MATH 4041 Final

David Chen, dc3451

December 23, 2020

I had some extra time, so I decided to type up some of this to make the graders' lives easier. The handwritten copies are at the end.

Q1

i

Note first that under the construction of $\mathbb{N}$ given in this class, we define addition as $\text{succ}(n)$ for some successor function; in particular, f here is exactly the successor function by definition, and via the construction, we get that there is no preimage of 1 (or 0, I can't remember the convention used in this class for the least element of $\mathbb{N}$, I just use 1 as the least element, none of the proofs change at all).

For injectivity, $f(n) = f(m) \implies n+1 = m+1 \implies n = m$. To see f is not surjective (alternatively, see note above) we have that $f(n) = 1 \implies n+1 = 1 \implies n < 1$, but 1 is the least element of $\mathbb{N}$. $\Rightarrow\!\!\!\!\!\!\Leftarrow$, so we get that 1 has no preimage under f and thus f is not surjective. However, for $n > 1$, $n-1 \in \mathbb{N}$, so $f(n-1) = n$ and thus the image of f is all of $\mathbb{N} \setminus \{1\}$.

ii

Pick any $k \in \mathbb{N}$, and define

$$g_k(n) = \begin{cases} k & n = 1 \\ n-1 & \text{otherwise} \end{cases}$$

such that for any $n \in \mathbb{N}$, $g_k(f(n)) = g(n+1)$ and since $n+1 \neq 1$, $g_k(n+1) = (n+1)-1 = n$. Thus, g_k is a left inverse for f.

In particular, for $n > 1$ and any left inverse g, $n-1 \in \mathbb{N}$, so $g(f(n-1)) = g(n) = n-1$ so for $n > 1$, g must map $n \mapsto n-1$; however, we can pick any $k \in \mathbb{N}$ for $g(1)$, so we have found all such left inverses. This gives an infinite amount of left inverses for f.

iii

Since we have that for any $n \in \mathbb{N}$, $n+1 \in \mathbb{N}$, we have $g_k(n+1) = n$, so every element of $\mathbb{N}$ has a preimage, so g_k is surjective, but $g(1) = g(k+1) = k$, and since $k+1 \neq 1$ (otherwise $f(k) = 1$, $\Rightarrow\!\!\!\!\!\!\Leftarrow$), we have that g_k is not injective for any k, and thus no left inverse is ever injective.

iv

We have that $\mathrm{Im}(f \circ h) \subset \mathrm{Im}(f)$, since $(f \circ h)(n) = m \implies f(h(n)) = m$, $h(n) \in \mathbb{N}$. Then, $\nexists n \in \mathbb{N} \mid (f \circ h)(n) = 1$, since we would then get $h(n)$ as a preimage under f for 1; $\Rightarrow\!\!\!\!\!\!\Leftarrow$, so no right inverse exists.

Q2

(a)

The order of $(\mathbb{Z}/25\mathbb{Z})^*$ is $\varphi(25) = 25 \cdot (1 - 1/5) = 20$.

(b)

$$
\begin{aligned}
2^1 &= 2 \mod 25 \\
2^2 &= 2 \cdot 2 = 4 \mod 25 \\
2^4 &= (2^2)^2 = 16 \mod 25 \\
2^5 &= 2^4 \cdot 2 = 32 = 7 \mod 25 \\
2^{10} &= (2^5)^2 = 49 = -1 = 24 \mod 25 \\
2^{20} &= (2^{10})^2 = -1^2 = 1 \mod 25
\end{aligned}
$$

The order of 2 in $(\mathbb{Z}/25\mathbb{Z})^*$ must divide $|(\mathbb{Z}/25\mathbb{Z})^*| = 20$, so it must be one of $1, 2, 4, 5, 10, 20$. Since we checked manually that it is not $1, 2, 4, 5, 10$, it must be of order 20 and thus a generator of $(\mathbb{Z}/25\mathbb{Z})^*$, since $(\mathbb{Z}/25\mathbb{Z})^*$ is finite, $|\langle 2 \rangle| = |(\mathbb{Z}/25\mathbb{Z})^*|$ and $\langle 2 \rangle \leq (\mathbb{Z}/25\mathbb{Z})^*$.

(c)

This happens when a is coprime to 20, as seen in class, so $a = 1, 3, 7, 8, 11, 13, 17, 19$. There $\varphi(20) = 20 \cdot (1 - 1/2)(1 - 1/5) = 8$ of these.

(d)

An element 2^a is of order n when $20/\gcd(20,a) = n$. In particular, for order 4, we have $2^5, 2^{15}$, for order 5, we have $2^4, 2^8, 2^{12}, 2^{16}$ and there are no elements of order 3.

Q3

i

We have

$$\sigma = (1,6,7,2)(4,8,5)$$

Note that disjoint cycles commute, so if $\sigma = \rho_1\rho_2\cdots\rho_n$,

$$\sigma^2 = (\rho_1\rho_2\cdots\rho_n)(\rho_1\rho_2\cdots\rho_n) = (\rho_1\rho_1\rho_2\rho_2\cdots\rho_n\rho_n) = \rho_1^2\rho_2^2\cdots\rho_n^2$$

and via induction,

$$\sigma^{k+1} = (\rho_1^k\rho_2^k\cdots\rho_n^k)(\rho_1\rho_2\cdots\rho_n) = (\rho_1^k\rho_1\rho_2^k\rho_2\cdots\rho_n^k\rho_n) = \rho_1^{k+1}\rho_2^{k+1}\cdots\rho_n^{k+1}$$

so

$$\sigma^4 = (1,6,7,2)^4(4,8,5)^3(4,8,5) = (4,8,5)$$

and

$$\sigma^6 = (1,6,7,2)^4(1,6,7,2)^2(4,8,5)^3(4,8,5)^3 = (1,7)(6,2)$$

and

$$\sigma^{12} = ((1,7)(6,2))^2 = (1,7)^2(6,2)^2 = 1$$

and in particular, this shows that $\sigma^2 \neq 1$ and $\sigma^3 \neq 1$, since otherwise $\sigma^4 = (\sigma^2)^2 = 1$ and same for $\sigma^6 = (\sigma^3)^2$. However, the order of σ must divide 12, so it is one of $1,2,3,4,6,12$; but we checked that it is not 1,2,3,4,6, so it must be 12.

ii

We have seen in class that an n-cycle can be written as the product of $n-1$ transpositions, so

$$\varepsilon(\sigma) = \varepsilon((1,6,7,2))\varepsilon((4,8,5)) = (-1)^3(-1)^2 = -1$$

so σ is odd.

iii

a

There are 2 non-trivial orbits, and 1 orbit of size 1. Take $\sigma^n \in \langle\sigma\rangle$, and note that

$$\sigma^n = (1,6,7,2)^n(4,8,5)^n$$

so if $k \in \{1,6,7,2\}$, $\sigma^n(k) \in \{1,6,7,2\}$ (the first orbit) and if $k \in \{4,8,5\}$, $\sigma^n(k) \in \{4,8,5\}$ (the second orbit), since only one of the cycles in σ moves these k. Lastly, the orbit of order 1 is $G \cdot 3 = \{3\}$.

b

As above, this is $\{4,8,5\}$, which is of order 3.

c

Take any element $\sigma^n \in G$. Then, $\sigma^n = \sigma^{3q+r}$ for $r = 0,1,2$, so $\sigma^n = (1,6,7,2)^n(4,8,5)^{3q}(4,8,5)^r$, but clearly the part $(1,6,7,2)^n$ fixes $\{4,8,5\}$, so we only care about $(4,8,5)^{3q}(4,8,5)^r = (4,8,5)^r$. Then, we have that $r = 1$ takes $5 \mapsto 4$ and $r = 2$ takes $5 \mapsto 8$, so we get that $r = 0$, so the stabilizer is $\{1, \sigma^3, \sigma^6, \sigma^9\}$, of order 4 (also computable via $|G|/|G_5| = 12/3$).

Q4

See the scans at the end of the pdf.

Q5

We have that Fermat gives $7^{22} \equiv 1 \mod 23$, so $7^{68} = (7^{22})^3 \cdot 7^2 \equiv 49 \equiv 3 \mod 23$, so the remainder will be $a = 3$.

Q6

i

We have directly from class that

$$|G| = |G_x| \cdot |G \cdot x|$$

or as we will use later $G_x = \frac{|G|}{|G \cdot x|}$.

ii

We have that conjugation of a product of disjoint cycles of lengths $r_1, r_2, \ldots, r_n$ results in a product of disjoint cycles of lengths $r_1, r_2, \ldots, r_n$ from one of the homeworks. Then, we have that the conjugacy class is some subset of $\{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ which on inspection are the only products of disjoint transpositions in S_4. Then, checking that all 3 are achieved,

$$\begin{aligned} 1 \cdot (1,2)(3,4) \cdot 1 &= (1,2)(3,4) \\ (1,3) \cdot (1,2)(3,4) \cdot (1,3) &= (1,4)(2,3) \\ (1,4) \cdot (1,2)(3,4) \cdot (1,4) &= (1,3)(2,4) \end{aligned}$$

so the orbit is exactly $\{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ which is of order 3.

iii

By definition, the centralizer of $(1,2)(3,4)$ is

$$\{g \in S_4 \mid g(1,2)(3,4)g^{-1} = (1,2)(3,4)\}$$

but this is also exactly the stablizer of $(1,2)(3,4)$ w.r.t the earlier group action. Then, from the first part, we get that the stablizer is going to have order $24/3 = 8$; since $8 = 2^3$ and $24 = 3 \cdot 2^3$, it must also be a 2-Sylow subgroup of S_4, which has order 24.

Q7

See the scans below.

Q8

Note $44 = 2^2 \cdot 11$, and has divisors $1, 2, 4, 11, 44$.

i

The order of a 2-Sylow subgroup will be $2^2 = 4$. The odd (that is, $\equiv 1 \mod 2$) divisors of 44 are 1 and 11, so there is either 1 or 11 2-Sylow subgroups.

ii

The order of an 11-Sylow subgroup will be 11. The $\equiv 1 \mod 11$ divisor of 44 is exactly 1, so there is a unique 11-Sylow subgroup.

iii

Since conjugating an 11-Sylow subgroup gives rise to another 11-Sylow subgroup, if H is that unique 11-Sylow subgroup, $gHg^{-1} = H$ for all $g \in G$, so H is normal and a nontrivial subgroup of G, so G is not simple.