Math 100A Notes (Professor: Aaron Pollack)

Isabelle Mills

October 14, 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 $f(P) = f(Q) \implies P = Q$. 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 $\{H_\alpha\}_{\alpha \in A}$ are subgroups of G. Then $\bigcap\limits_{\alpha \in A} H_\alpha$ 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 $1, x, \ldots, x^{n-1}$ 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 $1, x, \ldots, x^{n-1}$ 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 $1, x, \ldots, x^{n-1}$.

Corollary: If $S = \{k \in \mathbb{Z} \mid x^k = 1\} = \{0\}$, then $x^k = x^l \implies k - l = 0 \implies k = l$.

Lecture 5 Notes: 10/7/2024

If G is a group and $x \in G$, one says x has order n if n is the smallest positive integer for which $x^n = 1$. If there is no such integer, then we say x has infinite order.

Lemma: Suppose that G is a group, that $x \in G$ has order n, and that $\gcd(k, n) = d$. Then x^k has order ${}^{n}/{}_{d}$.

Proof:
Let $r = \mathrm{ord}(x^k)$. Then $x^{kr} = 1$, meaning $n \mid kr$. Since d divides both n and k, we thus have that $\frac{n}{d} \mid \frac{k}{d} r$. But $\gcd(\frac{n}{d}, \frac{k}{d}) = 1$ since $\gcd(n, k) = d$. So, we must have that $\frac{n}{d} \mid r$. Conversely, $(x^k)^{n/d} = (x^n)^{\frac{k}{d}} = 1$. So $r \mid \frac{n}{d}$. This means that $r = \frac{n}{d}$

If G is a group and $U \subseteq G$, one can form the subgroup $H = \langle U \rangle$ of G generated by U, meaning that H is the intersection of all subgroups of G containing U.

Some Example Groups:

- The Klein-4 Group consists of the matrices with the form: $\left[\begin{smallmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} \pm 1 & 0 \\ 0 & \mp 1 \end{smallmatrix}\right]$.
  It has four elements and is not cyclic.

- The Quaternion Group consists of the 8 elements in $\mathrm{GL}_2(\mathbb{C})$: $\pm\mathbf{1} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, $\pm\boldsymbol{I} = \left[\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right]$, $\pm\boldsymbol{J} = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$, and $\pm\boldsymbol{K} = \left[\begin{smallmatrix} i & 0 \\ 0 & i \end{smallmatrix}\right]$.

Proposition: Suppose $\varphi : G \longrightarrow G'$ is a group homomorphism. Then:

1. If $a_1, \cdots, a_k \in G_1$, then $\varphi(a_1 \cdots a_k) = \varphi(a_1) \cdots \varphi(a_2)$.
2. $\varphi(1_G) = 1_{G'}$
3. $\varphi(a^{-1}) = \varphi(a)^{-1}$

Proof:
(1) This is true by induction. For example:

$$\varphi(a_1 a_2 a_3) = \varphi(a_1 a_2)\varphi(a_3) = \varphi(a_1)\varphi(a_2)\varphi(a_3).$$

(2) $\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G)$. By multiplying $\varphi(1_G)^{-1}$ to both sides, we get that $\varphi(1_G) = 1_{G'}$.

(3) $1_{G'} = \varphi(1_G) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$. By multiplying $\varphi(a)^{-1}$ to both sides, we get that $\varphi(a)^{-1} = \varphi(a^{-1})$.

Suppose $\varphi : G \longrightarrow G'$ is a group homomorphism.

- The image of φ is: $\mathrm{im}(\varphi) = \varphi(G) = \{x \in G' \mid x = \varphi(a)$ for some $a \in G\}$.
- The kernel of φ is $\ker(\varphi) = \{x \in G \mid \varphi(x) = 1_{G'}\}$.

Proposition: Let $\varphi : G \longrightarrow G'$ be a group homomorphism. Then $\ker(\varphi) \subseteq G$ is a subgroup and $\mathrm{im}(\varphi)$ is a subgroup.

The kernel is a subgroup because if $\varphi(a) = 1_{G'} = \varphi(b)$, then $\varphi(ab) = 1_{G'}$. Also, if $\varphi(a) = 1_{G'}$, then $\varphi(a^{-1}) = \varphi(a)^{-1} = 1_{G'}$. And finally, $\varphi(1_G) = 1_{G'}$ as we showed earlier.

The image is subgroup because if $a', b' \in \mathrm{im}(\varphi)$, then there exists $a, b \in G$ with $\varphi(a) = a'$ and $\varphi(b) = b'$. Then $\varphi(ab) = a'b'$, meaning $a'b' \in \mathrm{im}(\varphi)$. Also, $\varphi(a^{-1}) = (a')^{-1}$, meaning $(a')^{-1} \in \mathrm{im}(\varphi)$. Finally, we know $1_{G'} \in \mathrm{im}(\varphi)$ because $\varphi(1_G) = 1_{G'}$.

Proposition: If $\rho_1 : G_1 \longrightarrow G_2$ and $\rho_2 : G_2 \longrightarrow G_3$ are group homomorphisms, then $\rho_2 \circ \rho_1 : G_1 \longrightarrow G_3$ is a group homomorphism.

Lecture 6 Notes: 10/9/2024

Let $b_1, \ldots, b_n$ be the standard basis of $\mathbb{R}^n$. Given any $\sigma \in S_n$, define a linear map $\rho(\sigma)$ on $\mathbb{R}^n$ such that $\rho(\sigma)(b_i) = b_{\sigma(i)}$. Or equivalently:

$$\rho(\sigma)(\alpha_1 b_1 + \ldots + \alpha_n b_n) = \alpha_{\sigma^{-1}(1)} b(1) + \ldots + \alpha_{\sigma^{-1}(n)} b(n)$$

Then ρ is a group homomorphism from S_n to $GL_n(\mathbb{R})$.

The proof for this is hopefully obvious.

Noting that $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ is a group homomorphism, given any $\sigma \in S_n$ we define the sign of the permutation: $\mathrm{sgn}(\sigma) = \det(\rho(\sigma))$. Note that by the proposition at the end of the last lecture, we know sgn is a group homomorphism.

Claim: $\mathrm{im}(\mathrm{sgn}) = \{1, -1\}$.

Proof:
Because S_n is finite, we know all $\sigma \in S_n$ have finite order. Thus, consider any $\sigma \in S_n$ with order k. Then we have that:

$$\sigma^k = 1 \Longrightarrow \rho(\sigma^k) = \rho(\sigma)^k = \rho(1).$$

In turn, $\det(\rho(\sigma)^k) = \det(\rho(\sigma))^k = \det(\rho(1))$. So $\mathrm{sgn}(\sigma)^k = 1$. But since $\mathrm{sgn}(\sigma) \in \mathbb{R}$, we must have that $\mathrm{sgn}(\sigma) = \pm 1$.

The kernel of the determinant homomorphism: $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ is called the special linear group $SL_n(\mathbb{R})$.

The kernel of the sign homomorphism $\mathrm{sgn} : S_n \longrightarrow \{-1, 1\}$ is called the alternating group: A_n. Also, we call the elements of A_n even permutations.

Suppose $H \subseteq G$ is a subgroup and $a \in G$. Then:

$$aH = \{g \in G \mid \exists h \in H \ s.t. \ g = ah\},$$

is called a left coset of H in G. One can similarly define a right coset Ha.

Proposition: Suppose $\varphi : G \longrightarrow G'$ is a group homomorphism, and let $K = \ker(\varphi)$. Then the following statements are equivalent for all $a, b \in G$:

1. $\varphi(a) = \varphi(b)$
2. $a^{-1}b \in K$
3. $b \in aK$
4. $aK = bK$

Proof:

$(1 \implies 2)$ If $\varphi(a) = \varphi(b)$, then:

$$\varphi(a^{-1}b) = \varphi(a^{-1})\varphi(b) = \varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = 1.$$

So $a^{-1}b \in K$.

$(2 \implies 3)$ If $a^{-1}b \in K$, then $b = a(a^{-1}b) \in aK$.

$(3 \implies 4)$ Suppose $b = ak$ for some $k \in K$. Then firstly, note that for all $c \in aK$, if $h \in K$ satisfies $c = ah$, then $c = akk^{-1}h = b(k^{-1}h)$. This shows that $aK \subseteq bK$. As for the other inclusion, note that $b = ak \implies a = bk^{-1}$. So $a \in bK$ and we can repeat the same reasoning as before.

This is actually a special case of the first corollary below.

$(4 \implies 1)$ If $aK = bK$, then we know there exists constants $k_1, k_2 \in K$ such that $ak_1 = bk_2$. In turn, $\varphi(a) = \varphi(ak_1) = \varphi(bk_2) = \varphi(b)$.

Lemma: Suppose $H \subseteq G$ is a subgroup, $x \in G$, and $g \in xH$. Then $xH = gH$.

Proof:

Let $g = xh'$ where $h_1 \in H$. Then $gh = xh'h \in xH$ for all $h \in H$. Hence, $gH \subseteq xH$. Conversely $x = g(h')^{-1}$. So $x \in gH$ and we can do the same reasoning as before to show that $xH \subseteq gH$.

Corollary: Suppose $H \subseteq G$ is a subgroup and $x, y \in G$. If $xH \cap yH \neq \emptyset$, then $xH = yH$.

Proof:

Suppose $xh_1 = g = yh_2$ with $h_1, h_2 \in H$. Then $xH = gH = yH$ by the previous lemma.

Corollary: A group homomorphism $\varphi : G \longrightarrow G'$ is injective if and only if its kernel is trivial (i.e. $\ker(\varphi) = \{1\}$).

Proof:

The forward implication is trivial by the definition of injectivity. As for the reverse implication, suppose $\ker(\varphi) = \{1\}$. Then:

$$\varphi(a) = \varphi(b) \implies a^{-1}b \in \ker(\varphi) = \{1\} \implies a^{-1}b = 1.$$

It follows that $a = b$.

Suppose G is a group and $a, g \in G$. Then gag^{-1} is called the conjugate of a by g.

Suppose G is a group and $N \subseteq G$ is a subgroup. The subgroup N is normal if $gng^{-1} \in N$ for all $n \in N$ and $g \in G$.

Proposition: Suppose $\varphi : G \longrightarrow G'$ is a group homomorphism. Then $\ker(\varphi) \subseteq G$ is a normal subgroup.

Proof:
Suppose $a \in \ker(\varphi)$ and $g \in G$. Then $gag^{-1} \in \ker(\varphi)$ because:

$$\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1$$

Lecture 7 Notes: 10/11/2024

You already know what an abelian group is. Note that every subgroup of an abelian group is normal because $ga = ag \Longrightarrow gag^{-1} = a$

Given a group G, define $Z(G) \coloneqq \{z \in G \mid zx = xz \text{ for all } x \in G\}$, Then $Z(G)$ is a normal subgroup of G called the center of G.

Proof that $Z(G)$ is a subgroup:

We know $1 \in Z(G)$.
Also if $z \in Z(G)$, then for all $x \in G$ we have that:

$$zx = xz \Rightarrow z^{-1}zxz^{-1} = z^{-1}xzz^{-1} \Rightarrow xz^{-1} = z^{-1}x.$$

Finally if $y, z \in Z(G)$, then for all $x \in G$ we have that:

$$(zy)x = z(yx) = z(xy) = (zx)y = (xz)y = x(zy)$$

Suppose $n \in \mathbb{Z}_+$. Then $\mu_n = \{z \in \mathbb{C}^\times \mid z^n = 1\}$ is a subgroup under complex multiplication. (μ_n is called the nth roots of unity.)

Note that the elements of μ_n are all the numbers of the form $e^{\frac{2\pi i a}{n}}$ where $a \in \mathbb{Z}$.

Also, μ_n has n elements and is cyclic (it is generated by $e^{\frac{2pi}{n}}$). This shows that for all $n \in \mathbb{Z}_+$ there is a cyclic group with n elements.

Examples of group isomorphisms: (I'm skipping writing down most of these cause they're not interesting)

Let G be an arbitrary group and $g \in G$. Then define $\rho_g : G \longrightarrow G$ such that $\rho_g(x) = gxg^{-1}$. Then ρ_g is a group isomorphism.

Proof:

- Homomorphism: $\rho_g(a)\rho_g(b) = gag^{-1}gbg^{-1} = gabg^{-1} = \rho_g(ab)$.
- Surjectivity: given $y \in G$, set $x = g^{-1}yg$. Then $\rho_g(x) = y$.
- Injectivity: $gag^{-1} = gbg^{-1} \Rightarrow g^{-1}gag^{-1}g = g^{-1}gbg^{-1}g \Rightarrow a = b$.

Fix a positive integer n and let a be an integer with $\gcd(a, n) = 1$. Then define $\varphi_a : \mu_n \longrightarrow \mu_n$ by $\varphi_a(\zeta) = \zeta^a$. This is an isomorphism.

Proof:

- homomorphism: since multiplication in $\mathbb{C}$ is commutative,
$$\varphi_a(\zeta_1\zeta_2) = (\zeta_1\zeta_2)^a = \zeta_1^a\zeta_2^a = \varphi_a(\zeta_1)\varphi_a(\zeta_2).$$
- Bijectivity: we know there exists $r, s \in \mathbb{Z}$ such that $ar + ns = 1$. So define $\varphi_r : \mu_n \longrightarrow \mu_n$. Then note that: $\varphi_r(\varphi_a(\zeta)) = \zeta^{ar} = \varphi_a(\varphi_r(\zeta))$ and $\zeta^{ar} = \zeta^{1-ns} = \zeta(\zeta^n)^{-s} = \zeta \cdot 1^{-s} = \zeta$. So, $\varphi_r = \varphi_a^{-1}$. Hence, φ_a is bijective.

If two groups are isomorphic, we write $G \approx G'$.

An isomorphism from a group G to itself is called an automorphism.

Two elements x, y of a group G are conjugate if there exists $g \in G$ such that $y = gxg^{-1}$.

Conjugates behave similar. For example, conjugates have the same order.

Lemma: Suppose $n \geq 1$ is an integer and $C_n = \langle x \rangle$ is a cyclic group generated by an element $x \in C_n$ (to be clear, this notation tells us that C_n has n elements). Suppose G is also a group and $y \in G$ satisfies that $y^n = 1$. Then there is a unique group homomorphism $\varphi : C_n \longrightarrow G$ with $\varphi(x) = y$.

Proof:
Define $\varphi(x^k) = y^k$ for all $k \in \mathbb{Z}$. This is well defined because $x^r = x^s \implies r - s \in n\mathbb{Z}$. So given that $x^r = x^s$, there exists $q \in \mathbb{Z}$ with $r = s + qn$ and $y^r = y^{s+qn} = y^s(y^n)^q = y^s$.

Having shown that this is well-defined, it's now trivial to see this is a group homomorphism.
$$\varphi(x^jx^k) = \varphi(x^{j+k}) = y^{j+k} = y^jy^k = \varphi(y^j)\varphi(y^k)$$

It should also be noted that φ is unique. This is because the fact that φ is a homomorphism means that $\varphi(x^k) = \varphi(x^{k-1})\varphi(x) = \ldots = (\varphi(x))^k = y^k$.

Proposition: Suppose $G = \langle x \rangle$ and $G' = \langle y \rangle$ are both cyclic of size n. Then G is isomorphic to G'.

Proof:
Let $\varphi : G \longrightarrow G'$ be the group homomorphism with $\varphi(x) = \varphi(y)$. It is clearly sujective, and since both G and G' have n elements, it must also be injective.

Corollary: Every cyclic group of size n is isomorphic to μ_n.

In a similar fashion, we can show every infinite cyclic group to be isomorphic to the integers $\mathbb{Z}$. (Note on notation: if I just write $\mathbb{Z}$, $\mathbb{R}$, or $\mathbb{C}$, assume I'm refering to the groups under addition.)

Proof that $\mathbb{R}$ is not isomorphic to $\mathbb{R}^\times$.

Suppose $\rho : \mathbb{R} \longrightarrow \mathbb{R}^\times$ is a group homomorphism. Then $\rho(x) = \rho(\frac{x}{2} + \frac{x}{2}) = \rho(\frac{x}{2})^2 > 0$. So $\rho(x) > 0$ for all x.

Lecture 8 Notes: 10/14/2024

Homework 1: Due 10/8/2024

1. Let S be a set with an associative law of composition and with an identity element. Let $G = \{x \in S \mid x \text{ has an inverse}\}$. Prove that G is a group with the law of composition from S.

   I'll be using multiplicative notation for composition on S. Firstly, to prove that the law of composition on S is closed over G, suppose $a, b \in G$, meaning there exists $a^{-1}, b^{-1} \in S$ which are inverses of a and b respectively. Then since $\cdot$ is associative on S, we know that $(b^{-1}a^{-1})ab = 1 = ab(b^{-1}a^{-1})$. So ab also has an inverse, meaning ab.

   Next, since 1 is its own inverse, we know $1 \in G$. Also, if $x \in G$, meaning that there exists $x^{-1} \in S$, then $(x^{-1})^{-1} = x$. So $x^{-1} \in G$ as well. Finally, we know that the law of composition on G is associative because we assumed it was associative on S. Hence, we've shown that $(G, \cdot)$ is a group.

2. Let $\mathrm{SL}_2(\mathbb{Z}) = \{\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mid a, b, c, d \in \mathbb{Z} \text{ and } \det(\gamma) = 1\}$. Prove that multiplication of matrices makes $\mathrm{SL}_2(\mathbb{Z})$ a group.

   To start, let's show that $\mathrm{SL}_2(\mathbb{Z})$ is closed under matrix multiplication.

   Suppose $\gamma_1 = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ and $\gamma_2 = \left[\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right]$ are elements of $\mathrm{SL}_2(\mathbb{Z})$. Then $\gamma_1\gamma_2 = \left[\begin{smallmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{smallmatrix}\right]$. Since the integers are closed under addition and multiplication, we know that all the elements of $\gamma_1\gamma_2$ are integers. Also, a fact from linear algebra is that $\det(\gamma_1\gamma_2) = \det(\gamma_1)\det(\gamma_2) = 1^2 = 1$. Hence $\gamma_1\gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$.

   If you don't trust that fact about determinants, then you can expand out the expression $(ae + bg)(cf + dh) - (ce + dg)(af + bh)$ yourself. Four of the terms cancel out and the other four can be factored as $(ad - bc)(eh - gf) = \det(\gamma_1)\det(\gamma_2)$.

   Next, observe that $\mathrm{SL}_2(\mathbb{Z})$ satisfies the rules of a group.

   1. $\mathbf{1} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ is a multiplicative identity element in $\mathrm{SL}_2(\mathbb{Z})$ since $\det(\mathbf{1}) = 1$.
   2. If $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then γ^{-1} exists and is in $\mathrm{SL}_2(\mathbb{Z})$.

      To start, we know that the matrix γ^{-1} exists because $\det(\gamma) \neq 0$. Also, note that:

      $$1 = \det(\mathbf{1}) = \det(\gamma\gamma^{-1}) = \det(\gamma)\det(\gamma^{-1}) = 1 \cdot \det(\gamma^{-1})$$

      Finally, if $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, then we know that $\gamma^{-1} = \frac{1}{\det(\gamma)}\left[\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right]$. Since $\det(\gamma) = 1$ and $a, b, c, d \in \mathbb{Z}$, this tells us that all the elements of γ^{-1} are integers.

We conclude that $\gamma^{-1} \in \mathrm{SL}_2(\mathbb{Z})$.

3. Matrix multiplication is associative on $\mathrm{SL}_2(\mathbb{Z})$ because it's associative on $\mathcal{M}(2, \mathbb{R})$.

3. A group homomorphism $\rho : G_1 \longrightarrow G_2$ is said to be *trivial* if $\rho(g) = 1$ for all $g \in G_1$. Otherwise, the homomorphism is said to be *nontrivial*. If $\mathbb{R}$ is the group of real numbers under addition and $\mathbb{R}^\times$ is the group of nonzero real numbers under multiplication, then find a non-trivial homomorphism $\rho : \mathbb{R} \longrightarrow \mathbb{R}^\times$.

Given any $\alpha \in \mathbb{R}$ such that $\alpha > 0$, define $\rho(x) = \alpha^x$ for all $x \in \mathbb{R}$. Note that $\rho(x) \neq 0$ for all $x \in \mathbb{R}$, meaing $\rho(x) \in \mathbb{R}^\times$ for all $x \in \mathbb{R}$. Then for all $x, y \in \mathbb{R}$, we have that:

$$\rho(x + y) = \alpha^{x+y} = \alpha^x \alpha^y = \rho(x)\rho(y)$$

Homework 2:

1. (Chapter 2, Problem 4.1) Let a and b be elements of a group G. Suppose that a has order 7 and $a^3 b = ba^3$. Prove that $ab = ba$.

Since $ba^3 = a^3 b$ and $a^7 = 1$, we have that:

$$b = a^3 ba^4 = a^3(ba^3)a = a^3(a^3 b)a = a^6 ba.$$

Composing both sides by a on the left, we get that $ab = 1ba = ba$.

2. (Chapter 2, Problem 4.3) Let a and b be elements of a group G. Prove that ab and ba have the same order.

Suppose n is the least positive integer for which $(ab)^n = 1$. Then note that $(ba)^k = b(ab)^{k-1}a$ for all $k \in \mathbb{Z}_+$. So, $(ba)^{n+1} = b(ab)^n a = ba$, which in turn means $(ba)^n = 1$. Also, from an earlier proposition, we know $(ab)^k = (ab)^{-1} = b^{-1}a^{-1}$ if and only if $k + 1 = n$. So n is the least positive integer for which $(ab)^n = 1$.

3. (Chapter 2, Problem 4.4) Suppose G is group that contains no proper (nontrivial) subgroup. Prove G is finite and has order 1 or order p where p is prime.

To start, obviously a trivial group contains no proper subgroup. So, we'll now assume that $\exists x \in G$ such that $x \neq 1$. We know that the cyclic group $\langle x \rangle$ is a nontrivial subgroup of G. Therefore, by our assumption about G, we know that $\langle x \rangle = G$.

Suppose x has infinite order. Then we have a contradiction because $\langle x^2 \rangle$ is a subgroup of $\langle x \rangle = G$ which doesn't contain $x \in G$ (by a previous proposition, if 0 is the only integer for which $x^0 = 1$, then $x^k = x^1 \Rightarrow k = 1$).

So, we know x has finite order $p \in \mathbb{Z}_+$. Furthermore, since $\langle x^k \rangle = G$ for all $k \in \mathbb{Z}_+$ by assumption, we know that x^k must also have order p for all $k \in \mathbb{Z}_+$. But by a previous proposition, we know that x^k has order $\frac{p}{\gcd(p,k)}$. So, if k is not a multiple of p, we must have that $\gcd(p,k) = 1$. Thus, p is coprime with every positive integer less than it, meaning that p must be prime.

Hence, if G is nontrivial, it must have a prime number of elements.

4. (Chapter 2, Problem 4.10) Suppose G is a group and $a, b \in G$ have finite order.

   (a) Suppose G is abelian. Then ab has finite order.

   Suppose a and b have orders n and m respectively. Then becaues G is abelian:

$$(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = 1^m1^n = 1$$

   So, the set of integers N such that $(ab)^N = 1$ contains a nonzero element.

   (b) Show by example that if G is not abelian, then ab need not have finite order.

   Consider the group of bijective functions on $\mathbb{Z}$ with function composition as it's rule of composition. Then define the functions:

$$f(n) = |n| \text{ and } g(n) = \begin{cases} n-1 & \text{if } n \text{ is even} \\ n+1 & \text{if } n \text{ if odd} \end{cases}$$

   Using multiplicative notation, we clearly have that $f^2 = 1 = g^2$. On the other hand, we can by induction show that $(fg)^N(1) \neq 1$ for all $N \in \mathbb{Z}_+$.

   Proof:

   - If n is odd and positive, then $fg(n) = f(n+1) = -n-1$ which is negative, even, and satisfies that $|fg(n)| > |n|$.
   - If n is even and negative, then $fg(n) = f(n-1) = -n+1$ which is positive, odd, and satisfies that $|fg(n)| > |n|$

   Since 1 is a positive odd number, we know that those will be the only two cases we run into when composing fg with itself. It follows that $(fg)^N(1) \neq 1$ for any $N \in \mathbb{Z}_+$ since $|(fg)^N(1)| \neq 1$ for any N.

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