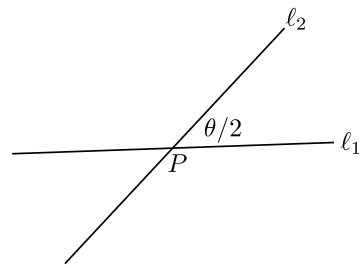
Math 561 H **Fall 2011**
Homework 5 **Drew Armstrong**

1. We saw in class that any element of the orthogonal group $O(2)$ has the form

$$R_\theta := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \text{or} \quad F_\theta := \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.$$

The matrix R_θ (with determinant 1) **rotates** the plane around 0 counterclockwise by the angle θ. The matrix F_θ (with determinant -1) **reflects** the plane across the line through 0 that has angle $\theta/2$ measured counterclockwise from the x-axis.

(a) For all angles $\alpha, \beta \in \mathbb{R}$, prove that $F_\alpha F_\beta = R_{\alpha-\beta}$.
(b) Consider lines ℓ_1 and ℓ_2 in $\mathbb{R}^2$ with intersection P and angle $\theta/2$ as below.



Let F_ℓ denote the reflection across line ℓ and let R_θ^P denote the rotation around the point P counterclockwise by θ. **Prove** that $F_{\ell_2} \circ F_{\ell_1} = R_\theta^P$. (Hint: You can assume that $P = 0$ and ℓ_1 is the x-axis. Use part (a).)

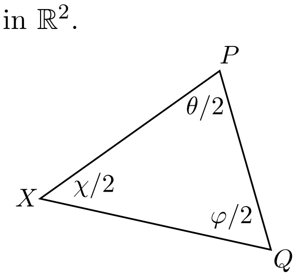
Proof. For part (a) we compute the matrix product to get

$$\begin{aligned} F_\alpha F_\beta &= \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} \begin{pmatrix} \cos\beta & \sin\beta \\ \sin\beta & -\cos\beta \end{pmatrix} \\ &= \begin{pmatrix} \sin\alpha\sin\beta + \cos\alpha\cos\beta & -(\sin\alpha\cos\beta - \cos\alpha\sin\beta) \\ \sin\alpha\cos\beta - \cos\alpha\sin\beta & \sin\alpha\sin\beta + \cos\alpha\cos\beta \end{pmatrix} \\ &= \begin{pmatrix} \cos(\alpha-\beta) & -\sin(\alpha-\beta) \\ \sin(\alpha-\beta) & \cos(\alpha-\beta) \end{pmatrix} = R_{\alpha-\beta}. \end{aligned}$$

We have shown that the product of two reflections is a rotation (or the identity). For part (b), let us assume that $P = 0$ and ℓ_1 is the x-axis. (This amounts to conjugation by an element of $\text{Isom}(\mathbb{R}^n)$, but never mind.) Then the matrices corresponding to the linear maps F_{ℓ_2} and F_{ℓ_1} are F_θ and F_0, respectively. By part (a) we find that the matrix of the composition $F_{\ell_2} \circ F_{\ell_1}$ is $F_\theta F_0 = R_\theta$, which is the matrix for R_θ^0. □

[Alternatively, you could use a purely geometric argument to prove part (b), in this case you could regard the calculation in part (a) as a **proof** of the trigonometric angle sum formulas.]

2. Consider the following triangle in $\mathbb{R}^2$.



Again let R^P_θ denote the rotation around point P counterclockwise by angle θ. **Prove** that

$$R^Q_\varphi \circ R^P_\theta = R^X_{-\chi}.$$

(Hint: Use Problem 1(b).) What happens when $\theta = \varphi \to 180°$?

Proof. This is fun. Let F_{PQ}, F_{PX} and F_{QX} denote the reflections in the (lines generating the) sides of the triangle. By Problem 1(b) we have $R^P_\theta = F_{PQ} \circ F_{PX}$ and $R^Q_\varphi = F_{QX} \circ F_{PQ}$. Composing these and using the fact that a reflection is its own inverse gives

$$\begin{aligned} R^Q_\varphi \circ R^P_\theta &= F_{QX} \circ F_{PQ} \circ F_{PQ} \circ F_{PX} \\ &= F_{QX} \circ (F_{PQ} \circ F_{PQ}) \circ F_{PX} \\ &= F_{QX} \circ F_{PX}. \end{aligned}$$

Next, note that the inverse of a clockwise rotation is a counterclockwise rotation by the same angle, hence $(R^X_\chi)^{-1} = R^X_{-\chi}$. Applying Problem 1(b) again gives

$$R^X_{-\chi} = (R_\chi)^{-1} = (F_{PX} \circ F_{QX})^{-1} = F^{-1}_{QX} \circ F^{-1}_{PX} = F_{QX} \circ F_{PX}.$$

□

[This is obviously the "correct" proof. (What would we have done without Problem 1(b)?) Now suppose that $\theta/2 = \varphi/2 \to 90°$. In this case the point X goes to infinity, the angle χ goes to 0, and the composition $R^Q_\varphi \circ R^P_\theta$ becomes a **translation** of the plane by the vector $2(P \to Q)$. So a translation is just a rotation around a "point at infinity" by an "infinitesimal angle". The group $\text{Isom}(\mathbb{R}^2)$ is interesting, isn't it?]

3. Let $\text{Isom}(\mathbb{R}^n)$ denote the group of isometries $\varphi : \mathbb{R}^n \to \mathbb{R}^n$. We know that if φ fixes the origin, then φ is an orthogonal linear map. Let $O(n) \leq \text{Isom}(\mathbb{R}^n)$ denote the subgroup fixing the origin. Given $\alpha \in \mathbb{R}^n$, define the translation $t_\alpha : \mathbb{R}^n \to \mathbb{R}^n$ by $t_\alpha(x) := x + \alpha$. Clearly this is an isometry. Let $\mathbb{R}^n_+ \leq \text{Isom}(\mathbb{R}^n)$ denote the (abelian) subgroup of translations, which is isomorphic to vector addition on $\mathbb{R}^n$ via $t_\alpha \circ t_\beta = t_{\alpha+\beta}$.

(a) Prove that every isometry $f \in \text{Isom}(\mathbb{R}^n)$ can be written **uniquely** in the form $f = t_\alpha \circ \varphi$ with $t_\alpha \in \mathbb{R}^n_+$ and $\varphi \in O(n)$. (Hint: Let $\alpha = f(0)$.)

(b) Given $\alpha \in \mathbb{R}^n$ and $\varphi \in O(n)$, prove that $\varphi \circ t_\alpha = t_{\alpha'} \circ \varphi$, where $\alpha' = \varphi(\alpha)$.

(c) Prove that $\mathbb{R}^n_+ \trianglelefteq \text{Isom}(\mathbb{R}^n)$, and hence $\text{Isom}(\mathbb{R}^n) = \mathbb{R}^n_+ \rtimes O(n)$. (This is the prototypical example of a semi-direct product.) Describe how to multiply the elements $t_\alpha \circ \varphi$ and $t_\beta \circ \psi$. Conclude that $\text{Isom}(\mathbb{R}^n) \not\approx \mathbb{R}^n_+ \times O(n)$.

Proof. To prove (a), consider an isometry $f \in \text{Isom}(\mathbb{R}^n)$ and let $\alpha := f(0) \in \mathbb{R}^n$. Then the isometry $t_{-\alpha} \circ f$ fixes the origin since $t_{-\alpha}(f(0)) = t_{-\alpha}(\alpha) = \alpha - \alpha = 0$. By the Cartan-Dieudonné Theorem (which we proved in class) it follows that $t_{-\alpha} \circ f = \varphi$ for some $\varphi \in O(n)$. Hence $f = t^1_{-\alpha} \circ \varphi = t_\alpha \circ \varphi$. This expression is unique because $\mathbb{R}^n_+ \cap O(n)$ is trivial — only the trivial translation fixes the origin. (Remind yourself why this implies uniqueness.) To prove part (b), consider any vector $x \in \mathbb{R}^n$ and observe that

$$\varphi \circ t_\alpha(x) = \varphi(t_\alpha(x)) = \varphi(x + \alpha) = \varphi(x) + \varphi(\alpha) = t_{\varphi(\alpha)}(\varphi(x)) = t_{\varphi(\alpha)} \circ \varphi(x).$$

Here we used the fact that $\varphi \in O(n)$ is linear. To prove (c), let $t_\alpha \in \mathbb{R}^n_+$ and consider an arbitrary element of $\text{Isom}(\mathbb{R}^n)$, which by part (a) we can take to be $t_\beta \circ \varphi$ for $\varphi \in O(n)$. By part (b) we know that $\varphi \circ t_\alpha \circ \varphi^{-1} = t_{\varphi(\alpha)}$. Then conjugating t_α by $t_\beta \circ \varphi$ gives

$$\begin{aligned} (t_\beta \circ \varphi) \circ t_\alpha \circ (t_\beta \circ \varphi)^{-1} &= t_\beta \circ \varphi \circ t_\alpha \circ \varphi^{-1} \circ t_{-\beta} \\ &= t_\beta \circ t_{\varphi(\alpha)} \circ t_{-\beta} \\ &= t_{\varphi(\alpha)}. \end{aligned}$$

Hence $\mathbb{R}^n_+$ is closed under conjugation by $\text{Isom}(\mathbb{R}^n)$ and we conclude that $\mathbb{R}^n_+ \trianglelefteq \text{Isom}(\mathbb{R}^n)$. Parts (a), (b) and (c) imply that $\text{Isom}(\mathbb{R}^n)$ has a semi-direct product structure $\text{Isom}(\mathbb{R}^n) = \mathbb{R}^n_+ \rtimes O(n)$ with group operation given by

$$(t_\alpha \circ \varphi) \circ (t_\beta \circ \rho) = t_{\alpha+\varphi(\beta)} \circ (\varphi\rho).$$

We could phrase this abstractly as a product on ordered pairs $(t_\alpha, \varphi)(t_\beta, \rho) = (t_{\alpha+\varphi(\beta)}, \varphi\rho)$, where $\alpha + \varphi(\beta)$ takes place in $\mathbb{R}^n_+$ and $\varphi\rho$ takes place in $O(n)$. This is **not** a direct product because the direct product structure is defined by

$$(t_\alpha, \varphi)(t_\beta, \rho) := (t_{\alpha+\beta}, \varphi\rho).$$

Our product is not direct is because $O(n)$ acts on $\mathbb{R}^n_+$ in a non-trivial way (another way of saying this is that $O(n)$ and $\mathbb{R}^n_+$ don't commute inside $\text{Isom}(\mathbb{R}^n)$ — see part (b)). ☐

[So, if you care about isometries of Euclidean space then you care about semi-direct products.]

4. The Lemma That Is Not Burnside's is a nice way to compute the number of orbits when a finite group G acts on a finite set S. Here you will prove it.

(a) Let $S^g = \{s \in S : gs = s\}$ be the set fixed by $g \in G$ and let $G_s = \{g \in G : gs = s\}$ be the subgroup of G that fixes $s \in S$. Count the elements of the set $\{(g, s) \in G \times S : gs = s\}$ in two different ways to show that

$$\sum_{g\in G} |S^g| = \sum_{s\in S} |G_s|.$$

(b) Let $G(s) = \{gs : g \in G\}$ be the orbit generated by $s \in S$ and let S/G denote the set of orbits (which, recall, partition the set S). Prove that

$$\sum_{s\in S} \frac{1}{|G(s)|} = |S/G|.$$

(c) Combine (a) and (b) to prove that

$$|S/G| = \frac{1}{|G|} \sum_{g\in G} |S^g|.$$

That is, the number of orbits is equal to the average number of elements of S fixed by an element of G. (Hint: Orbit-Stabilizer Theorem.)

Proof. For part (a), let $X = \{(g, s) \in G \times S : gs = s\}$. We can count the elements of X in two ways. First, given a group element $g \in G$, there are exactly $|S^g|$ elements $s \in S$ such that $(g, s) \in X$, hence $|X| = \sum_{g\in G} |S^g|$. On the other hand, given an element $s \in S$, there are exactly $|G_s|$ group elements $g \in G$ such that $(g, s) \in X$, hence $|X| = \sum_{s\in S} |G_s|$. We conclude that $\sum_{s\in S} |G_s| = |X| = \sum_{g\in G} |S^g|$. Next, consider the sum $\sum_{s\in S} 1/|G(s)|$, where $G(s)$ is the G-orbit of $s \in S$. If we partition the set S into orbits $S/G = \{O_1, \ldots, O_k\}$, then for each $s \in O_i$ we have $G(s) = O_i$. Then we can partition the sum over orbits to get

$$\sum_{s\in S} \frac{1}{|G(s)|} = \sum_{i=1}^{k} \sum_{s\in O_i} \frac{1}{|O_i|} = \sum_{i=1}^{k} |O_i| \frac{1}{|O_i|} = \sum_{i=1}^{k} 1 = k = |S/G|.$$

Finally, we apply the Orbit-Stabilizer Theorem (i.e. $|G| = |G(s)||G_s|$ for all $s \in S$) to get

$$\sum_{g\in G} |S^g| = \sum_{s\in S} |G_s| = \sum_{s\in S} \frac{|G|}{|G(s)|} = |G| \sum_{s\in S} \frac{1}{|G(s)|} = |G||S/G|.$$

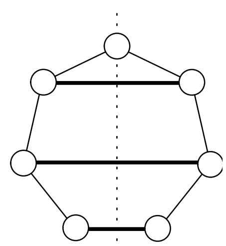
Dividing by $|G|$ gives the result. ☐

5. We say a bracelet of size n is a circular string of n black and white beads. We say that two bracelets are **equal** if they differ by a dihedral symmetry. (You can rotate a bracelet and you can take it off your wrist, flip it over, and put it back on.) Use The Lemma That Is Not Burnside's to **compute the number of bracelets of size** 7.

Let X be the set of circular arrangements of 7 black or white beads. We regard these as fixed in the plane (so that we can say e.g. that "bead number i is white"), hence we have $|X| = 2^7 = 128$. However, a bracelet doesn't have a "bead number i". Instead, we let D_7 act on X by rotation and reflection, and note that two arrangements represent the same bracelet if and only if they are in the same D_7 orbit. By Burnside's Lemma, the number of bracelets/orbits is

$$|X/D_7| = \frac{1}{|D_7|} \sum_{g \in D_7} |X^g|.$$

To solve this, we need to compute $|X^g|$ — the number of arrangements fixed by g — for each $g \in D_7$, which is 14 computations in total. However, the number $|X^g|$ is constant over each conjugacy class in D_7, so there are really only 5 computations (the number of D_7-conjugacy classes). First note that $g = 1$ fixes all 128 arrangements. The rotations come in three pairs $\{\rho, \rho^{-1}\}$, $\{\rho^2, \rho^{-2}\}$ and $\{\rho^3, \rho^{-3}\}$, where ρ is rotation by $2\pi i/7$. In principle we might need to do 3 calculations, but since $1, 2, 3$ are all coprime to 7, we find that any of these six rotations can only fix the all-white arrangement and the all-black arrangement. Finally, there is one class of 7 reflections, show below. The number of arrangements invariant under a reflection is $2^4 = 16$. Indeed, since beads on the same horizontal level have the same color and there are 2 possible colors, we have $2^4 = 16$ choices.



Finally, we conclude that the number of bracelets is

$$|X/D_7| = \frac{1}{14}[128 + 2 + 2 + 2 + 2 + 2 + 2 + 16 + 16 + 16 + 16 + 16 + 16 + 16] = 18.$$

You see that Burnside's Lemma is very useful. In general, we can use the same method to count k-colored necklaces with n beads (where we allow cyclic symmetry) and k-colored bracelets with n beads (where we allow dihedral symmetry). If $N_k(n)$ and $B_k(n)$ are the numbers of k-colored necklaces and bracelets, respectively, with n beads, then we find

$$N_k(n) = \frac{1}{n} \sum_{d|n} \varphi(d)\, k^{n/d},$$

and

$$B_k(n) = \begin{cases} \frac{1}{2} N_k(n) + \frac{1}{4}(k+1)k^{n/2} & \text{for } n \text{ even} \\ \frac{1}{2} N_k(n) + \frac{1}{2} k^{(n+1)/2} & \text{for } n \text{ odd} \end{cases}$$

Verify that $N_1(n) = 1$. Verify that $B_2(7) = 18$.