j \leq n$. Since A and B have the same entries they are equal. □

(We know that we can think of matrices $A \in M_n(\mathbb{R})$ under multiplication as linear functions from $\mathbb{R}^n$ to $\mathbb{R}^n$ under composition. **[And this is the correct way to think.]** Problem 7 shows that we could also think of a matrix $A \in M_n(\mathbb{R})$ as a **bilinear** function from $\mathbb{R}^n \times \mathbb{R}^n$ to $\mathbb{R}$. Unfortunately, such functions cannot be composed. What could matrix multiplication mean in this case?)

8. Let $(u, v) = u^T v$ denote the dot product of column vectors $u, v \in \mathbb{R}^n$. We define the length $\|u\|$ of a vector u by $\|u\|^2 := (u, u)$, so that $\|u - v\|$ represents the distance between two vectors u, v. Now consider an orthogonal matrix $A \in O_n(\mathbb{R})$. Given two vectors $u, v \in \mathbb{R}^n$, **prove** that $\|u - v\| = \|Au - Av\|$.

Proof. Since $A \in O_n(\mathbb{R})$ note that $A^T A = I$. Then by definition we have

$$\begin{aligned}\|Au - Av\|^2 = \|A(u - v)\|^2 = (A(u - v))^T(A(u - v)) = (u - v)^T A^T A(u - v) \\ = (u - v)^T I(u - v) = (u - v)^T(u - v) = \|u - v\|^2.\end{aligned}$$

Taking square roots gives the result. □

(It is also true — but harder to show — that **any** isometry (distance-preserving map) of $\mathbb{R}^n$ that fixes the origin $0 \in \mathbb{R}^n$ is given by $u \mapsto Au$ for some orthogonal matrix $A \in O_n(\mathbb{R})$. This fact is a bit surprising, and it gives a strong geometric meaning to the orthogonal group.)