

Assignment #9

26 March 2025

Abstract

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

1. *Proposition.* $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} / \langle (2, 2) \rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. $\langle (2, 2) \rangle = \{(2, 2), (0, 4), (2, 6), (0, 8), (2, 10), (0, 0)\}$

$|(0, 1) + \langle (2, 2) \rangle| = 4$ because $4 \cdot (0, 1) = (0, 4) \in \langle (2, 2) \rangle$.

$|(1, 0) + \langle (2, 2) \rangle| = 4$ because $4 \cdot (1, 0) = (0, 0) \in \langle (2, 2) \rangle$.

The existence of elements of order 4 rules out $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

But the maximum order of an element is 4, because any element of the quotient group must take the form $((1, 0) + \langle (2, 2) \rangle)^a ((1, 0) + \langle (2, 2) \rangle)^b$, whose order is bounded by $\text{lcm}(a, b)$, and $\text{lcm}(4, 4) = 4$, which rules out $\mathbb{Z}/8\mathbb{Z}$.

2. *Proposition.* $(\mathbb{Z}/32\mathbb{Z})^\times / \{1, 31\} \cong \mathbb{Z}/8\mathbb{Z}$.

Proof. Let $H := \{1, 31\}$. $(\mathbb{Z}/32\mathbb{Z})^\times$ is known to be generated by 3 and 31 (shown in the table at

https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n#Examples_2). We have $31H = H$

(and $|31| = 2$), whereas $|3| = 8$, but an element of order 8 rules out $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. $G := (\mathbb{Z}/16\mathbb{Z})^\times$, $H := \{1, 15\}$, $K := \{1, 9\}$.

Proposition. $H \cong K$.

Proof. $15 \cdot 15 \pmod{16} = 1$ and $9 \cdot 9 \pmod{16} = 1$. Alternatively, there is only one group of order 2.

Proposition. $G/H \not\cong G/K$.

Proof. K does not have any elements of order 4, but H does (e.g., $3^2 \pmod{16} = 9$, $3^3 \pmod{16} = 11$, $3^4 \pmod{16} = 1$, but in H , 3 is in a coset with 13, which is not equal to 11 or 9). This was checked using the following Python program (modified from Assignment #2):

```
def quotient_group_of_units_element_orders(n, H):
    orders = {}
    factors = {
        int(f)
        for f in subprocess.run(["/usr/bin/factor", str(n)], capture_output=True)
        .stdout.decode("utf-8")
        .split(": ")[1]
        .split()
    }
    for i in range(1, n):
        if any(i // f == i / f for f in factors):
            # not in the group
            continue
        x = i
        order = 1
        while x not in H:
            x *= i
            x %= n
            order += 1
        orders[i] = order
    return orders
```

```

if __name__ == "__main__":
    print(quotient_group_of_units_element_orders(16, [1, 9]))
    print(quotient_group_of_units_element_orders(16, [1, 15]))

```

4. *Theorem.* If $H \trianglelefteq G$, then $|gH| \mid |g|$.

Proof. Because $g^{|g|} = 1$, it follows that $gH^{|g|} = 1H$ because we can do coset arithmetic using representatives. But then $|g|$ is divisible by $|gH|$ by Corollary 2 of Gallian's Theorem 4.1

5. *Theorem.* Let $H \trianglelefteq G$. If G/H has an element of order n , then so does G .

Proof. Suppose that $|gH| = n$. By the previous exercise, $|g|$ is a multiple of n , that is, $g^{nk} = 1$ for some k .¹ So then $(g^k)^n = 1$, which is to say $|g^k| \leq n$.

We need to rule out that $|g^k| < n$. Suppose $|g^k| = m < n$. Then $(g^k)^m = g^{km} = 1$. Because nk is the smallest power of g that's equal to 1, we must have $nk \leq km$, which implies $n \leq m$. But earlier we said $m < n$. Contradiction!

¹Thanks to Claude Sonnet 3.7 and OpenAI o3-mini-high for guidance in what follows.