Math 100A Notes (Professor: Aaron Pollack)

Isabelle Mills

October 5, 2024

Lecture 1 Notes: 9/27/2024

Motivation for this class:
Let $\mathcal{F}$ be any figure in $\mathbb{R}^2$. We want some way of talking about the symmetries of $\mathcal{F}$.

Letting d be the standard metric for $\mathbb{R}^2$, we say $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ is distance preserving if $d(P, Q) = d(f(P), f(Q))$ for all $P, Q \in \mathbb{R}^2$. If f is distance-preserving and $f(\mathcal{F}) = \mathcal{F}$, then we call f a symmetry of $\mathcal{F}$.

We define $\mathrm{Sym}(\mathcal{F})$ to be the set of symmetries of $\mathcal{F}$.

Lemma 2: The set $\mathrm{Sym}(\mathcal{F})$ has the following properties:

1. The identity map Id is in $\mathrm{Sym}(\mathcal{F})$
2. If $f \in \mathrm{Sym}(\mathcal{F})$, then $f^{-1} \in \mathrm{Sym}(\mathcal{F})$.

   I realize we haven't yet shown that every $f \in \mathrm{Sym}(\mathcal{F})$ is a bijection. Given such an f, it's easy to see that f must be injective. After all, the distance preserving property of f means that $f(P) = f(Q) \Longrightarrow P = Q$. Showing that f is surjective is harder. By assumption, we know that f is surjective when restricted to $\mathcal{F}$. More complicatedly, we can show that f must have a certain form which happens to be surjective. Perhaps I'll prove that later.

   Once, you've accepted that f^{-1} exists, then it's clearly true that f^{-1} is also distance preserving with $f^{-1}(\mathcal{F}) = \mathcal{F}$.
3. If $f_1, f_2 \in \mathrm{Sym}(\mathcal{F})$, then $f_1 \circ f_2 \in \mathrm{Sym}(\mathcal{F})$ and $f_2 \circ f_1 \in \mathrm{Sym}(\mathcal{F})$.

   This is pretty trivial to show.

Now while it's all good that we have a concrete way of describing the symmetries of a figure, our current terminology is not the most useful. After all, suppose $\mathcal{S}$ and $\mathcal{S}'$ are two squares such that $\mathcal{S}$ is centered at the origin and $\mathcal{S}'$ is centered at the point $(5, 5)$. Then even though we know both $\mathcal{S}$ and $\mathcal{S}'$ have symmetries in the form of rotating and reflecting, the particular functions in $\mathrm{Sym}(\mathcal{S})$ and $\mathrm{Sym}(\mathcal{S})$ will be different (except for Id). So, how do we compare the symmetries of those two squares?

Aside start…

Proof that all symmetries are surjective (taken from our textbook):

Note:

- Our textbook calls a distance-preserving function $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ an isometry.
- Rather than writing $f_1 \circ f_2$ to represent function composition, our textbook just writes $f_1 f_2$.

Some Facts:

(a) Orthogonal linear operators are isometries.

Let φ be n orthogonal linear map. φ being linear means that $\varphi(u) - \varphi(v) = \varphi(u - v)$. Meanwhile, φ being orthogonal means that $|\varphi(u-v)| = \sqrt{\varphi(u-v) \cdot \varphi(u-v)} = \sqrt{(u-v) \cdot (u-v)} = |u - v|$. So, for any $u, v \in \mathbb{R}^n$, we have that $|\varphi(u) - \varphi(v)| = |u - v|$.

(b) The translation t_a by a vector a defined by $t_a(x) = x + a$ is an isometry.

For any $u, v \in \mathbb{R}^n$, we have $|t_a(u) - t_a(v)| = |u + a - v - a| = |u - v|$.

(c) The composition of isometries is an isometry.

If f_1, f_2 are isometries, then for all $u, v \in \mathbb{R}^n$, we have that $|f_1(f_2(u)) - f_1(f_2(v))| = |f_2(u) - f_2(v)| = |u - v|$.

Theorem 6.2.3: The following conditions on a map $\varphi : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ are equivalent:

(a) φ is an isometry such that $\varphi(0) = 0$.

(b) φ preserves dot products: $\varphi(u) \cdot \varphi(w) = u \cdot w$ for all $u, w \in \mathbb{R}^n$.

(c) φ is an orthogonal linear operator.

Proof:
(c) $\Longrightarrow$ (a)
This comes both from the first fact on this page plus the fact that all linear operators map 0 to 0.

(b) $\Longrightarrow$ (c)
Our challenge here is to show that such a φ has to be linear operator.

Lemma: For $x, y \in \mathbb{R}^n$, if $(x \cdot x) = (x \cdot y) = (y \cdot y)$, then $x = y$.

Proof: $|x - y|^2 = (x - y) \cdot (x - y) = (x \cdot x) - 2(x \cdot y) + (y \cdot y)$.

Consider any $u, v \in \mathbb{R}^n$ and set $w = u + v$. Then set $u' = \varphi(u)$, $v' = \varphi(v)$, and $w' = \varphi(w)$. To show that $w' = v' + u'$, we shall show that $(w' \cdot w') = (w' \cdot (u' + v')) = ((u' + v') \cdot (u' + v'))$.

Firstly, simplify our equation to:

$$(w' \cdot w') = (w' \cdot u') + (w' \cdot v') = (u' \cdot u') + 2(u' \cdot v') + (v' \cdot v')$$

Next, since φ is assumed to preserve dot products, we can thus simplify our equation to:

$$(w \cdot w) = (w \cdot u) + (w \cdot v) = (u \cdot u) + 2(u \cdot v) + (v \cdot v)$$

And since $w = u + b$, all of those equalities are true. Hence, we know by our lemma above that $w' = u' + v'$.

Meanwhile, let $v \in \mathbb{R}^n$ and set $u = cv$ where c is a constant. Then define u' and v' as before. Then we can do a few trivial simplications to show that $(u' \cdot u')$, $(u' \cdot cv')$ and $(cv' \cdot cv')$ are all equal to $c^2(v \cdot v)$. So, $u' = cv'$.

(a) $\Longrightarrow$ (b)
Since φ is distance preserving, we know that $\forall u, v \in \mathbb{R}^n$,
$$(\varphi(u) - \varphi(v)) \cdot (\varphi(u) - \varphi(v)) = (u - v) \cdot (u - v)|.$$

By plugging in $v = 0$, this simplifies to $(\varphi(u) \cdot \varphi(u)) = (u \cdot u)$. Similarly, by plugging in $u = 0$, we can get that $(\varphi(v) \cdot \varphi(v)) = (v \cdot v)$. So, by expanding and canceling out parts of our above expression, we get that:
$$-2(\varphi(u) \cdot \varphi(v)) = -2(u \cdot v).$$

Corollary 6.2.7: Every isometry f of $\mathbb{R}^n$ is the composition of an orthogonal linear operator and a translation. Specifically, if $f(0) = a$, then $f = t_a\varphi$ where t_a is a translation and φ is an orthogonal linear operator.

Proof:
Let f be an isometry, let $a = f(0)$, and define $\varphi = t_{-a}f$. Then clearly $t_a\varphi = f$. So, we just need to show that φ is an orthogonal linear operator. To prove this, first note that φ is the composition of two isometries, and is thus an isometry itself. Also, $\varphi(0) = -a + f(0) = -a + a = 0$. So applying theorem 6.2.3, we know that φ is an orthogonal linear operator.

Now we've proven in other classes that both translations and linear orthogonal operators on $\mathbb{R}^n$ are surjective. So, all isometries are the composition of surjections, meaning they are surjective themselves. And since we also previously proved that all isometries are injective, we know they are bijective and have inverses.

Aside over...

Lecture 2 Notes: 9/30/2024

I already covered everything from this lecture in my math journal (pages 40-42).

Lecture 3 Notes: 10/2/2024

Suppose G_1 and G_2 are groups. A map $\rho : G_1 \longrightarrow G_2$ is called a group homomorphism if $\rho(xy) = \rho(x)\rho(y)$ for all $x, y \in G_1$. If ρ is bijective, we say that ρ is an isomorphism, and that G_1 and G_2 are isormophic. Also if ρ is bijective, we have that ρ^{-1} is also a group homomorphism.

If two groups are isomorphic, then we can say they are in a sense equivalent.

Suppose G is a group and $H \subseteq G$. Then H equipped with the law of composition of G restricted to $H \times H$ is a subgroup if:

- $1 \in H$
- $x \in H \implies x^{-1} \in H$
- $x, y \in H \implies xy \in H$

Example: If $\mathbb{R}^\times = (\mathbb{R} - \{0\}, \times)$, then some non-trivial subgroups of $\mathbb{R}^x$ are:

- $M_2 = \{1, -1\}$
- $\mathbb{Z}^x = \mathbb{Z} - \{0\}$
- $\mathbb{Q}^x = \mathbb{Q} - \{0\}$
- $H = \{a^n \in \mathbb{R} \mid n \in \mathbb{Z}\}$.

Theorem: Let S be a subgroup of $(\mathbb{Z}, +)$ (the set of integers equipped with integer addition). Then either $S = \{0\}$ or $S = \mathbb{Z}a = \{na \mid n \in \mathbb{Z}\}$ where a is the least positive element of S.

Proof:
We clearly have that $\{0\}$ and $\mathbb{Z}a$ are groups under addition for any $a \in \mathbb{Z}_+$. Meanwhile, suppose $S \neq \{0\}$ is a subgroup of $(\mathbb{Z}, +)$. Then, by taking inverses if necessary, we know $S \cap \mathbb{Z}_+$ is nonempty. Since $\mathbb{Z}_+$ is well-ordered, there exists a least element in $S \cap \mathbb{Z}_+$ which we'll call a.

Trivially, we have that $\mathbb{Z}a \subseteq S$. Meanwhile consider any $n \in S$. Then $n = qa + r$ for some $q \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, a-1\}$. However, since $r = n - qa$ and $n, -qa \in S$, we must have that $r \in S$. And, the only allowed value for r such that $r \in S$ is $r = 0$. Thus, $n \in \mathbb{Z}a$, meaning we've shown that $S \subseteq \mathbb{Z}_a$.

Lecture 4 Notes: 10/4/2024

As an immediate application of the above theorem, note that $S = \mathbb{Z}a + \mathbb{Z}b = \{ma + nb \mid m, n \in \mathbb{Z}\}$ is subgroup of $\mathbb{Z}$ under addition.

This is trivial to prove.

By our previous theorem, we know that $S = \mathbb{Z}d$ for some unique positive integer d. So, we define the greatest common divisor of a and b to be $\gcd(a, b) := d$.

Proposition: Let $a, b \in \mathbb{Z}$ be not both 0 and $d = \gcd(a, b)$.

1. There exists $r, s \in \mathbb{Z}$ such that $d = ra + sb$
2. d divides a and b (written $d \mid a$ and $d \mid b$).

Both of these claims are trivially true by our definition of S.

3. If $e \in \mathbb{Z}$ and e divides a and b, then e divides d. This is why d is called the "greatest common divisor" of a and b.

    Let $r, s \in \mathbb{Z}$ such that $d = ra + sb$. Then letting $a = en$ and $b = em$, we have that $d = (rn + sm)e$, meaning $e \mid d$.

An algorithm for finding $\gcd(a, b)$ is given as follows:

1. Assume without loss of generality that $a \geq b \geq 0$ and $a \neq 0$.
2. If $b = 0$, then $\gcd(a, b) = \gcd(b, a) = a$
3. Else, there exists $q, r \in \mathbb{Z}$ with $0 \leq r < b$ and $a = qb + r$. We claim that $\gcd(a, b) = \gcd(b, r)$.

    This is because if $d \mid a$ and $d \mid b$, then we know $d \mid (qb + r)$ and $d \mid qb$, meaning that $d \mid (qb + r - qb) = r$. On the other hand, if $e \mid r$ and $e \mid b$, then $e \mid (qb + r) = a$. So a and b have the same common factors as b and c.

Suppose $a, b \in \mathbb{Z}$. We say a and b are relatively prime iff $\gcd(a, b) = 1$.

Corollary: $\gcd(a, b) = 1$ if and only if there exists $r, s \in \mathbb{Z}$ such that $ra + sb = 1$.

Proof:
($\Longrightarrow$) By definition, $\gcd(a, b) \in \mathbb{Z}a + \mathbb{Z}b$.
($\Longleftarrow$) If $ra + sb = 1$, then 1 must be the least positive element of $\mathbb{Z}a + \mathbb{Z}b$. So $\gcd(a, b) = 1$.

Lemma: Suppose $\gcd(a, b) = 1$ and $a \mid bc$. Then $a \mid c$.

Proof:
Let $1 = ra + sb$ where $r, s \in \mathbb{Z}$. Then $c = rac + sbc = (rc + s\frac{bc}{a})a$ where $\frac{bc}{a}$ is an integer. So $a \mid c$.

Corollary: Suppose p is a prime integer. If $a, b \in \mathbb{Z}$ and $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Proof:
Suppose $p \nmid a$. Then $\gcd(p, a) = 1$ because the only positive divisor of p other than p is 1. So there exists $r, s \in \mathbb{Z}$ such that $1 = rp + sa$. In turn, since $\frac{ab}{p}$ is an integer, we have $b = rpb + sab = p(rb + s\frac{ab}{p})$, meaning $p \mid b$.

Problem: Suppose p is prime and that $a \in \mathbb{Z}$ is not a multiple of p. Then there exists $x \in \mathbb{Z}$ so that ax is one more than some multiple of p.

Proof:
Like before, we must have that $\gcd(a, p) = 1$, meaning that there exists $r, s \in \mathbb{Z}$ such that $rp + sa = 1$. So, if we set $x = s$, we'd be done cause $xa = (-r)p + 1$.

More interestingly, we can guarentee that xa is one more than a nonnegative multiple of p as follows:

Note that $sa = -rp + 1 \implies (s^2a)a = (r^2p - 2r)p + 1 = r(rp - 2)p + 1$. Since $p \geq 2$, we have that $r \geq 1 \implies (rp - 2) > 0$, meaning $r(rp - 2) > 0$. Meanwhile, we have that $r \leq 0 \implies (rp - 2) < 0$, which in turn means $r(rp - 2) \geq 0$.

Setting $x = s^2a$ and $n = r^2p - 2r$, we thus have that $xa = np + 1$ where np is a nonnegative multiple of p.

Lemma: Suppose G is a group and H_1, H_2 are subgroups of G. Then $H_1 \cap H_2$ is a subgroup of G.

This is rather trivial to prove. So do it yourself! :3

Because of the above lemma, given $a, b \in \mathbb{Z}$, we have that $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$ for some integer $m \geq 0$. We call m the least common multiple of a and b, and we denote $\operatorname{lcm}(a, b) := m$.

Proposition: Let a and b be nonzero integers and $m = \operatorname{lcm}(a, b)$.

1. m is nonzero.
2. m is divisible by both a and b

   Both of these points are trivial from the fact that $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$ and $ab \in \mathbb{Z}m$, meaning that $\mathbb{Z}m - \{0\} \neq \emptyset$.
3. If $n \in \mathbb{Z}$ such that $a \mid n$ and $b \mid n$, then $m \mid n$.

   This comes trivially from the fact that $n \in \mathbb{Z}a$ and $n \in \mathbb{Z}b$ means that $n \in \mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$

Suppose G is a group and $x \in G$. Then let $H = \{x^k \mid k \in \mathbb{Z}\} \subseteq G$. We clearly have that H is a subgroup of G. We call it the cyclic subgroup of G generated by x, and denote it $H = \langle x \rangle$.

Proposition: Let $S = \{k \in \mathbb{Z} \mid x^k = 1\}$

1. S is a subgroup of $(\mathbb{Z}, +)$.

   This is rather trivial to show. So do it yourself!!
2. Suppose $S \neq \{0\}$, meaning $S = \mathbb{Z}n$ for some positive integer n. Then $1, x, \dots, x^{n-1}$ are the distinct elements of $\langle x \rangle$, meaning the order of $\langle x \rangle$ is n.

   Proof:
   $x^k = x^l \iff x^{k-l} = 1$. Hence, since n is the minimum positive integer such that $x^n = 1$, we know that $1, x, \dots, x^{n-1}$ are distinct. On the other hand, if $k = qn + r$ for any $q, r \in \mathbb{Z}$ with $0 \leq r < n$, then $x^k = (x^n)^q x^r = x^r$. So the only elements of $\langle x \rangle$ are $1, x, \dots, x^{n-1}$.

Our textbook is *Algebra, Second Edition* by Michael Artin.