Math 100A Notes (Professor: Aaron Pollack)

Isabelle Mills

October 29, 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 $\bigcap_{\alpha \in A} H_\alpha$ 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:

$$\varphi(a_1a_2a_3) = \varphi(a_1a_2)\varphi(a_3) = \varphi(a_1)\varphi(a_2)\varphi(a_3).$$

(2) $\varphi(1_G) = \varphi(1_G1_G) = \varphi(1_G)\varphi(1_G)$. 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: $\text{im}(\varphi) = \varphi(G) = \{x \in G' \mid x = \varphi(a) \text{ for some } a \in G\}$.
- 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 $\text{im}(\varphi)$ 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 $a', b' \in \text{im}(\varphi)$, then there exists $a, b \in G$ with $\varphi(a) = a'$ and $\varphi(b) = b'$. Then $\varphi(ab) = a'b'$, meaning $a'b' \in \text{im}(\varphi)$. Also, $\varphi(a^{-1}) = (a')^{-1}$, meaning $(a')^{-1} \in \text{im}(\varphi)$. Finally, we know $1_{G'} \in \text{im}(\varphi)$ 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: $\text{sgn}(\sigma) = \det(\rho(\sigma))$. Note that by the proposition at the end of the last lecture, we know sgn is a group homomorphism.

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

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 $\text{sgn}(\sigma)^k = 1$. But since $\text{sgn}(\sigma) \in \mathbb{R}$, we must have that $\text{sgn}(\sigma) = \pm 1$.

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 $\text{sgn} : S_n \longrightarrow \{-1, 1\}$ 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. Then analogous theorems can be proven.

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 $h' \in H$. 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 $ga = ag \implies gag^{-1} = a$

Given a group G, define $Z(G) := \{z \in G \mid zx = xz \text{ for all } x \in G\}$, 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 $e^{\frac{2\pi ia}{n}}$ 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 $G \cong G'$.

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 $x^r = x^s \Longrightarrow r - s \in n\mathbb{Z}$. 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

I already know what partitions, equivalence relations, and equivalence classes are.

Examples: Let G be a group and $H \subseteq G$ is a subgroup.

- The collection of cosets of H in G is a partition of G.

  To see why look at the second lemma on page 10.

- Define $a \sim b$ if $\exists h \in H$ so that $b = ah$. Then $\sim$ is an equivalence relation.

  To see why:

  - $1 \in H \Rightarrow a = a1 \Rightarrow a \sim a$
  - $a \sim b \Rightarrow \exists h \in H \ s.t. \ b = ah \Rightarrow a = bh^{-1} \Rightarrow b \sim a$
  - $a \sim b \sim c \Rightarrow \exists h_1, h_2 \in H \ s.t. \ b = ah_1, \ \ c = bh_2 \Rightarrow c = ah_1h_2 \Rightarrow a \sim c$

- Define $a \sim b$ if b is conjugate to a. Then $\sim$ is an equivalence relation.

  To see why:

  - $a = 1a1^{-1} \Rightarrow a \sim a$
  - $a \sim b \Rightarrow \exists g \in G \ s.t. \ a = gbg^{-1} \Rightarrow b = g^{-1}a(g^{-1})^{-1} \Rightarrow b \sim a$
  - $a \sim b \sim c \Rightarrow \exists g, h \in G \ s.t. \ b = gag^{-1}, \ \ c = hbh^{-1}$. So:
    $$c = hgag^{-1}h^{-1} = (hg)a(hg)^{-1} \Rightarrow a \sim c$$

- If $f : S \longrightarrow T$ is a map of sets define $a \sim b$ if $f(a) = f(b)$.

Suppose S is a set with an equivalent relation $\sim$. Given $a \in S$, we denote the equivalence class of a as C_a.

We define the quotient set $\overline{S}$ to be the set whose elements are the equivalence classes C_a of $\sim$ on S.

Suppose $\varphi : G \longrightarrow G'$ is a group homomorphism. If $a, b \in G$, we write $a \equiv b$ if $\varphi(a) = \varphi(b)$. Note that letting $K = \ker(\varphi)$, we have that $a \equiv b$ if and only if $aK = bK$. So $\equiv$ is an equivalence relation.

Given a group G and subgroup H, we denote G/H for the set of cosets of H. The index of a subgroup H of a group G is the number of left cosets of H in G. It is denoted $[G : H]$.

Lemma 3w5: Let H be a subgroup of a group G. Then every left coset of H in G has the same cardinality.

Proof:
Suppose xH and yH are two cosets. Define $f : xH \longrightarrow yH$ as $f(g) = yx^{-1}g$. Then f is a bijection.

Theorem 3w6: Suppose G is a finite group and H is a subgroup of G. Then $|G| = [G : H]|H|$.

Since each coset is disjoint and has the same cardinality, this is pretty trivial.

Lagrange's theorem If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.

Corollary 3w8: Suppose G is a finite group and $g \in G$. Then the order of g divides $|G|$.

Proof:
Let $H = \langle g \rangle$ and apply Lagrange's theorem.

Corollary 3w9: Suppose p is a prime integer and G is a group of order p. Let a be an element of G distinct from the identity. Then all of G is the cyclic group generated by a.

Proof:
Let $H = \langle a \rangle$. Then by Lagrange's theorem, we know $|H|$ divides $|G| = p$. But $|H| \neq 1$. So $|H| = p$.

Lecture 9 Notes: 10/16/2024

Lemma 3w10: Suppose $\varphi : G \longrightarrow G'$ is a group homomorphism. Then $|\operatorname{im}(\varphi)| = [G : \ker \varphi]$.

Proof:
Let $K = \ker(\varphi)$. Then $\varphi(a) = \varphi(b)$ if and only if $aK = bK$. So, there is a bijective correspondance between the left cosets of K and $\operatorname{im}(\varphi)$.

Corollary 3w11: Let $\varphi : G \longrightarrow G'$ be a homomorphism of finite groups. Then:

1. $|G| = |\ker(\varphi)| \cdot |\operatorname{im}(\varphi)|$
2. $|\ker(\varphi)|$ divides $|G|$.
3. $|\operatorname{im}(\varphi)|$ divides $|G|$ and $|G'|$.

Proof:
Substituting in $[G : \ker(\varphi)] = |\operatorname{im}(\varphi)|$ into theorem 3w6, we get that $|G| = |\operatorname{im}(\varphi)| \cdot |\ker(\varphi)|$. The rest follows trivially from and Lagrange's theorem.

Theorem 3w12: Suppose $G \subseteq H \subseteq K$ with G being a finite group, H being a subgroup of G, and K being a subgroup of H. Then $[G : K] = [G : H][H : K]$.

Proof:
Suppose $[G : H] = m$ and $[H : K] = n$. Then there exists $g_i \in G$ and $h_j \in H$ satisfying that $G = g_1H \cup \ldots \cup g_mH$ and $H = h_1K \cup \ldots \cup h_mK$ where each union is of disjoint sets.

Now note that $\{g_ih_jK \mid j \in \{1, \ldots, n\}\}$ is a partition of g_iH. To prove this, note that given any $x \in g_iH$, there exists $h \in H$ such that $x = g_ih$. But note that for some h_j and $k \in K$, we have that $h = h_jk$. So $x \in g_ih_jk$ for some $h_j \in K$. At the same time, we can fairly trivially see that $g_ih_jK \subseteq g_iH$ for all j. And, we already showed that nonequal cosets are disjoint.

So, $G = \bigcup_{i=1}^{m} \bigcup_{j=1}^{n} g_ih_jK$.

Proposition 3w13: Let H be a subgroup of a group G. The following are equivalent.

1. H is normal.
2. $gHg^{-1} = H$ for all $g \in G$

   (It's fairly trivial to see that $(aH)b = a(Hb)$ for all $a, b \in G$).
3. $gH = Hg$ for all $g \in G$.
4. Every left coset of G is a right coset of G (and vice versa)

Proof:
(1) $\Longrightarrow$ (2)
If H is normal, then by definition $gHg^{-1}, g^{-1}Hg \subseteq H$. In turn, $H = g^{-1}(gHg^{-1})g \subseteq g^{-1}(H)g$. So $gHg^{-1} = H$.

(2) $\Longrightarrow$ (1)
(2) $\Longleftrightarrow$ (3)
(3) $\Longrightarrow$ (4)
These are trivial.

(4) $\Longrightarrow$ (1)
Suppose $gH = Hg'$. Then $g \in Hg'$ because $g = g1 \in gH$. So, $Hg = Hg' = gH$.

Proposition 3w14: Suppose G is a group.

1. If $g \in G$ and H is a subgroup of G, then gHg^{-1} is a subgroup of G.
2. If G has one subgroup of order r, that subgroup is normal.

Conjugation by g is a group automorphism. So the image (which equals gHg^{-1}) of that homomorphism restricted to H is a subgroup of G.

The other claim comes from the fact that if $|H| = |gHg^{-1}|$. So if G only has one subgroup of order r and H is a subgroup of order r, then $|gHg^{-1}| = r$ implies that $gHg^{-1} = H$.

Modular Arithmetic

One says two integers a, b are equivalent modulo n if $a + n\mathbb{Z} = b + n\mathbb{Z}$. This is the same as saying $a - b \in n\mathbb{Z}$. One writes $a \equiv b \pmod{n}$.

Proposition 3w16: Suppose $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$. Then:

- $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$
- $a_1 a_2 \equiv b_1 b_2 \pmod{n}$

Proof:
We know $b_1 = a_1 + k_1 n$ and $b_2 = a_2 K k_2 n$ for some integers k_1, k_2. Thus:

- $b_1 + b_2 = a_1 + a_2 + (k_1 + k_2)n$
- $b_1 b_2 = a_1 a_2 + a_1 k_2 n + a_2 k_1 n + k_1 k_2 n^2 = a_1 a_2 + (a_1 k_2 + a_2 k_1 + k_1 k_2 n)n$

Fixing n, then given $a \in \mathbb{Z}$, we denote it's equivalence class $\overline{a} = a + n\mathbb{Z}$. (specifically $a + n\mathbb{Z}$ is a coset of $n\mathbb{Z}$). Note that $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Given $\overline{a}$ and $\overline{b}$ in $\mathbb{Z}/n\mathbb{Z}$, we define $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$. This is well defined by the previous proposition.

Proposition 3w17: Fix a positive integer n,

- Addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ is commutative and associative.
- Multiplication in $\mathbb{Z}/n\mathbb{Z}$ distributes over addition.
- The class $\overline{0}$ is an identity for addition, and every element of $\mathbb{Z}/n\mathbb{Z}$ has an additive inverse.
- The class $\overline{1}$ is an identity for multiplication.

This all follows from the fact that $\mathbb{Z}$ has these properties.

Proposition 3w18: The set $\mathbb{Z}/n\mathbb{Z}$ with law of composition being addition is a group. It is cyclic of order n.

This is because it is generated by $\overline{1}$.

Note that the map $\rho : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mu_0$ given by $\rho(a + n\mathbb{Z}) = e^{\frac{2\pi i a}{n}}$ is an isomorphism.

Let $(\mathbb{Z}/n\mathbb{Z})^\times$ be the set of all $x \in \mathbb{Z}/n\mathbb{Z}$ with multiplicative inverses.

Lemma 3w20: Suppose $n \in \mathbb{Z}$ is nonzero and $a \in \mathbb{Z}$. Then there exists $b \in \mathbb{Z}$ so that $ab \equiv 1 \pmod{n}$ if and only if $\gcd(a, n) = 1$.

Proof:
If b exists, then $ab = 1 + kn$ for some $k \in \mathbb{Z}$. So, $ab - kn = 1$, meaning $\gcd(a, n) = 1$. You can just flip that reasoning to get the other direction implication.

Proposition 3w21: The set $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group under multiplication.

Proof:
This is a special case of homework 1 problem 1.

Corollary 3w22: If p is a prime number, the size of $(\mathbb{Z}/p\mathbb{Z})^\times$ is $p-1$. Consequently if $p \not| a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof:
The first part is just applying lemma 3w20. To get the second part, note that the order of a must divide $p-1$. If $|\langle a \rangle| = \frac{p-1}{d}$, then it follows that:

$$(a^{\frac{p-1}{d}})^d \equiv a^{p-1} \equiv 1 \pmod{p}.$$

Hence, $a^{p-1} \equiv 1 \pmod{p}$ for all $a \in (\mathbb{Z}/p\mathbb{Z})^\times$.

More generally, we define $\varphi(n) = |\{x \in \mathbb{Z} \mid 1 \leq x < n \text{ and } \gcd(x,n) = 1\}|$. This is called Euler's totient function. Then:

Corollary 3w23: Suppose $\gcd(a,n) = 1$. Then the size of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$ and $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Now if you are paying attention, the group of integers under addition module n can be thought of as a special case of the more general theory below.

Suppose G is a group and N is a normal subgroup. we define $\overline{G} = G/N$. And if $a \in G$, we define $\overline{a} = aN \in G/N$.

Let $\pi : G \longrightarrow \overline{G}$ denote the surjective map $\pi(a) = \overline{a}$ (this is the canonical map).

Theorem 3w24: There is a law of composition on $\overline{G}$ that makes it into a group such that $\pi : G \longrightarrow \overline{G}$ is a surjective group homomorphism whose kernel is N.

Proof:
Lemma 3w25: The formula $(aN)\cdot(bN) = (abN)$ is a well-defined law of composition on $\overline{G}$.

Proof: Suppose $a' = an_1$ and $b' = bn_2$. Then:

$$a'b' = an_1bn_2 = a(bb^{-1})n_1bn_2 = ab(b^{-1}n_1b)n_2 \in abN$$

This works because $b^{-1}n_1b \in N$ since N is normal.

Lemma 3w26: Given the law of composition defined above and the set $\overline{G}$, we have the following:

1. The set $1N = N$ is an identity for the law of composition on $\overline{G}$.
2. The inverse of aN is $a^{-1}N$.
3. The law of composition on $\overline{G}$ is associative.

Proof:
All of these follow directly from the the fact that G is a group.

Now that we know that $\overline{G}$ is a group when equipped with the above law of composition, it's pretty clear that π is a surjective group homomorphism. All that's left to do now is show that $\ker(\pi) = N$. To do this, note that $\pi(a) = aN = 1N$ if and only if $a \in N$.

First Isomorphism Theorem: Let $\varphi : G \longrightarrow G'$ be a group homomorphism with kernel N, and let $\pi : G \longrightarrow \overline{G} = G/N$ be the canonical map. Then there is a unique group homomorphism $\overline{\varphi} : \overline{G} \longrightarrow G'$ for which $\varphi = \overline{\varphi} \circ \pi$. The map $\overline{\varphi} : \overline{G} \longrightarrow \varphi(G)$ is an isomorphism.

Proof:
Note that by a proposition on page 11, we know that N is normal.

- **Uniqueness:** In order for $\varphi = \overline{\varphi} \circ \pi$, we must have that $\overline{\varphi}(\overline{a}) = \varphi(a)$. Thus, if $\overline{\varphi}$ exists, then it is unique.
- **Well-defined:** Define $\overline{\varphi}(aN) = \varphi(a)$. THis is well-defined as $\varphi(an) = \varphi(a)$ due to $n \in \ker(\varphi)$.
- **Group homomorphism:**
$$\overline{\varphi}((aN)(bN)) = \overline{\varphi}(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(aN)\overline{\varphi}(bN).$$
- **Isomorphism:** $\overline{\varphi}$ is injective because $\overline{\varphi}(aN) = \varphi(a) = 1$ implies that $a \in N$. So the kernel is trivial. Also, the image of $\overline{\varphi}$ is $\varphi(G)$.

Some applications of the above theorem:

- The quotient of $GL_n(\mathbb{R})$ by the normal subgroup $SL_n(\mathbb{R})$ is isomorphic to $\mathbb{R}^\times$.
- There's a longer problem here that I'm skipping for now. Maybe I'll cover it on page ___.

Suppose G, H are groups. One can define a law of composition on $G \times H$ as $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Proposition 3w28: This makes $G \times H$ a group. The identity is $(1, 1)$ and the inverse of $(g, h) = (g^{-1}, h^{-1})$.

If R is a group and $\varphi_1 : R \longrightarrow G$ and $\varphi_2 : R \longrightarrow G$ are group homomorphisms, then $\varphi : R \longrightarrow G \times H$ given by $\varphi(r) = (\varphi_1(r), \varphi_2(r))$ is a group homomorphism.

Hopefully this is obvious. So I'm not proving this.

Lemma 3w29: Suppose m, n are positive integers with m dividing n. Then the map $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ sending $a + n\mathbb{Z}$ to $a + m\mathbb{Z}$ is a well-defined surjective group homomorphism.

Proof:
To start, note that this is well defined because if $a \in b + n\mathbb{Z}$, then we know $a = b + nr$ for some $r \in \mathbb{Z}$. Then since $n = md$ for some $d \in \mathbb{Z}$, it follows that $a = b + m(dr) \in b + m\mathbb{Z}$. In other words, $a \in b + n\mathbb{Z} \Longrightarrow a + m\mathbb{Z} = b + m\mathbb{Z}$.

To see that this is a group homomorphism, just note that:
$(a+nr)+(b+ns) = (a+m(dr))+(b+m(ds)) = (a+b)+m(dr+ds) = (a+b)+n(r+s)$

Finally, it's pretty trivial to see that this is surjective.

Lecture 11 Notes: 10/21/2024

Chinese Remainder Theorem: Suppose r, s are coprime positive integers. Then the map $\mathbb{Z}/(rs)\mathbb{Z} \longrightarrow (\mathbb{Z}/r\mathbb{Z}) \times (\mathbb{Z}/s\mathbb{Z})$ given by $n + rs\mathbb{Z} \mapsto (n + r\mathbb{Z}, n + s\mathbb{Z})$ is an isomorphism.

Proof:
Here is an equivalent statement: Suppose r, s are coprime positive integers. Then the map $\mathbb{Z} \longrightarrow (\mathbb{Z}/r\mathbb{Z}) \times (\mathbb{Z}/s\mathbb{Z})$ sending $n \in \mathbb{Z}$ to $(n + r\mathbb{Z}, n + s\mathbb{Z})$ is surjective with $(rs)\mathbb{Z}$ as it's kernel.

Proof:
To start, note that the maps $\mathbb{Z} \longrightarrow \mathbb{Z}/r\mathbb{Z}$ and $\mathbb{Z} \longrightarrow \mathbb{Z}/s\mathbb{Z}$ such that $a \mapsto a + r\mathbb{Z}$ and $a \mapsto a + s\mathbb{Z}$ respectively are both group homomorphisms. Combining this with what was discussed on the last page, we know that the map sending $n \in \mathbb{Z}$ to $(n + r\mathbb{Z}, n + s\mathbb{Z})$ is a group homomorphism.

Side note: under additive notation, the law of composition of the product $G \times H$ of two groups G and H is:
$$(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2).$$

Now since $\gcd(r, s) = 1$, there exists $a, b \in \mathbb{Z}$ such that $ar + bs = 1$. Now set $u = bs$ and $v = ar$. Then note that $u \mapsto (1, 0)$ and $v \mapsto (0, 1)$. It follows that $xu + yv = (x + r\mathbb{Z}, y + s\mathbb{Z})$. So the map is surjective.

Meanwhile, note that if $r \mid n$ and $s \mid n$, then we can say that $s \mid r(\frac{n}{r})$. But now note that since $\gcd(s, r) = 1$, we must have that $s \mid \frac{n}{r}$. So, $rs \mid n$. Similarly, if $rs \mid n$, we obviously have that $r \mid n$ and $s \mid n$. So it follows that the kernel of this map is $(rs)\mathbb{Z}$.

Now the reason why this statement is equivalent to the original is that we can now use the first isomorphism theorem to state that our original map from $\mathbb{Z}/(rs)\mathbb{Z}$ to $(\mathbb{Z}/r\mathbb{Z}) \times (\mathbb{Z}/s\mathbb{Z})$ is an isomorphism.

Lemma 4w4: Suppose $\varphi : G \longrightarrow G'$ is a group homomorphism, and let $H' \subseteq G'$ be a subgroup. Let $H = \varphi^{-1}(H')$. Then:

1. H is a subgroup of G that contains $\ker(\varphi)$.

   Proof:
   We know $1 \in H$. Also, if $h \in H$, then $\varphi(h^{-1}) = \varphi(h)^{-1} \in H'$. So $h^{-1} \in H$. Finally, if $h_1, h_2 \in H$, then $\varphi(h_1 h_2) = \varphi(h_1)\varphi(h_2) \in H'$. So, $h_1 h_2 \in H$.

   Also, the fact that $\ker(\varphi) \subseteq H$ is just because $1 \in H'$.

2. If H' is normal, then so is H.

   Proof:
   We know that $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} \in H'$ for all $h \in H$ and $g \in G$. So, $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$.

3. If H is normal and φ is surjective, then H' is normal.

   Fuck you, do this proof yourself. It's not that hard.

Theorem 4w5: Let $\varphi : G \longrightarrow G'$ be a surjective group homomorphism with kernel K.

1. There is a bijective correspondance between subgroups of G' and subgroups of G containing K. The correspondence is $H \mapsto \varphi(H)$ for $H \subseteq G$ and $H' \mapsto \varphi^{-1}(H')$ for $H' \subseteq G'$.

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:

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

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 $n = 0$ is the only integer for which $x^n = 1$, then $x^k = x^1 \Rightarrow k = 1$).

So, we know x has finite order $p \in \mathbb{Z}_+$. Furthermore, for all $k \in \mathbb{Z}_+$, we know that if $x^k \neq 1$, then by our assumption about G we have that $\langle x^k \rangle = G$ and thus x^k must also have order p. But by a previous proposition, we know that x^k has order $\frac{p}{\gcd(p,k)}$. So, p must be coprime with all positive integers less than p, meaning that p is 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:

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

   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 consider the bijections on $\mathbb{Z}$:

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

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

   So, (fg) has infinite order.

5. (Chapter 2, Problem 5.1) Let $\varphi : G \longrightarrow G'$ be a surjective group homomorphism.

   (a) A group is called cyclic if $G = \langle x \rangle$ is generated by a single element $x \in G$. Prove that if G is cyclic, then G' is cyclic.

   Suppose $x \in G$ generates G, and define $y = \varphi(x)$. Since φ is surjective, we know that given any $z \in G'$, there exists $k \in \mathbb{Z}$ with $\varphi(x^k) = z$. So:

   $$z = \varphi(x^k) = (\varphi(x))^k = y^k$$

   Thus, G' is cyclic and generated by y.

   (b) Prove that if G is abelian, then G' is abelian.

   Given any $a, b \in G'$, pick $a', b' \in G$ such that $\varphi(a') = a$ and $\varphi(b') = b$. Then $ab = \varphi(a')\varphi(b') = \varphi(a'b') = \varphi(b'a') = \varphi(b')\varphi(a') = ba$.

Homework 3:

1. (Chapter 2, Problem 8.3) Suppose p is a prime number and G is a group with order p^n for a positive integer n. Prove that G contains an element of order p.

   Since the order of any element of G must divide $|G|$, we have that if $|G| = p$ where p is prime, then the cyclic group of any non-identity element must have order p as well. Hence, this problem holds true when $n = 1$.

   Now suppose $|G| = p^N$ and assume the problem holds true for $n < N$. Choose a not equal to 1 in G, and consider the cyclic group $\langle a \rangle$. We know that $|\langle a \rangle|$ must divide p^N. And since the only factors of p^N have the form p^k where k is a nonnegative integer at most N, we know that $|\langle a \rangle| = p^k$ for some integer $0 \leq k \leq N$.

   If $k < N$, then we can apply our inductive hypothesis to say that there is an element of order p in $\langle a \rangle$ and thus in G.

   If $k = N$, then consider the cyclic group $\langle a^{(p^{N-1})} \rangle$ Note that $(a^{(p^{N-1})})^p = a^{(p^N)} = 1$. Also, for any integer $k \in \{1, \ldots, p-1\}$, we know that $0 < kp^{N-1} < p^N$, meaning $(p^{N-1})^k - 0$ is not a multiple of p^N. So, $a^{(p^{N-1})} \in G$ has order p.

2. (Chapter 2, Problem 8.5) Suppose G is a finite group and that G contains an element of order 10 and an element of order 6. Prove that $|G|$ is a multiple of 30.

   Since the order of any element of G must divide $|G|$, we know that both 10 and 6 must divide $|G|$. Importantly, letting $m = \operatorname{lcm}(6, 10)$, we know from a proposition in class that for any n satisfying that $10 \mid n$ and $6 \mid n$, we know that $m \mid n$. So m must divide $|G|$. And it just so happens that $m = \operatorname{lcm}(6, 10) = 30$.

3. (Chapter 2, Problem 8.6) Suppose $\varphi : G \longrightarrow G'$ is a group homomorphism, $|G| = 18$ and $|G'| = 15$. Assume that φ is not the trivial homomorphism. What is the order of $\ker(\varphi)$.

   We know that $|\ker(\varphi)| \cdot |\operatorname{im}(\varphi)| = |G'|$, and that $|\operatorname{im}(\varphi)| \neq 1$. As a result we know one of the following cases is true:

   - $|\ker(\varphi)| = 1$ and $|\operatorname{im}(\varphi)| = 18$
   - $|\ker(\varphi)| = 2$ and $|\operatorname{im}(\varphi)| = 9$
   - $|\ker(\varphi)| = 3$ and $|\operatorname{im}(\varphi)| = 6$
   - $|\ker(\varphi)| = 6$ and $|\operatorname{im}(\varphi)| = 3$
   - $|\ker(\varphi)| = 9$ and $|\operatorname{im}(\varphi)| = 2$

   But then note that taking into account that $|G'| = 16$, there is only one option above that satisfies that $|\operatorname{im}(\varphi)|$ divides 16. Hence, we know that:

   $$|\ker(\varphi)| = 9 \text{ and } |\operatorname{im}(\varphi)| = 2$$

4. (Chapter 2, Problem 8.10) Suppose G is a group and N is a subgroup of G of index 2. Prove that N is normal.

   Note that since $[G : N] = 2$ and $N = 1N$ is a coset of N, we know that the other coset must be $G \setminus N$.

   Now I'm running out of time and thus didn't have time to show this. But to be fully accurate, since we defined the index of a group to be based on the number of left cosets, we need to show that there are the same number of right and left cosets. At least if G is finite, then this is trivial (because all the reasoning we've done in class could just as easily have been done using right-cosets)

   So assuming that $[G : N]$ also gives the number of right cosets, then note that as before, we have that the right cosets of G are N and $G \setminus N$. So, every left coset of N is a right coset of N and vice versa. It follows that N is normal.

Homework 4:

1. Suppose $r_1, \ldots, r_n$ are positive integers. Say that the r_j are pairwise coprime if $\gcd(r_i, r_j) = 1$ for all $i \neq j$. Prove the following generalization of the Chinese Remainder Theorem: Assume the positive integers $r_1, \ldots, r_n$ are pairwise coprime. Then the canonical map:
$$\mathbb{Z}/(r_1 \cdots r_n)\mathbb{Z} \longrightarrow (\mathbb{Z}/r_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/r_n\mathbb{Z})$$
given by $a + r_1 \cdots r_n\mathbb{Z} \mapsto (a + r_1\mathbb{Z}, \ldots, a + r_n\mathbb{Z})$ is an isomorphism.

   We already proved the case where $n = 2$ in class. So, let's now proceed by induction.

   Firstly, observe that if r_n is coprime with $r_1, \ldots, r_{n-1}$, then we have that r_n is coprime with $r_1 \cdots r_{n-1}$. To see this, assume for the sake of contradiction that there exists $d \neq 1$ which divides both r_n and $r_1, \ldots, r_{n-1}$. Since r_n and r_1 are coprime, we know that $d \not| r_1$. Thus, $d \,|\, r_1(r_2 \cdots r_{n-1}) \Longrightarrow d \,|\, r_2 \cdots r_{n-1}$. Repeating this reasoning, we will eventually get that $d \,|\, r_{n-1}$. This contradicts that r_{n-1} and r_n are coprime.

   Thus, using the Chinese Remainder theorem, we know the canonical map $a + r_1 \cdots r_n\mathbb{Z} \mapsto (a + r_1 \cdots r_{n-1}\mathbb{Z}, a + r_n\mathbb{Z})$ is an isomorphism.

   By induction, we can say that the canonical map $a + r_1 \cdots r_{n-1}\mathbb{Z} \mapsto (a + r_1\mathbb{Z}, \ldots, a + r_{n-1}\mathbb{Z})$ is an isomorphism.

   It follows that the map below is an isomorphism:
$$(a + r_1 \cdots r_{n-1}\mathbb{Z}, a + r_n\mathbb{Z}) \mapsto (a + r_1\mathbb{Z}, \ldots, a + r_{n-1}\mathbb{Z}, a + r_n\mathbb{Z})$$

   And finally, since the composition of two group isomorphisms is itself a group isomorphism, we thus know that the map given by the problem is an isomorphism.

2. Suppose p is a prime number. Prove Wilson's Theorem: $(p-1)! \equiv -1 \pmod{p}$.

   Consider that if $a^2 \equiv 1 \pmod{p}$, then we must have that $a^2 - 1 = (a+1)(a-1) \equiv 0 \pmod{p}$. As a result, we know that p divides either $(a+1)$ or $(a-1)$. In the first case, we'd have that $a \equiv p - 1 \pmod{p}$. In the other case, we'd have that $a \equiv 1 \pmod{p}$.

   Now if $p = 2$, then the theorem is true because $(p-1)! = 1 \equiv -1 \pmod{2}$. So, we can now assume that $p - 1 \not\equiv 1 \pmod{p}$. Then note that $(p-1)! = (p-1)(p-2)\cdots(2) \equiv -1 \cdot (p-2)\cdots(2)$.

Now $(p-2)\cdots(2)$ consists of $p-3$ terms distinct from 1 and $p-1$. This is importantly an even number of terms. Also, each term will be the unique inverse of precisely one other term in that expansion because we've already shown that none of those terms are their own inverses. Hence, we can replace half of them with the inverses of the other half. And since $(\mathbb{Z}/p\mathbb{Z})^\times$ is abelian, we can rearrange terms to show their product is equivalent to 1 modulo p.

Thus, we conclude that $(p-1)! \equiv -1 \cdot (p-2)\cdots(2) \equiv -1$.

3. Suppose n is an integer and $n \equiv 3 \pmod 4$. Prove that there does not exist integers x, y with $x^2 + y^2 = n$.

To see why this is, consider the table below where each entry gives the equivalence class of $x^2 + y^2$ modulo 4 depending on the equivalence class of x and y module 4.

	$x \equiv 0$	$x \equiv 1$	$x \equiv 2$	$x \equiv 3$
$y \equiv 0$	0	1	0	1
$y \equiv 1$	1	2	1	2
$y \equiv 2$	0	1	0	1
$y \equiv 3$	1	2	1	2

Notice that in none of the above entries do we have that $x^2+y^2 \equiv 3 \pmod 4$. Thus, given any integers x and y, it is impossible for $x^2 + y^2$ to be in the set $3 + 4\mathbb{Z}$ which contains n.

4. Suppose p is a prime number and $p \equiv 1 \pmod 4$. Then there exists $x \in \mathbb{Z}$ with $x^2 + 1 \equiv 0 \pmod p$.

By Wilson's theorem, we know that $(p-1)(p-2)\ldots(2)(1) \equiv -1 \pmod p$. We can rewrite this as follows:

$$\begin{aligned} & (p-1)(p-2)\ldots(\tfrac{p+1}{2})(\tfrac{p-1}{2})\ldots(2)(1) \equiv -1 \\ \implies\ & (-1)(-2)\ldots(-\tfrac{p-1}{2})(\tfrac{p-1}{2})\ldots(2)(1) \equiv -1 \\ \implies\ & (-1)^{\frac{p-1}{2}}((\tfrac{p-1}{2})!)^2 \equiv -1 \end{aligned}$$

We know that $p+1 \equiv -p+1 = -(p-1) \pmod p$. And since 2 has a unique inverse in $\mathbb{Z}/p\mathbb{Z}$, we can thus say that $\frac{p+1}{2} \equiv -\frac{p-1}{2} \pmod p$.

Since $p \equiv 1 \pmod 4$, we know that $p-1$ is a multiple of 4. It follows that $\frac{p-1}{2}$ is a multiple of 2. Thus $(-1)^{\frac{p-1}{2}} = 1$. And hence, $((\frac{p-1}{2})!)^2 \equiv -1 \pmod p$. Setting $x = (\frac{p-1}{2})!$, we thus have that $x^2 + 1 \equiv 0 \pmod p$.

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