Math 71: Algebra **Fall 2022**

PSET 2 — 2022-11-11

Prof. Voight ***Student: Amittai Siavava***

Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

(a) ***Abstract Algebra*** by **David S. Dummit & Richard M. Foote**.

(b) ***Algebra*** by **Jacob K. Goldhaber & Gertrude Ehrlich**

Problems

1. (DF 0.1.7) Let $f\colon A \to B$ be a surjective map of sets. For $y \in B$, let

$$f^{-1}(y) := \{x \in A : f(x) = y\}$$

be the *preimage* or *fiber* of f over y. (The map f is bijective if and only if $f^{-1}(y) = \{x\}$ consists of a single element $x \in A$, in which case we can define f^{-1} as a function, removing the set brackets. But we always have fibers.) Define a relation by $a \sim b$ if $f(a) = f(b)$. Show that this relation is an equivalence relation whose equivalence classes are the fibers of f.

What we know (so far):

(a) f is surjective, meaning, for every $y \in B$, there exists **at least one** $x \in A$ such that $f(x) = y$.

(b) We define the relation $a \sim b$ to hold if $f(a) = f(b)$. From this, we can note:

  (a) **Symmetry:** $a \sim b \implies f(a) = f(b) \implies f(b) = f(a) \implies b \sim a$.

  (b) **Reflexivity:** For every $a \in A$ acted on by f, $f(a) = f(a)$, so $a \sim a$.

  (c) **Transitivity:** If $a \sim b$ and $b \sim c$, then $f(a) = f(b) = f(c)$, so $a \sim c$.

Since $\sim$ has symmetry, reflexivity, and transitivity, we can conclude that $\sim$ is an equivalence relation.

Next, we show that the equivalence classes of $\sim$ are the fibers of f.

First, let's define the equivalence classes of $\sim$.
Since f is surjective, for every $y \in B$, there exists at least one $x \in A$ such that $f(x) = y$.
Let's take one such element, $x_0 \in A$ and its corresponding $y_0 \in B$ such that $f(x_0) = y_0$.
The equivalence class of x_0 under f is the set of all elements $x \in A$ such that $f(x) = f(x_0) = y_0$.

This, by definition, implies that $x \sim x_0$, and $x \in f^{-1}(y_0)$.

$$[x_0] = \{x \in A \colon x \sim x_0 \qquad \text{(meaning } f(x) = f(x_0))\}$$

Next, we need to show that the equivalence classes of $\sim$ are the fibers of f.

Let's take an arbitrary equivalence class $[x_0]$ such as the one derived above.

We know that $[x_0] \subseteq A$ and $f(x) = y_0$ for all $x \in [x_0]$.

Then, by definition of inverses, $f^{-1}(y_0) = [x_0]$.

Generally, $[x] = f^{-1}(f(x))$ for all $x \in A$, and $[x]$ is the equivalence class of x under $\sim$.

2. (sorta-not-really DF 0.3.15(b))

(a) For $a = 69$ and $n = 372$, determine the greatest common divisor $g := \mathbf{gcd}\ (a,\ n)$, the least common multiple $\mathbf{lcm}\ (a,\ b)$, and write $g = ax + by$ with $x, y \in \mathbb{Z}$. Is $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$? If so, what is $\overline{a}^{-1}$?

Factoring, we get $69 = 3 \cdot 23$ and $372 = 2^2 \cdot 3 \cdot 31$.

By definition, given:

$$a = 1^{a_1} \cdot 2^{a_2} \cdot 3^{a_3} \cdots (n-1)^{a_{n-1}} \cdot n^{a_n}$$
$$b = 1^{b_1} \cdot 2^{b_2} \cdot 3^{b_3} \cdots (n-1)^{b_{n-1}} \cdot n^{b_n}$$

Then we can define the gcd and lcm as:

$$\mathbf{gcd}\ (a,\ b) = 1^{\min(a_1,b_1)} \cdot 2^{\min(a_2,b_2)} \cdot 3^{\min(a_3,b_3)} \cdots (n-1)^{\min(a_{n-1},b_{n-1})} \cdot n^{\min(a_n,b_n)}$$
$$\mathbf{lcm}\ (a,\ b) = 1^{\max(a_1,b_1)} \cdot 2^{\max(a_2,b_2)} \cdot 3^{\max(a_3,b_3)} \cdots (n-1)^{\max(a_{n-1},b_{n-1})} \cdot n^{\max(a_n,b_n)}$$

For $a = 69$ and $b = 372$, we get:

$$\mathbf{gcd}\ (69,\ 372) = 2^0 \cdot 3 \cdot 23^0 \cdot 31^0 = 3$$
$$\mathbf{lcm}\ (69,\ 372) = 2^2 \cdot 3 \cdot 23 \cdot 31 = 8556$$

Using the Euclidean algorithm:

$$372 = 69 \cdot 5 + 27$$
$$69 = 27 \cdot 2 + 15$$
$$27 = 15 \cdot 1 + 12$$
$$15 = 12 \cdot 1 + 3$$
$$12 = 3 \cdot 4 + 0$$

Back-substituting, we get:

$$\begin{aligned} 3 &= 15 - 12 \\ &= 15 - (27 - 15) = 2 \cdot 15 - 27 \\ &= 2(69 - 2 \cdot 27) - 27 = 2 \cdot 69 - 5 \cdot 27 \\ &= 2 \cdot 69 - 5(372 - 5 \cdot 69) = 27 \cdot 69 - 5 \cdot 372 \\ &= 27 \cdot 69 - 5 \cdot 372 \end{aligned}$$

Thus, we can write $3 = 27 \cdot 69 - 5 \cdot 372$, with $x = 27$ and $y = -5$.

Is $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$? If so, what is $\overline{a}^{-1}$?

No, $\overline{69} \notin (\mathbb{Z}/372\mathbb{Z})^{\times}$ because $\mathbf{gcd}\ (69,\ 372) \neq 0$ (that is, 69 and 372 are not coprime).

(b) Taking $n = 89$, what is the order of $\overline{2}$ in $(\mathbb{Z}/n\mathbb{Z})^{\times}$?

The order $o(\overline{a})$ of an element $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ is the smallest positive integer k such that $\overline{a}^k \equiv 1 \pmod{n}$.

For a single element, we can use the following algorithm to find the order:

```
function order (a, n)
  k = 1
  while a^k is not congruent to 1 mod n
    k = k + 1
  return k
```

We get:

```
ghci> order 2 89
Found 2 ^ 11 = 2048 == 1 (mod 89)
```

The order of $\overline{2}$ in $(\mathbb{Z}/89\mathbb{Z})^{\times}$ is 11.

(c) How many elements are there in $(\mathbb{Z}/360\mathbb{Z})^{\times}$?

All elements in $(\mathbb{Z}/n\mathbb{Z})^{\times}$ have to be coprime to n.

There are a total of $\phi(n)$ relatively prime numbers less than n.

We can calculate the value of $\phi(n)$ for reasonably small n using a simple algorithm:

```
function phi (n)
  count = 0
  for i = 1 to n
    if gcd (i, n) == 1
      count = count + 1
  return count
```

We get:

```
ghci> phi 360
96
```

Optionally, we can also factor $360 = 2^3 \cdot 3^2 \cdot 5$ and use the multiplicative property of the *phi* function to get:

$$
\begin{aligned}
\phi(360) &= \phi(2^3 \cdot 3^2 \cdot 5) \\
&= \phi(2^3) \cdot \phi(3^2) \cdot \phi(5) \\
&= (2^3 - 2^2) \cdot (3^2 - 3) \cdot (5 - 1) \\
&= 8 \cdot 6 \cdot 4 \\
&= 96
\end{aligned}
$$

Hence, there are a total of 96 elements in $(\mathbb{Z}/360\mathbb{Z})^\times$.

3. (DF 1.3.1, sorta 1.3.7)

(a) Let σ be the permutation

$$1 \mapsto 3,\ 2 \mapsto 4,\ 3 \mapsto 5,\ 4 \mapsto 2,\ 5 \mapsto 1$$

and τ be the permutation

$$1 \mapsto 5,\ 2 \mapsto 3,\ 3 \mapsto 2,\ 4 \mapsto 4,\ 5 \mapsto 1.$$

Find the cycle decompositions of each of the following: $\sigma, \tau, \sigma^2, \sigma^{-1}, \sigma\tau, \tau\sigma, \tau^2\sigma$. Do σ and τ commute?

(a) σ

$$\begin{aligned} 1 &\mapsto 3 \\ 2 &\mapsto 4 \\ 3 &\mapsto 5 \\ 4 &\mapsto 2 \\ 5 &\mapsto 1 \\ &= (1\ 3\ 5)\ (2\ 4) \end{aligned}$$

(b) τ

$$\begin{aligned} 1 &\mapsto 5 \\ 2 &\mapsto 3 \\ 3 &\mapsto 2 \\ 4 &\mapsto 4 \\ 5 &\mapsto 1 \\ &= (1\ 5)\ (2\ 3)\ (4) \\ &= (1\ 5)\ (2\ 3) \end{aligned}$$

(c) σ^2

$$1 \mapsto 3 \mapsto 5$$

$$2 \mapsto 4 \mapsto 2$$

$$3 \mapsto 5 \mapsto 1$$

$$4 \mapsto 2 \mapsto 4$$

$$5 \mapsto 1 \mapsto 3$$

$$= (1\ 5\ 3)\ (2)\ (4)$$

$$= (1\ 5\ 3)$$

(d) σ^{-1}

$$1 \mapsto 5$$

$$2 \mapsto 4$$

$$3 \mapsto 1$$

$$4 \mapsto 2$$

$$5 \mapsto 3$$

$$= (1\ 5\ 3)\ (2\ 4)$$

(e) $\sigma\tau$

$$1 \mapsto 5 \mapsto 1$$

$$2 \mapsto 3 \mapsto 5$$

$$3 \mapsto 2 \mapsto 4$$

$$4 \mapsto 4 \mapsto 2$$

$$5 \mapsto 1 \mapsto 3$$

$$= (1)\ (2\ 5\ 3\ 4)$$

$$= (2\ 5\ 3\ 4)$$

(f) $\tau\sigma$

$$\begin{aligned}
1 &\mapsto 3 \mapsto 2 \\
2 &\mapsto 4 \mapsto 4 \\
3 &\mapsto 5 \mapsto 1 \\
4 &\mapsto 2 \mapsto 3 \\
5 &\mapsto 1 \mapsto 5 \\
&= (1\ 2\ 4\ 3)\ (5) \\
&= (1\ 2\ 4\ 3)
\end{aligned}$$

(g) $\tau^2\sigma$

$$\begin{aligned}
1 &\mapsto 3 \mapsto 2 \mapsto 3 \\
2 &\mapsto 4 \mapsto 4 \mapsto 4 \\
3 &\mapsto 5 \mapsto 1 \mapsto 5 \\
4 &\mapsto 2 \mapsto 3 \mapsto 2 \\
5 &\mapsto 1 \mapsto 5 \mapsto 1 \\
&= (1\ 3\ 5)(2\ 4)
\end{aligned}$$

(h) Do σ and τ commute?

No. As demonstrated above: $\sigma\tau \neq \tau\sigma$.

This is expected, since the cycles in σ are not disjoint from the cycles in τ.

(b) Write out the cycle decomposition of each element of order 2 in the symmetric group S_4. How many such elements are there of each cycle type?

(a) There are 9 elements of order 2 in S_4.

$$(1\ 2)$$
$$(1\ 3)$$
$$(1\ 4)$$
$$(2\ 3)$$
$$(2\ 4)$$
$$(3\ 4)$$
$$(1\ 2)\ (3\ 4)$$
$$(1\ 3)\ (2\ 4)$$
$$(1\ 4)\ (2\ 3)$$

(b) There are 6 elements of order 2 in S_4. There are 3 elements of cycle type $(1\ 2)$, 2 elements of cycle type $(1\ 3)$, and 1 element of cycle type $(1\ 4)$.

(c) How many elements are in the set $\{\sigma \in S_5 : \sigma(2) = 5\}$?

We are fixing the map $2 \mapsto 5$. This means 2 maps to only 5, and no other number maps to 5.

$$1 \mapsto \{1\ 2\ 3\ 4\}$$
$$2 \mapsto \{5\}$$
$$3 \mapsto \{1\ 2\ 3\ 4\}$$
$$4 \mapsto \{1\ 2\ 3\ 4\}$$
$$5 \mapsto \{1\ 2\ 3\ 4\}$$

Once we have fixed the map $2 \mapsto 5$, we have 4 possible mappings for each of the remaining 4 numbers of S_5. Thus, there are 4 choices for the second mapping.

We then have one less choice for the third mapping, and so on. In particular, there will be 3 choices for the third element, 2 choices for the fourth element, and 1 choice for the fifth element.

The number of elements is $4 \cdot 3 \cdot 2 \cdot 1 = 4! = 24$.

4. (some of DF 1.6.6)

(a) Let $\mathbb{R}^\times = \mathbb{R} \smallsetminus \{0\}$ be the set of nonzero real numbers. Then $\mathbb{R}^\times$ is a group under multiplication. Define a second binary operation on $\mathbb{R}^\times$ by $x * y = xy/2$ for $x, y \in \mathbb{R}^\times$. Show that $(\mathbb{R}^\times, *)$ is a group, and find an isomorphism $\phi\colon (\mathbb{R}^\times, \cdot) \xrightarrow{\sim} (\mathbb{R}^\times, *)$. *[Hint: if it helps, write $G = \mathbb{R}^\times$ in the second case with the nonstandard operation.]*

Let's pick arbitrary $x, y, z \in \mathbb{R}^\times$. Then:

$$x * y = \frac{xy}{2} \in \mathbb{R}^\times \qquad \text{(Closure)}$$

$$(x * y) * z = \frac{xy}{2} * z = \frac{xyz}{4} = x * \frac{yz}{2} = x * (y * z) \qquad \text{(Associative)}$$

$$x * 2 = x \cdot \frac{2}{2} = x = 2 \cdot \frac{x}{2} = 2 * x \qquad \text{(Identity = 2)}$$

$$x * (4/x) = x \cdot \frac{4}{2x} = 2 = \frac{4}{x} \cdot \frac{x}{2} = (4/x) * x \qquad \text{(Inverse of } x \text{ is} = 4/x)$$

Thus, $(\mathbb{R}^\times, *)$ is a group.

Let's define $\phi\colon (\mathbb{R}^\times, \cdot) \xrightarrow{\sim} (\mathbb{R}^\times, *)$ by $\phi(r) = 2r$ for $r \in \mathbb{R}^\times$. Then:

$$\begin{aligned}
\phi(xy) &= \phi(x) * \phi(y) \qquad \text{(Required condition)} \\
2xy &= 2x * 2y \\
2xy &= 2x \cdot \frac{2y}{2} \\
2xy &= 2xy
\end{aligned}$$

Furthermore, if ϕ is an isomorphism then it needs to map the identity in $(\mathbb{R}^\times, \cdot)$ to the identity in $(\mathbb{R}^\times, *)$.

$$\phi(e_1) = \phi(e_2)$$

$$e_1 = 1$$

$$e_2 = 2$$

$$\phi(e_1) = \phi(1) = 2 \cdot 1 = 2 = e_2$$

Thus, ϕ is *proven consistent* as an isomorphism between $(\mathbb{R}^\times, \cdot)$ and $(\mathbb{R}^\times, *)$.

(b) Prove that the groups $\mathbb{Z}$ (under $+$) is not isomorphic to $\mathbb{Q}$ (under $+$). *[Remark: there is a bijection from $\mathbb{Z}$ to $\mathbb{Q}$ that is not a homomorphism, and a homomorphism that is not a bijection!]*

Let's take $\phi\colon \mathbb{Q} \xrightarrow{\sim} \mathbb{Z}$ to be an isomorphism. Then:

(a) By definition, ϕ needs to map the identity in $\mathbb{Q}$ to the identity in $\mathbb{Z}$.

(b) By definition, ϕ needs to be distributive over the group operations $(+)$.

That is: $\phi(x + y) = \phi(x) + \phi(y)$ for all $x, y \in \mathbb{Q}$.

Let's take an arbitrary $q \in \mathbb{Q}$ such that $2 \nmid q$. Let's take a corresponding $z \in \mathbb{Z}$ such that $\phi(q) = z$.
Then, by the distributivity of ϕ: $\phi(q) = \phi(q/2 + q/2) = \phi(q/2) + \phi(q/2)$.
Let's define $z' \in \mathbb{Z}\colon\ z' = \phi(q/2)$. Then:

$$\begin{aligned} \phi(q) &= z \\ \phi(\frac{q}{2} + \frac{q}{2}) &= z \\ 2z' &= z \\ z' &= \frac{z}{2} \end{aligned}$$

We can conclude that, given $\phi(q) = z \in Z$, then $\phi(q/2) = z/2$ is not in $\mathbb{Z}$ for any q such that $2 \nmid \phi(q)$.
For a specific example, consider the instances of q such that $\phi(q) \in \{1, 3, 5, 7, \ldots\}$ (the odd positive integers). Then, $\phi(q/2) \in \{\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{7}{2}, \ldots\} \notin \mathbb{Z}$.
This contradiction (ϕ mapping elements from Q to $\mathbb{Z}$ yet the same elements are seen to not be in $\mathbb{Z}$) proves that ϕ is not an isomorphism, and $\mathbb{Z}$ is not isomorphic to $\mathbb{Q}$ under addition.

5. Let $\phi\colon G \to H$ be a bijective homomorphism, with inverse $\phi^{-1}\colon H \to G$. Show that ϕ^{-1} is also a homomorphism.

What we know (so far):

(i) That ϕ is a bijection tells us that:

  (a) ϕ is injective — that is, for every $g_1, g_2 \in G$ such that $\phi(g_1) = \phi(g_2)$, we have $g_1 = g_2$.

  (b) ϕ is surjective — that is, for every $h \in H$, there is a $g \in G$ such that $\phi(g) = h$.

(ii) That ϕ is a homomorphism tells us that for every $g_1, g_2 \in G$, $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.

(iii) That ϕ^{-1} is the inverse of ϕ tells us that, $\phi^{-1}(\phi(g)) = g$ for every $g \in G$, and $\phi(\phi^{-1}(h)) = h$ for every $h \in H$.

Next, let's pick two elements $a, b \in G$, and corresponding elements $a', b' \in H$ such that $\phi(a) = a'$ and $\phi(b) = b'$.

By property (3) above, $\phi^{-1}(a') = a$ and $\phi^{-1}(b') = b$.

By property (2) above, $\phi(ab) = \phi(a)\phi(b) = a'b'$.

From this, we aim to show that ϕ^{-1} is a homomorphism by showing that $\phi^{-1}(a'b') = \phi^{-1}(a')\phi^{-1}(b') = ab$.

$$\begin{aligned}
\phi(ab) &= \phi(a)\phi(b) = a'b' \\
\phi^{-1}(\phi(ab)) &= \phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(a'b') \quad \text{(Invert both sides)} \\
\phi^{-1}(\phi(ab)) &= \phi^{-1}(\phi(a))\phi^{-1}(\phi(b)) = \phi^{-1}(a'b') \quad \text{(By (ii) above)} \\
\phi^{-1}(\phi(ab)) &= \phi^{-1}(a')\phi^{-1}(b') = \phi^{-1}(a'b') \quad (\text{Since } \phi(a) = a', \phi(b) = b') \\
ab &= \phi^{-1}(a')\phi^{-1}(b') = \phi^{-1}(a'b') \quad (\text{Since } \phi^{-1}(\phi(x)) = x)
\end{aligned}$$

Thus, we see that $\phi^{-1}(a'b') = \phi^{-1}(a')\phi^{-1}(b') = ab$, and ϕ^{-1} is a homomorphism.