Assignment #5

1 March 2025

Abstract

Homework exercises for Prof. Dusty Ross's "Modern Algebra I".

1. **a**. *Proposition.* $\mathbb{Z}/8\mathbb{Z}$ and $(\mathbb{Z}/16\mathbb{Z})^\times$ are not isomorphic.

Proof. Suppose they were. Then $(\mathbb{Z}/16\mathbb{Z})^\times$ would have an element of order 8. But it doesn't. ($|1| = 1$ because $1^1 \cong 1 \mod 16$, $|3| = 4$ because $3^4 \cong 1 \mod 16$, $|5| = 4$ because $5^4 \cong 1 \mod 16$, $|7| = 2$ because $7^2 \cong 1 \mod 16$, $|9| = 2$ because $9^2 \cong 1 \mod 16$, $|11| = 4$ because $11^4 \cong 1 \mod 16$, $|13| = 4$ because $13^4 = 1 \mod 16$, $|15| = 2$ because $15^2 \cong 1 \mod 16$.) Contradiction!

b. *Proposition.* $\mathbb{Z}/6\mathbb{Z}$ and $(\mathbb{Z}/9\mathbb{Z})^\times$ are isomorphic.

Proof. Consider $(2\ 4\ 8\ 7\ 5\ 1) \in S_6$. As a 6-cycle, $(2\ 4\ 8\ 7\ 5\ 1)$ generates a cyclic group of order 6, so is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. (There is only one cyclic group of a given order up to isomorphism.) But the set-elements in the cycle also represent iterated multiplication by 2 mod 9: $2 \cdot 2 \cong 4 \mod 9$, $4 \cdot 2 \cong 8 \mod 9$, $8 \cdot 2 \cong 7 \mod 9$, *&c.*, so the cycle is ismorphic to $(\mathbb{Z}/9\mathbb{Z})^\times$.

2. **a**. *Proposition.* $\varphi(x) = x^3$ is an automorphism on $(\mathbb{Z}/16\mathbb{Z})^\times$.

Proof. (Bijection.) We use the Python code

```
from math import gcd

    for i in range(1, 17):
        if gcd(i, 16) == 1:
            print(i, i**3 % 16)
```

to compute the values of φ. It prints

```
1 1
3 11
5 13
7 7
9 9
11 3
13 5
15 15
```

We observe that every number only appears once in the right column (injectivity, no comdomain element mapped to more than once), and that every number in the right column appears in the left column (surjectivity, every codomain element is mapped to).

(Homomorphism.) $\varphi(x)\varphi(y) = x^3y^3$, and $\varphi(xy) = (xy)^3$, but in an abelian group like $(\mathbb{Z}/16\mathbb{Z})^\times$, we can commute elements, so $(xy)^3 = xyxyxy = xxxyyy = x^3y^3$.

b. *Proposition.* $\varphi(x) = x^2$ is not an automorphism of $(\mathbb{Z}/16\mathbb{Z})^\times$.

Proof. $3^2 \mod 16 \cong 9$ and $5^2 \mod 16 \cong 9$, so φ is not injective.

3. *Proposition.* $\varphi(n) = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ is an isomorphism between $\mathbb{Z}$ and $\left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} : n \in \mathbb{Z} \right\}$.

Proof. (Injectivity.) Suppose $\varphi(n) = \varphi(m)$. Then $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$. So $n = m$.

(Surjectivity.) Given a matrix of the form $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$, we can find a k such that $\varphi(k) = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$, namely $k := n$.

(Homomorphism.) $\varphi(n)\varphi(m) = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1\cdot 1 + n\cdot 0 & 1\cdot m + n\cdot 1 \\ 0\cdot 1 + 1\cdot 0 & 0\cdot m + 1\cdot 1 \end{bmatrix} = \begin{bmatrix} 1 & m+n \\ 0 & 1 \end{bmatrix} = \varphi(mn)$

4. *Proposition.* An automorphism φ of D_{2n} maps every rotation to a rotation.

Proof. Isomorphisms preserve the order of elements: $|r| = n$, so $|\varphi(r)| = n$. An element of order n in D_{2n} must be a rotation, so $\varphi(r)$ is a rotation. But then every other rotation $\varphi(r^k)$ for $k \in \{2...n-1\}$ gets mapped to $\varphi(r)^k$, which, as the power of a rotation, is also a rotation.

5. We want to compute the six left cosets of $H := \{(1), (12)(34), (13)(24), (14)(23)\}$ in S_4. Doing this manually would be an affront to human dignity. Let's write a Python program to do it.

```
from itertools import permutations
from collections import defaultdict
class Permutation:
    def __init__(self, data):
        self.data = data
    def __hash__(self):
        return hash(tuple(self.data))
    def cycles(self):
        placed = set()
        cycles = []
        while len(placed) < len(self.data):
            smallest_unplaced = sorted(set(self.data) - placed)[0]
            cursor = smallest_unplaced
            current_cycle = []
            while not current_cycle or cursor != current_cycle[0]:
                current_cycle.append(cursor)
                placed.add(cursor)
                cursor = self.data[cursor-1]
            else:
                cycles.append(current_cycle)
                smallest_unplaced = sorted(set(self.data) - placed)
                cursor = smallest_unplaced
                current_cycle = []
        return cycles
    def __repr__(self):
        cycles = self.cycles()
        if all(len(cycle) == 1 for cycle in cycles):
            return "1"
        def print_cycle(cycle):
            return "(" + " ".join(str(element) for element in cycle) + ")"
        return "".join(print_cycle(cycle) for cycle in cycles if len(cycle) != 1)
    def __eq__(self, other):
        return self.data == other.data
    def __lt__(self, other):
        return self.data < other.data
    def __mul__(self, other):
        return Permutation([other.data[a-1] for a in self.data])
if __name__ == "__main__":
        h = [
        Permutation([1, 2, 3, 4]),
        Permutation([2, 1, 4, 3]),
        Permutation([3, 4, 1, 2]),
        Permutation([4, 3, 2, 1]),
```

```
]
s_4 = [Permutation(p) for p in permutations((1, 2, 3, 4))]
coset_map = defaultdict(list)
for element in s_4:
    coset = tuple(sorted(element * h_j for h_j in h))
    coset_map[coset].append(element)
for coset, elements in coset_map.items():
  print(
      " = ".join([
          "{" + ', '.join(repr(coset_member) for coset_member in coset) + "}",
          *[repr(element)+"H" for element in elements]
      ])
  )
```

Running the program yields:

```
zmd@system76-pc:~/Documents/School/Algebra$ python3 symmetric_cosets.py
{1, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)} = 1H = (1 2)(3 4)H = (1 3)(2 4)H = (1 4)(2 3)H
{(3 4), (1 2), (1 3 2 4), (1 4 2 3)} = (3 4)H = (1 2)H = (1 3 2 4)H = (1 4 2 3)H
{(2 3), (1 2 4 3), (1 3 4 2), (1 4)} = (2 3)H = (1 2 4 3)H = (1 3 4 2)H = (1 4)H
{(2 3 4), (1 2 4), (1 3 2), (1 4 3)} = (2 3 4)H = (1 2 4)H = (1 3 2)H = (1 4 3)H
{(2 4 3), (1 2 3), (1 3 4), (1 4 2)} = (2 4 3)H = (1 2 3)H = (1 3 4)H = (1 4 2)H
{(2 4), (1 2 3 4), (1 3), (1 4 3 2)} = (2 4)H = (1 2 3 4)H = (1 3)H = (1 4 3 2)H
```