Assignment #2

30 January 2025

Abstract

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

1. **a**. The elements of $(\mathbb{Z}/20\mathbb{Z})^\times$ (I'm refusing to call it $U(20)$, which notation seems less motivated) are $\{1, 3, 7, 9, 11, 13, 17, 19\}$. Thus, $\left|(\mathbb{Z}/20\mathbb{Z})^\times\right| = 8$.

b. We want to find the order of all the elements of $(\mathbb{Z}/20\mathbb{Z})^\times$. Manual computation is beneath us, so let's write a computer program to do it. In Python:

```
import subprocess
def group_of_units_element_orders(n):
    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 != 1:
            x *= i
            x %= n
            order += 1
        orders[i] = order
    return orders
if __name__ == "__main__":
    print(group_of_units_element_orders(20))
```

Running this program yields the result

```
zmd@system76-pc:~/Documents/School/Algebra$ python3 u20_order.py
 {1: 1, 3: 4, 7: 4, 9: 2, 11: 2, 13: 4, 17: 4, 19: 2}
```

(The Claude Sonnet 3.5 LLM assistant (*claude.ai*) caught a bug in a previous revision of this program.)

2. **a**. In the additive group $\mathbb{Q}$, $\left\langle \frac{1}{2} \right\rangle = \left\{ \frac{-n}{2} : n \in \mathbb{N}_0 \right\} \cup \left\{ \frac{n}{2} : n \in \mathbb{N}_0 \right\}$

b. In the multiplicative group $\mathbb{Q}^\times$, $\left\langle \frac{1}{2} \right\rangle = \left\{ \frac{1}{2^n} : n \in \mathbb{N}_0 \right\} \cup \{2^n : n \in \mathbb{N}_0\}$

3. We're looking for an element b such that $b^3 = a$. $|a| = 7$ implies that the group has at least the elements $\{a, a^2, a^3, a^4, a^5, a^6, 1\}$. Our desired b might be one of the non-identity powers of a: if we call that power k, we would have $a^{3k} = a$, and thus, $3k \equiv 1 (\text{mod } 7)$. Going through the list: $3 \cdot 2 = 6$ is 6 mod 7 ✘, $3 \cdot 3 = 9$ is 2 mod 7 ✘, $3 \cdot 4 = 12$ is 5 mod 7 ✘, $3 \cdot 5 = 15$ is 1 mod 7 ✓. Thus $b := a^5$ works. (After being initially stuck on this exercise, I got hints from chatting to the DeepSeek R1 and Claude Sonnet 3.5 LLM assistants.)

4. **a**. *Theorem.* If $H \leq G$ and $K \leq G$, then $H \cap K \leq G$.

Proof. Suppose x, $y \in H$, K. By the subgroup criterion, $xy^{-1} \in H$ and $xy^{-1} \in K$. But that means that $xy^{-1} \in H \cap K$, which is *quod erat demonstrandum.*

b. In $\mathbb{Z}/12\mathbb{Z}$, $\langle 4 \rangle$ and $\langle 6 \rangle$ are subgroups, but $\langle 4 \rangle \cup \langle 6 \rangle$ is not a subgroup, because it's not closed: for example, $4 + 6 = 10$ (and $10 \notin \langle 4 \rangle, \langle 6 \rangle$).

5. *Theorem.* $C_G(a) \leq G$.

Lemma. If y commutes with a, then so does y^{-1}.

Proof. If $ya = ay$, then $yay^{-1} = ayy^{-1}$, so $yay^{-1} = a$, so $y^{-1}yay^{-1} = y^{-1}a$, so $ay^{-1} = y^{-1}a$. This proves the lemma.

Now suppose x, $y \in C_G(a)$. Then $xy^{-1}a = xay^{-1} = axy^{-1}$, so $xy^{-1} \in C_G(a)$, which is *quod erat demonstrandum.*