Math 561 H **Fall 2011**
Homework 2 Solutions **Drew Armstrong**

---

1. Let $\varphi : G \to H$ be a homomorphism of groups. Prove that $\text{im}\,\varphi$ is a subgroup of H.

Proof. First we show that $\mathsf{im}\,\varphi$ is closed. To see this, suppose that $x, y \in \mathsf{im}\,\varphi$, so there exist $a, b \in G$ such that $\varphi(a) = x$ and $\varphi(b) = y$. It follows that $xy = \varphi(a)\varphi(b) = \varphi(ab)$, hence $xy \in \mathsf{im}\,\varphi$. Next, recall from Proposition 2.5.3 in the text that $\varphi(1_G) = 1_H$ and $\varphi(a^{-1}) = \varphi(a)^{-1}$ for all $a \in G$. It follows that $\mathsf{im}\,\varphi$ contains 1_H and is closed under inversion. □

2. Let G be a set with binary operation $(a, b) \mapsto ab$ and consider the following possible axioms:

(1) $\forall\, a, b \in G, a(bc) = (ab)c$.
(2) $\exists\, e \in G, \forall\, a \in G, ae = ea = a$.
(3) $\forall\, a \in G, \exists\, b \in G, ab = ba = e$.
(3') $\forall\, a \in G, \exists\, b \in G, ab = e$.

Prove that the axioms (3) and (3') are equivalent. That is, show that (1), (2), and (3) hold if and only if (1), (2), and (3') hold. (One direction is easy. For the other direction, let $a \in G$. Then there exist $b, c \in G$ such that $ab = e$ and $bc = e$. Show that $a = c$.)

Proof. Assume that (1) and (2) hold. In this case we wish to show that (3)⇔(3'). The fact that (3) implies (3') is trivial. So suppose that (3') holds. That is, every element of the set G has a right inverse. We wish to show (3) — that every element actually has a two-sided inverse. To do this, let $a \in G$. By (3') there exist $b, c \in G$ such that $ab = e$ and $bc = e$. But then applying (1) and (2) gives

$$a = ae = a(bc) = (ab)c = ec = c.$$

It follows that $ab = ba = e$ and hence b is a two-sided inverse for a. □

3. Let H, K be subgroups of G. Prove that $H \cap K$ is also a subgroup of G.

Proof. To show that $H \cap K$ is closed, let $a, b \in H \cap K$. Since H and K are both closed we have $a, b \in H \Rightarrow ab \in H$ and $a, b \in K \Rightarrow ab \in K$. Thus ab is in H and K. In other words, $ab \in H \cap K$. Next, we know that $1_G \in H$ and $1_G \in K$, hence $1_G \in H \cap K$. Finally, let $a \in H \cap K$. Then $a \in H \Rightarrow a^{-1} \in H$ and $a \in K \Rightarrow a^{-1} \in K$. Hence $a^{-1} \in H \cap K$. □

4. (a) Consider a homomorphism $\varphi : \mathbb{Z}^+ \to G$ with $\varphi(1) = g \in G$. Describe $\text{im}\,\varphi$ and $\ker\varphi$.
(b) Describe the set of **automorphisms** $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$.

(a) Since φ is a homomorphism, note that

$$\varphi(n) = \varphi(1 + 1 + \cdots + 1) = \varphi(1)\varphi(1)\cdots\varphi(1) = gg\cdots g = g^n$$

for all positive integers n. Then since φ preserves the identity and inverses, it follows that $\varphi(n) = g^n$ for all $n \in \mathbb{Z}$. (In particular, φ is completely determined by the choice of $\varphi(1)$.) We conclude that $\mathsf{im}\,\varphi$ is the cyclic subgroup $\langle g \rangle \leq G$ generated by the element $g \in G$. Now suppose that $|\langle g \rangle| = a$. If $a < \infty$ then we have $\varphi(n) = g^n = e$ if and only if $n = ak$ for some $k \in \mathbb{Z}$, hence $\mathsf{ker}\,\varphi = a\mathbb{Z} = \{ak : k \in \mathbb{Z}\}$. If $a = \infty$ then note that $g^n = e$ if and only if $n = 0$, hence $\mathsf{ker}\,\varphi = \{0\} = 0\mathbb{Z}$. (This formula could be uniform if you're willing to define $\infty\mathbb{Z} = 0\mathbb{Z}$.)

(b) Now consider a homomorphism $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ (that is, let $G = \mathbb{Z}$). By part (a) the map φ is completely determined by the choice of $\varphi(1) = m \in \mathbb{Z}$. For which m is φ an automorphism (i.e. a bijection)? For φ to be **surjective** we must have $\mathsf{im}\,\varphi = \mathbb{Z}$. Since $\mathsf{im}\,\varphi = \langle m \rangle = m\mathbb{Z}$, this will happen if and only if $m = 1$ or $m = -1$. In both of these cases m has order ∞ in $\mathbb{Z}$ so the kernel is $\ker \varphi = \{0\}$, and we conclude that φ is also **injective**.

Conclusion: There are exactly two automorphisms $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$; call them $\varphi_1(1) := 1$ and $\varphi_2(1) := -1$. Thus $\mathrm{Aut}(\mathbb{Z}^+)$ is a group of order 2 with group table:

$\circ$	φ_1	φ_2
φ_1	φ_1	φ_2
φ_2	φ_2	φ_1

What is the identity element of this group?

5. Given a group G, define its center:

$$Z(G) := \{g \in G : \forall\, h \in G, gh = hg\}.$$

Prove that $Z(G)$ is a normal subgroup of G. (We write $Z(G) \trianglelefteq G$.)

Proof. There are a few ways to think about this. The most concrete way uses Definition 2.5.10 in the text which says that a subgroup $N \leq G$ is normal iff for all $a \in N$ and $g \in G$ we have $gag^{-1} \in N$. So let $a \in Z(G)$ and $g \in G$. We wish to show that $gag^{-1} \in Z(G)$. But by definition we have $ag = ga$. Hence $gag^{-1} = agg^{-1} = a \in Z(G)$ as desired.

A more abstract proof uses that fact that $N \leq G$ is normal iff there exists a group homomorphism $\varphi : G \to G'$ such that $N = \ker \varphi$. In this case we can define a homomorphism $\phi : G \to \mathrm{Aut}(G)$ by sending a group element $g \in G$ to the conjugation map $\phi_g : G \to G$ defined by $\phi_g(h) := ghg^{-1}$ for all $h \in G$. (One needs to check that indeed ϕ is a homomorphism.) Then note that $\ker \phi = Z(G)$. □

Problem 6 had a problem, so I've deleted it. I meant to ask this: Prove that the "center" of the set of $n \times n$ real matrices, defined by $Z(M_n(\mathbb{R})) = \{A \in M_n(\mathbb{R}) : \forall X \in M_n(\mathbb{R}), AX = XA\}$, is equal to the set of scalar matrices $\{cI : c \in \mathbb{R}\}$. (The analogous statement for **invertible** matrices is also true, but harder to show.)

Proof. Let $S = \{cI : c \in \mathbb{R}\}$ denote the set of scalar matrices. We wish to show that $S = Z(M_n(\mathbb{R}))$. First note that $S \subseteq Z(M_n(\mathbb{R}))$. Indeed, given $cI \in S$ we have $cIX = cX = XcI$ for all $X \in M_n(\mathbb{R})$. To complete the proof we must show that $Z(GL_n(\mathbb{R})) \subseteq S$. So suppose $A \in Z(M_n(\mathbb{R}))$ and let a_{ij} denote the entry of A in the i-th row and j-th column. Let E_{ij} denote the matrix with a 1 in the (i, j) position and zeroes elsewhere. Since $A \in Z(M_n(\mathbb{R}))$ we have $AE_{ij} = E_{ij}A$, which reads as:

$$i \begin{pmatrix} & \overset{j}{a_{1i}} & \\ & a_{2i} & \\ & \vdots & \\ & a_{ii} & \\ & \vdots & \\ & a_{ni} & \end{pmatrix} = i \begin{pmatrix} & & & \overset{j}{} & & \\ a_{j1} & a_{j2} & \cdots & a_{jj} & \cdots & a_{jn} \\ & & & & & \end{pmatrix}$$

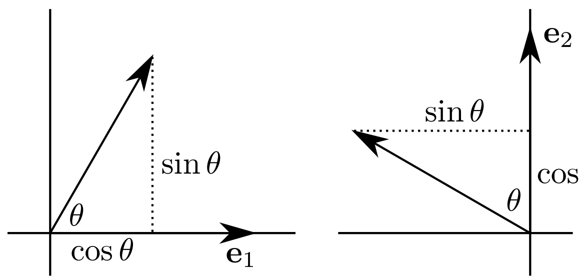
Here i and j label the i-th row and the j-th column of each matrix. Blank space indicates that all the other entries are zero. Since the matrices are equal component-by-component we conclude that all of the displayed symbols are zero except for $a_{ii} = a_{jj}$. Applying this argument for all $1 \leq i < j \leq n$ shows that the diagonal entries of A are all equal and the off-diagonal entries are all zero. That is, $A \in S$.

□

7. Consider the matrix $R_\theta := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

(a) Given $\mathbf{x} \in \mathbb{R}^2$ show that $R_\theta\,\mathbf{x}$ is the rotation of $\mathbf{x}$ by θ degrees counterclockwise. (Hint: It suffices to let $\mathbf{x} = \mathbf{e}_1$ and $\mathbf{x} = \mathbf{e}_2$.)
(b) If $A \in SO_2(\mathbb{R})$ prove that $A = R_\theta$ for some $\theta \in \mathbb{R}$.
(c) Verify that the map $\varphi(e^{i\theta}) := R_\theta$ is an isomorphism $U(1) \approx SO_2(\mathbb{R})$.

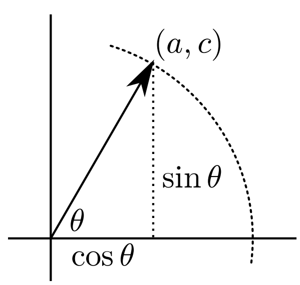
Proof. For part (a), Let $T_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ denote the map that rotates a vector by θ degrees counterclockwise. Then note that $T_\theta(\mathbf{e}_1) = (\cos\theta, \sin\theta)^T$ and $T_\theta(\mathbf{e}_2) = (-\sin\theta, \cos\theta)^T$ as in the following figure:



Finally, since rotation is a **linear** map, we have

$$T_\theta \begin{pmatrix} x \\ y \end{pmatrix} = T_\theta(x \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \end{pmatrix}) = xT_\theta \begin{pmatrix} 1 \\ 0 \end{pmatrix} + yT_\theta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$= x \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} + y \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Thus we have $T_\theta(\mathbf{x}) = R_\theta \mathbf{x}$ for all $\mathbf{x} \in \mathbb{R}^2$, as desired. For part (b) suppose that $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is in $SO(2)$. Note that $A^{-1} = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, hence the condition $A^{-1} = A^T$ implies that $a = d$ and $b = -c$. Thus A is of the form $A = \left(\begin{smallmatrix} a & -c \\ c & a \end{smallmatrix}\right)$ with determinant $a^2 + c^2 = 1$. This means that $(a, c) \in \mathbb{R}^2$ is a point on the unit circle. Let θ be the angle that the corresponding vector makes with the x-axis, as in the following picture:



We conclude that $a = \cos\theta$ and $c = \sin\theta$, as desired. For part (c), consider the map $\varphi : U(1) \to SO(2)$ given by $\varphi(e^{i\theta}) = R_\theta$. To show that φ is **injective**, suppose that $\varphi(e^{i\alpha}) = \varphi(e^{i\beta})$ — i.e. $R_\alpha = R_\beta$ — for some $\alpha, \beta \in \mathbb{R}$. The fact that $R_\alpha = R_\beta$ means that the two rotations do the same thing. In other words, $\alpha - \beta = 2\pi k$ for some $k \in \mathbb{Z}$. This implies that $\cos(\alpha) = \cos(\beta)$ and $\sin(\alpha) = \sin(\beta)$. By Euler's formula ($e^{i\theta} = \cos\theta + i\sin\theta$ for all $\theta \in \mathbb{R}$) we have $e^{i\alpha} = e^{i\beta}$. The fact that φ is **surjective** follows directly from part (b). Finally, to see that φ is a homomorphism note that $R_\alpha R_\beta = R_{\alpha+\beta}$. One could show this, for instance, by quoting the angle-sum triginometric formulas. But I think it is better to observe that $R_\alpha R_\beta$ is the function that rotates a vector by β, **then** rotates by α, which is the same thing as rotating by $\alpha + \beta$. We conclude that

$$\varphi(e^{i\alpha}e^{i\beta}) = \varphi(e^{i(\alpha+\beta)}) = R_{\alpha+\beta} = R_\alpha R_\beta = \varphi(e^{i\alpha})\varphi(e^{i\beta}),$$

as desired. □

[Problem 7(b) has an analogue in 3-dimensions: If $A \in SO(3)$ then A is a rotation by some angle about an axis in $\mathbb{R}^3$. (See "Euler's Theorem" 5.1.25 in the text.) Since $SO(3)$ is a group, this theorem has a remarkable consequence — which is **not** obvious, either algebraically or geometrically: The composition of rotations about any two axes in $\mathbb{R}^3$ is a rotation about some other axis in $\mathbb{R}^3$.]

8. Given $a, b \in G$ we say that a and b are conjugate if there exists $g \in G$ such that $a = gbg^{-1}$. **Prove** that conjugacy is an equivalence relation on G. (The equivalence classes are called conjugacy classes.) **Prove**: If $a, b \in G$ are conjugate then they have the same order.

Proof. To show transitivity, suppose that a is conjugate to b and b is conjugate to c. That is, there exist $g, h \in G$ such that $a = gbg^{-1}$ and $b = hch^{-1}$. Then

$$a = gbg^{-1} = ghch^{-1}g^{-1} = (gh)c(gh)^{-1},$$

hence a is conjugate to c. To show symmetry, suppose a is conjugate to b. That is, there exists $g \in G$ such that $a = gbg^{-1}$. But then $b = (g^{-1})a(g^{-1})^{-1}$, hence b is conjugate to a. Finally, note that $a = eae^{-1}$ for all $a \in G$, hence a is conjugate to itself. We conclude that conjugacy is an equivalence relation.

Now consider $a, b \in G$ with $a = gbg^{-1}$ for some $g \in G$. We claim that a and b have the same order. Indeed, consider the conjugation map $\phi_g : G \to G$ defined by $\phi_g(h) = ghg^{-1}$ for all $h \in G$. It is easy to see that ϕ_g restricts to a bijection $\phi_g : \langle b \rangle \to \langle a \rangle$ of cyclic subgroups. (You proved a special case on the first homework.) □