Categories, Symmetry and Manifolds

Math 4800, Fall 2020

2. Abelian Groups. The category of abelian groups is a precursor to the category of vector spaces that is the context for an undergraduate course in linear algebra. Abelian groups are simultaneously simpler than vector spaces (fewer rules) and more complicated (the number theory of the integers comes into play). Cyclic groups are the most basic abelian groups, with abelian groups of symmetries. Even the simplest non-cyclic abelian group, though, has non-commuting symmetries.

Abelian Groups. The category $\mathfrak{Ab}$ of abelian groups is defined by:

- The objects of $\mathfrak{Ab}$ are triples $(A, +, 0)$ consisting of a set A, an operation

$$+ : A \times A \to A$$

and an element $0 \in A$ with the following properties:

(i) $+$ is both commutative and associative.

(ii) $0 \in A$ is an identity element for $+$, i.e. $0 + a = a$ for all $a \in A$.

(iii) Every element $a \in A$ has an *additive inverse* $-a$ such that $a + (-a) = 0$.

- The morphisms in $\mathfrak{Ab}$ are the **linear functions** $f : A \to B$, meaning that

$$f(0) = 0 \text{ and } f(a_1 + a_2) = f(a_1) + f(a_2) \text{ for all } a_1, a_2 \in A$$

and then it also follows that $f(-a) = -f(a)$.

This defines a category since a composition of linear functions is linear and:

$$1_A : A \to A \text{ is evidently linear}$$

Examples of Abelian Groups. (a) The integers with addition $(\mathbb{Z}, +, 0)$.

(b) The rational numbers $(\mathbb{Q}, +, 0)$ or real numbers $(\mathbb{R}, +, 0)$.

(c) The integers (mod n) $(\mathbb{Z}/n\mathbb{Z}, +, 0)$ with addition (for any $n \in \mathbb{N}$).

(d) The non-zero rationals or reals with *multiplication*: $(\mathbb{Q}^*, \cdot, 1)$ or $(\mathbb{R}^*, \cdot, 1)$.

(e) The exponential $e^x : (\mathbb{R}, +, 0) \to (\mathbb{R}^*, \cdot, 1)$ is a linear function.

$$e^0 = 1 \quad \text{and} \quad e^{x_1 + x_2} = e^{x_1} \cdot e^{x_2}$$

The image of the exponential is the group $(\mathbb{R}^{>0}, \cdot, 1)$ of **positive** real numbers, and the inverse function of the exponential is the natural logarithm.

Lemma 2.1. If a linear function $f : A \to B$ is a bijection, then the inverse function $f^{-1} : B \to A$ is also linear, and so f is an isomorphism in the category $\mathfrak{Ab}$.

Proof. Let $b_1, b_2 \in B$. Then $f(0) = 0$, so $f^{-1}(0) = 0$ and:

$$f(f^{-1}(b_1) + f^{-1}(b_2)) = f(f^{-1}(b_1)) + f(f^{-1}(b_2)) = b_1 + b_2$$

because f is linear, so $f^{-1}(b_1) + f^{-1}(b_2) = f^{-1}(b_1 + b_2)$ showing that f^{-1} is linear.

Lemma 2.2. For any pair of abelian groups A and B, the set:

$$\text{hom}(A, B) \text{ is itself an abelian group.}$$

Proof. The addition of linear functions is defined by:

$$(f + g)(a) = f(a) + g(a)$$

with 0 being the zero function and $-f(a) := f(-a)$ as the additive inverse of f.

Products. If A and B are abelian groups, then their Cartesian product:

$$A \times B \text{ with } (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \text{ and } 0 = (0, 0)$$

and linear projections is the product of A and B in the category of abelian groups (as in Project 1). This is **also** the coproduct with the following linear maps:

$$i : A \to A \times B;\ i(a) = (a, 0) \text{ and } j : B \to A \times B; j(b) = (0, b)$$

Example. (a) $(\mathbb{Z}^r = \mathbb{Z} \times \cdots \times \mathbb{Z}, +, (0, ..., 0))$ is the free abelian group of rank r. The elements of $\mathbb{Z}^r$ are r-tuples $(a_1, ..., a_r)$ of integers with "vector" addition.

(b) The composition of linear functions is a *bilinear* function of abelian groups:

$$\circ : \hom(S, T) \times \hom(R, S) \to \hom(R, T)$$

i.e. $(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g$ and $f_1 \circ (g_1 + g_2) = f_1 \circ g_1 + f_1 \circ g_2$. Is it linear?

(c) For free abelian groups $\mathbb{Z}^c$ and $\mathbb{Z}^r$, the abelian group

$$\hom(\mathbb{Z}^c, \mathbb{Z}^r)$$

is also a free, of rank rc. As with linear maps of vector spaces, the elements $f \in \hom(\mathbb{Z}^c, \mathbb{Z}^r)$ can be interpreted as $r \times c$ **matrices** M. Recall that:

$$f(1, 0, ..., 0) \text{ is the first column of } M,\ f(0, 1, 0, ..., 0) \text{ is the second column, etc.}$$

(which is why I used the letter c) and the addition of linear functions is captured by addition of matrices while the composition of linear functions is captured by **matrix multiplication**

$$\hom(\mathbb{Z}^r, \mathbb{Z}^s) \times \hom(\mathbb{Z}^c, \mathbb{Z}^r) \to \hom(\mathbb{Z}^c\mathbb{Z}^s);\ M \circ N = M \cdot N$$

and therefore the symmetries of a free abelian group $\mathbb{Z}^r$ are the *unimodular* $r \times r$ matrices of integers, i.e. the matrices with integer entries and determinant ± 1. These are symmetry groups that are worthy of a project!

Subgroups. A subset $B \subset A$ of an abelian group A is a **subgroup** of A if $0 \in B$ and B is closed under addition and inverses. The **span** of a subset $S \subset A$ is the smallest subgroup B of A that contains S, in which case we also say that S **generates** the subgroup B. Concretely, we can generate all the elements of B as linear combinations of elements of S:

$$B = \{n_1 a_1 + ... + n_m a_m \mid m \in \mathbb{N}, a_i \in S,\ n_i \in \mathbb{Z}\}$$

where $na = a + \cdots + a$ is defined by repeated addition (or subtraction if $n < 0$).

An abelian group A is **finitely generated** if it can be generated by a set with finitely many elements. A group A is **cyclic** if it can be generated by **one** element.

Example. $(\mathbb{Z}, +, 0)$ is a cyclic group, generated by either the element 1 or -1. Given $a_1, a_2 \in \mathbb{Z}$, let $d = \gcd(a_1, a_2)$. Then using Euclid's algorithm we can solve

$$d = b_1 a_1 + b_2 a_2$$

with integers b_1 and b_2. It follows that a_1 and a_2 together generate the *same* subgroup of $\mathbb{Z}$ as d does. From this we conclude that every subgroup of $\mathbb{Z}$ is cyclic. In fact, if $S \subset \mathbb{Z}$, then the group generated by S is also generated by the gcd of the elements of S.

Defintion 2.3. The subgroup of $\mathbb{Z}$ generated by n is called $n\mathbb{Z}$.

Subgroups of $\mathbb{Z}$. The objects of the category $\mathfrak{Subg}_{\mathbb{Z}}$ of subgroups of $\mathbb{Z}$ are:

$$n\mathbb{Z} \text{ for natural numbers } n \in \mathbb{N} \text{ (including } n = 0)$$

and the inclusions are the morphisms (as in the categories of subsets).

Question. What are the product and coproduct of $n\mathbb{Z}$ and $m\mathbb{Z}$ in this category?

Contrasting Example. $(\mathbb{Q}, +, 0)$ is not finitely generated. If

$$\left\{\frac{a_1}{n_1}, ..., \frac{a_m}{n_m}\right\} \subset \mathbb{Q}$$

is a finite set of rational numbers, then the denominator of any linear combination of these generators must divide the least common multiple of $n_1, ..., n_m$. In particular, if p is a prime that does not divide any n_i, then $1/p$ is not in the span.

Quotient Groups. One of the distinctive features of the category of abelian groups is the existence of a **quotient group** A/B of an abelian group A by a subgroup $B \subset A$. A subgroup $B \subset A$ determines an *equivalence relation* on A:

$$a_1 \sim a_2 \text{ if and only if } a_1 + b = a_2 \text{ for some } b \in B$$

The equivalence class containing $a \in A$ is denoted by $a + B = \{a + b \mid b \in B\}$ and is called the *coset containing* a of the subgroup B. Two cosets $a + B$ and $a' + B$ are the same if and only if $a' = a + b$ for some $b \in B$. The set of distinct cosets:

$$A/B = \{a + B\}$$

is an abelian group, with the zero coset being $B = 0 + B$ and addition rule:

$$(a_1 + B) + (a_2 + B) = (a_1 + a_2) + B$$

This is a quotient of the abelian group A in the sense that it comes with a surjection:

$$q : A \to A/B \text{ given by } q(a) = a + B$$

Example. The quotient of $\mathbb{Z}$ by the subgroup $n\mathbb{Z}$ is the abelian group:

$$\mathbb{Z}/n\mathbb{Z} \;\text{ of integers modulo } n$$

The cosets of $n\mathbb{Z}$ are the sets: $\{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \cdots, (n-1) + n\mathbb{Z}\}$ which are in bijection with the set $\{0, 1, ..., n-1\}$ and the addition rule is the usual addition modulo n. These are the **finite cyclic groups** (all generated by $1+n\mathbb{Z}$) in contrast with the infinite cyclic group $\mathbb{Z}$.

Note. The multiplication of integers also is well-defined on cosets:

$$(a_1 + n\mathbb{Z}) \cdot (a_2 + n\mathbb{Z}) = a_1a_2 + n\mathbb{Z}$$

giving a multiplication (with the usual properties) on $\mathbb{Z}/n\mathbb{Z}$.

Question. When is the product of finite cyclic groups: $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ cyclic? (Hint: this is answered by the Chinese Remainder Theorem).

Kernels, Images and Cokernels. A linear map $f : A \to B$ of abelian groups determines some special subgroups and quotient groups.

- The **kernel** of f is the subgroup $K = \{a \in A \mid f(a) = 0\} \subset A$.
- The **image** of f is the subgroup $I = f(A) \subset B$
- The **coimage** of f is the quotient abelian group A/K and
- The **cokernel** of f is the quotient abelian group $C = B/I$.

Proposition 2.4. A linear map $f : A \to B$ determines an isomorphism:

$$\overline{f} : A/K \to I$$

from the coimage abelian group to the image abelian group.

Proof. The linear map $\overline{f}$ is defined by

$$\overline{f}(a + K) = f(a)$$

This is well-defined since $f(a + k) = f(a) + f(k) = f(a)$ for all elements $k \in K$.

It is surjective, since it has the same image set as f does, and if

$$f(a + K) = f(a' + K) \text{ then}$$

- $f(a) = f(a')$
- $0 = f(a') - f(a) = f(a' - a)$
- $a' - a = k \in K$
- $a' = a + k$ and so finally $a + K = a' + K$ are the same coset.

So $\overline{f}$ is also injective, and therefore an isomorphism. □

The kernel and cokernel round out a four-term "long exact sequence":

$$0 \to K \overset{i}{\to} A \overset{f}{\to} B \overset{q}{\to} C \to 0$$

in which the kernel of each linear map is isomorphic to the image of the one before. (Note that i is the inclusion linear map of the kernel subgroup $K \subseteq A$).

Examples. (a) The linear function $f : \mathbb{Z} \to \mathbb{Z}$, $f(a) = na$, is injective and:

$$0 \to \mathbb{Z} \overset{\cdot n}{\to} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

is the associated (three-term!) exact sequence. (The image of $\cdot n$ is $n\mathbb{Z}$).

(b) The linear function $f : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$, $f(a) = 2a$ has the associated sequence:

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \overset{\cdot 2}{\to} \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

Symmetries. The symmetries of a **cyclic** group are already very subtle.

Guiding Principle. Let $a \in A$ generate a cyclic group A. Then a linear map:

$$f : A \to A$$

is completely determined by where it takes the generator, since:

$$f(0) = 0, f(a) = b, f(-a) = -b, f(2a) = 2b, \text{ etc}$$

and $\sigma : A \to A$ is a **symmetry** if and only if $\sigma(a) = b$ is another generator of A. This value is the *seed* of the symmetry σ (with respect to the generator a).

Symmetries of $\mathbb{Z}$. We start with the generator $1 \in \mathbb{Z}$. Then:

$$\sigma(1) = 1 \text{ is the seed of the identity and } \sigma(1) = -1$$

is the seed of the linear map $\sigma(a) = -a$. Notice that $\sigma \circ \sigma = 1_{\mathbb{Z}}$.

Remark. The symmetries of $\mathbb{Z}$ are isomorphic to the abelian group:

$$(\{\pm 1\}, \cdot, 1)$$

which is itself isomorphic to the two element cyclic abelian group $(\mathbb{Z}/2\mathbb{Z}, +, 0)$. Why?

Symmetries of $\mathbb{Z}/n\mathbb{Z}$. Our first task is to find all the generators of the cyclic group $\mathbb{Z}/n\mathbb{Z}$. For b to be a generator, every element of $\mathbb{Z}/n\mathbb{Z}$ must be in the list:

$$0, b, 2b, 3b, ... \text{ of elements of } \mathbb{Z}/n\mathbb{Z}$$

and it suffices find $1 + n\mathbb{Z}$ in the list to conclude that every element is in the list. (Note that we are identifying b with $b + n\mathbb{Z}$). But

$$1 + n\mathbb{Z} = mb + n\mathbb{Z}$$

for some m if and only if $1 + na = mb$ for some $a \in \mathbb{Z}$. This is the case if and only if $\gcd(b, n) = 1$ (Euclid's algorithm again).We conclude that:

- The generators of $\mathbb{Z}/n\mathbb{Z}$ are the cosets $b + n\mathbb{Z}$ with $\gcd(b, n) = 1$.

Moreover, if $\sigma(1) = b$ and $\tau(1) = c$ are the seeds for two symmetries, then:

$$\sigma \circ \tau(1) = \sigma(c) = c \cdot \sigma(1) = c \cdot b$$

so $c \cdot b = b \cdot c$ is the seed for the composition. This shows that the **composition** symmetries of $\mathbb{Z}/n\mathbb{Z}$ corresponds to **multiplication** of the seeds, and therefore that the symmetries with composition aret an abelian group that is isomorphic to:

$$((\mathbb{Z}/n\mathbb{Z})^* := \{b \in \{1, ..., n\} \text{ that are relatively prime to } n\}, \cdot, 1)$$

Question. What is the *inverse* of b in this group?

Example. (a) There are four symmetries of $\mathbb{Z}/8\mathbb{Z}$, with seeds: $\sigma(1) = 1, 3, 5$ or 7. Each symmetry satisfies $\sigma^2(1) = (\sigma(1))^2 = 1 \pmod 8$, so in particular, the group of symmetries is **not** isomorphic to the cyclic group $\mathbb{Z}/4\mathbb{Z}$. In fact, it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. One isomorphism to $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +, (0, 0))$ is given by:

$$f(1) = (0, 0), f(3) = (1, 0), f(5) = (0, 1), f(7) = (1, 1)$$

(b) There are also four symmetries of $\mathbb{Z}/5\mathbb{Z}$ with seeds: $\sigma(1) = 1, 2, 3, 4$. This group **is** cyclic, generated by either of the seeds $\sigma(1) = 2$ or $\sigma(1) = 3$.

(c) The symmetries of an abelian group that is not cyclic often do not commute. For example, consider the symmetries:

$$\sigma : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

These are the six 2×2 matrices of 0's and 1's with nonzero determinant (mod 2):

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

with mod 2 multplication. Here,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

but

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

Remark. These symmetries can be identified with the permutations of [3] in such a way that matrix multiplication corresponds to the composition of permutations.

Theorem 2.5. The symmetry group $((\mathbb{Z}/p\mathbb{Z})^*, \cdot, 1)$ is cyclic when p is a prime.

Proof. The amusing idea is to count the generators before knowing they exist. We first note that $(\mathbb{Z}/p\mathbb{Z}, +, \cdot, 0, 1)$ is a field. This is because:

$$(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, ..., p-1\}$$

since p is prime, so every non-zero element has a multiplicative inverse.

A polynomial of degree d with coefficients in a field has at most d roots. Thus,

$$x^{p-1} - 1$$

has at most $p-1$ roots. But every $b \in (\mathbb{Z}/p\mathbb{Z})^*$ is a root of this polynomial. This is known as **Fermat's Little Theorem**. To see it, consider the linear function:

$$f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z};\ f(m) = mb$$

This is a bijection because b has a multiplicative inverse, so the products:

$$1 \cdot 2 \cdots m \cdots (p-1) = (1b) \cdot (2b) \cdots (mb) \cdots ((p-1)b) \text{ in } \mathbb{Z}/p\mathbb{Z}$$

Dividing both sides by $(p-1)!$ gives the Little Theorem. This factorizes:

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1))$$

For each $b \in (\mathbb{Z}/p\mathbb{Z})^*$, let d be the smallest positive power such that $b^d = 1$. This is the **order** of b, written $\operatorname{ord}(b) = d$. Then d is a divisor of $p-1$ because otherwise $e = \gcd(d, p-1) < d$ and using Euclid's algorithm, we could solve:

$$e = md + n(p-1) \text{ giving } b^e = (b^d)^m \cdot (b^{p-1})^n = 1 \text{ for a smaller value } e$$

Now we finally claim that for **every** divisor d of $p-1$,

$$(*)\ \#\{b \in (\mathbb{Z}/p\mathbb{Z})^* \mid \operatorname{ord}(b) = d\} = \phi(d)$$

where $\phi(d)$ is the **Euler ϕ function** counting the number of elements in $(\mathbb{Z}/d\mathbb{Z})^*$. This includes the existence of elements of order $p-1$, i.e. generators, since:

$$\phi(p-1) > 0 \text{ counts the set of generators!}$$

So verifying $(*)$ proves the Theorem and also counts the generators. Euler's formula:

$$\sum_{d|n} \phi(d) = n$$

can be found in a number theory text, but here is a proof that also proves $(*)$.

If $\operatorname{ord}(b) = d$, then the powers of b are **all of the** roots of the polynomial $x^d - 1$, and in particular every element of order d is a power of b. On the other hand, if $\gcd(m, d) = e > 1$ then $(b^m)^{(d/e)} = 1$, so $\operatorname{ord}(b^m) < d$. Thus we get:

$$\#\{b \in (\mathbb{Z}/p\mathbb{Z})^* \mid \operatorname{ord}(b) = d\} \le \phi(d)$$

since the set is either empty or, if $\operatorname{ord}(b) = d$ for some b, then the set consists only of powers of b that are relatively prime to d. On the other hand, looking at the n roots of $x^n - 1$ with coefficients in the **complex numbers**, it is easy to see that there are complex roots $e^{2\pi i m/n}$ of all orders d dividing n and that there are $\phi(d)$ of them. This gives Euler's formula which in turn gives:

$$p - 1 = \#(\mathbb{Z}/p\mathbb{Z})^* = \sum_{d|p-1} \#\{b \in (\mathbb{Z}/p\mathbb{Z})^* \mid \operatorname{ord}(b) = d\} \le \sum_{d|p-1} \phi(d) = p - 1$$

But this shows that the equality $(*)$ holds for **all** orders including $p-1$ itself. $\square$

Example. Let's see how this plays out for some small primes.

(p = 5)

$$p - 1 = 4 = \phi(1) + \phi(2) + \phi(4) = 1 + 1 + 2$$

and

$$x - 1 = x - 1 \quad \text{(1 is the unique element of order 1)}$$
$$x^2 - 1 = (x-1)(x-4) \quad \text{(4 is the unique element of order 2)}$$
$$x^4 - 1 = (x-1)(x-2)(x-4)(x-3) \quad \text{(2 and 3 are the elements of order 4)}$$

(p = 7)

$$p - 1 = 6 = \phi(1) + \phi(2) + \phi(3) + \phi(6) = 1 + 1 + 2 + 2$$

and

$$x - 1 = (x - 1)$$
$$x^2 - 1 = (x-1)(x-6) \quad \text{(6 is the unique element of order 2)}$$
$$x^3 - 1 = (x-1)(x-2)(x-4) \quad \text{(2 and 4 are the elements of order 3)}$$
$$x^6 - 1 = (x-1)(x-3)(x-2)(x-6)(x-4)(x-5) \quad \text{(3 and 5 are the elements of order 6)}$$

On the other hand:

(n = 8) doesn't follow the pattern because $x^2 - 1$ has **4** roots!.

The argument that a polynomial of degree d has at most d roots was central to the proof of Theorem 2.5 and requires the coefficients to be in a field since it rests on the **unique factorization** of polynomials. With coefficients in $(\mathbb{Z}/8\mathbb{Z})$,

$$x^2 - 1 = (x-3)(x-5) = (x-1)(x-7)$$

and so in particular unique factorization fails in this context.

Remark. it is not easy to find a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ when p is a very large prime. It is an open question whether or not 2 is infinitely often a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. This is a case of the Artin conjecture. (Recall that 2 is not a generator when $p = 7$)

Assignment 2.

1. What are the product and coproduct of $n\mathbb{Z}$ and $m\mathbb{Z}$ in the category $\mathfrak{S}ubg_{\mathbb{Z}}$?

2. (a) Prove that the linear map:

$$f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z};\ f(a) = (a, a)$$

is an isomorphism of abelian groups.

(b) Prove that the linear map:

$$g : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z};\ g(a) = (a, a)$$

is **not** an isomorphism of abelian groups.

(c) Explain why the two abelian groups:

$$\mathbb{Z}/mn\mathbb{Z} \text{ and } \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

are not isomorphic if $\gcd(m, n) > 1$.

(d)* Improve (a). Show that the linear map:

$$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z};\ f(a) = (a, a)$$

is an isomorphism when $\gcd(m, n) = 1$ by finding the inverse linear map using the Chinese Remainder Theorem.

3. How would you find the inverse of the symmetry $\sigma(1) = b$ for seed $b \in (\mathbb{Z}/n\mathbb{Z})^*$?

4. Find all the symmetry groups $((\mathbb{Z}/n\mathbb{Z})^*, \cdot, 1)$ for $n = 2, ..., 20$.

5. Find an explicit "isomorphism" between the symmetries of [3] and of $\mathbb{Z}/2 \times \mathbb{Z}/2$ that takes composition of permutations to multiplication of matrices (mod 2).

6. Given a *finite* abelian subgroup $B \subset A$, prove that every coset $a + B$ has the same number of elements. Conclude that if A is also finite, then the number of elements of B **divides** the number of elements of A, and in fact that:

$$|B| \cdot |A/B| = |A|$$

(where $|S|$ is the number of elements of a set S).

7. Extend the last Example to primes $p = 11$ and $p = 13$.

Project Ideas.

2.1. Every finitely generated abelian group is isomorphic to the product of finitely many cyclic groups. Why?

2.2. Explore the symmetries of $\mathbb{Z}^2$. These are the 2×2 matrices with integer coefficients and determinant ± 1.