Homework 3
MATH 541: Abstract Algebra 1
Spring 2023

Hongtao Zhang

Sec. 0.1: 7
Sec. 0.2: 7
Sec. 0.3: 8
Sec. 1.7: 18, 19, 23
Sec. 2.1: 3

0.1.7

Proof. To be an equivalence relation, we need three condtions.

$$\begin{cases} a \sim a \\ a \sim b \iff b \sim a \\ a \sim b \wedge b \sim c \implies a \sim c \end{cases}$$

It is very clear that $a \sim a$ because by the definitions of a function f, $f(a) = f(a)$.
If $f(a) = f(b)$ then $f(b) = f(a)$ so $a \sim b \implies b \sim a$.
$f(a) = f(b) \wedge f(b) = f(c) \implies f(a) = f(c)$, so $a \sim b \wedge b \sim c \implies a \sim c$.
We know that the fibers of element y are $\{x \in X : f(x) = y\}$. Therefore, it is very clear that if $a \sim b$, then a,b are in the fibers of $f(a)$. □

0.2.7

Proof. Proof by contradiction

Assume there exists an a such that $a^2 = pb^2$, and write $a = \prod_n p_{an}, b = \prod_n p_{bn}$ then we know that $a^2 = (\prod_n p_{an})^2 = pb^2 = p(\prod_n p_{bn})^2$

Because we know that for every integer, there's an unique prime decomposition, so the power of left primes must match the power of right primes.

However, because we know that p is a prime, and all primes component from b will have even power, so the power of p must be odd, which mismatched the power of a's decomposition, which is a contradiction. □

0.3.8

0.3.6

Proof. the square of $\bar{0}^2 = \bar{0}$ Assume we have an element a in $\bar{1}$, write $a = (4b+1)$ for some integer b.

$$a^2 = aa = (4b+1)(4b+1) = 16b + 4b + 4b + 1 \mod 4 = 1$$

For $\bar{2}$

$$(4b+2)(4b+2) = 16b + 8b + 8b + 4 \mod 4 = 0$$

For $\bar{3}$

$$(4b+3)(4b+3) \mod 4 = 9 \mod 4 = 1$$

$\square$

0.3.7

Proof. We know that $a^2, b^2 \mod 4 = 0$ or 1, therefore $a^2 + b^2 \mod 4 \leq 2$ $\square$

0.3.8

Proof. Proof by contradiction

Assume the solution exists.

We know that $a^2 + b^2 \mod 4 \neq 3$, so $c^2 \mod 4 \neq 1$, which means $c^2 \mod 4 = 0$

Also we know that $a^2 \mod 4 < 2$, and we know that $c^2 \mod 4 = 0$.

Therefore, $(a^2 + b^2) \mod 4 = 0$

Therefore $a^2 \mod 4 = b^2 \mod 4 = 0$.

Therefore, $\frac{a^2}{4}, \frac{b^2}{4}, \frac{c^2}{4} \in \mathbb{Z}$.

Therefore, $\frac{a^2}{4}, \frac{b^2}{4}, \frac{c^2}{4}$ satisfy the same constraint, so we can contiuously divide out by 4, and the equation still satisfy.

However, it is impossible for a^2, b^2, c^2 to have infinite many factor of 4, which is a contradiction.

$\square$

1.7.18

Proof. 1. Reflexivity. This is true because $\mathbb{1} \in H$, and $\mathbb{1}a = a$

2. Symmetry. This is true because inverse.

$$a \sim b \implies \exists h : ha = b \implies h^{-1}b = a$$

The argument is symmetric so the other side is the same.

3. transitivity. This is true because group is closed.

$$a \sim b, b \sim c \implies \exists h_1, h_2 : h_1 a = b, h_2 b = c$$

$$\implies h_2 h_1 a = c \implies \exists k = h_2 h_1 \in H : ka = c \implies a \sim c$$

$\square$

1.7.19

Bijection

Proof. Proof of Injective by contradiction

Suppose $\exists h_1, h_2 : h_1 \neq h_2 \wedge h_1 x \equiv h_2 x$, because $\exists x^{-1} : h_1 x x^{-1} = h_2 x x^{-1} = h_1 = h_2$, which is a contradtion.

Proof of surjective

There's nothing to be proved here because by definition $\forall o \in \mathcal{O} : \exists h : hx = o$.

$\square$

Lagrange's Theorem

Proof. From the preceding exercise we know that by applying h to the element, we can define an equivalence relation.

Therefore, we can see that $\mathcal{O}_x$ will define a partition of G.

Further we know that $\forall x, y \in G \wedge \mathcal{O}_x \neq \mathcal{O}_y : |\mathcal{O}_x| = |\mathcal{O}_y| = |H|$.

Because $\mathcal{O}$ is a partition, so $|G| = \sum_x \mathcal{O}_x$, combining the previous two statement, $\exists u \in \mathbb{Z} : |G| = u|\mathcal{O}| \implies |G| = u|H|$. □

2.1.3

a

Proof. Check closed under inversion.

$$r^4 = \mathbb{1} \implies r^2 r^2 = \mathbb{1} \implies r^2 = (r^2)^{-1}$$

$$s^2 = \mathbb{1} \implies s = s^{-1}$$

$$(sr^2)^2 = sr^2 sr^2 = sr^2 r^{-2} s = ss = \mathbb{1} \implies sr^2 = (sr^2)^{-1}$$

Closed under multiplcation (skip some trivial cases)

$$r^2 s = r^2 s = r^{-2} s = sr^2$$

$$r^2 sr^2 = sr^{-2} r^2 = s$$

$$sr^2 r^2 = s\mathbb{1} = s$$

$$ssr^2 = r^2$$

$$sr^2 s = ssr^{-2} = r^{-2} = r^2$$

□

b

Proof. Close under inversion:

r^2 has been checked before

$$srsr = srr^{-1}s = \mathbb{1}$$

$$sr^3 sr^3 = sr^3 r^{-3} s = \mathbb{1}$$

Close under multiplcation (skip trivial)

$$r^2 sr = r^2 r^{-1} s = rs = sr^{-1} = sr^3$$

$$r^2sr^3 = r^{-1}s = sr$$

$$sr^3r^2 = sr^5 = sr$$

$$srsr^3 = srr^{-3}s = sr^-2s = s^2r^2 = r^2$$

$$sr^3sr = sr^3r^{-1}s = sr^2s = ssr^{-2} = r^{-2} = r^2$$

$\square$