

# Homework

Ding Yaoyao, 516030910572

2017-09-22

## Exercise 1-3

5

- Closure: If  $a, b \in G$ , there are  $c, d \in G$  such that  $a = c^m, b = d^m$ . Then  $ab = c^m d^m = (cd)^m \in G$  (Because group  $G$  is an abelian group).
- Identity:  $e = e^m \in G$ .
- Inverse: If  $a = b^m \in G$ , then  $a^{-1} = (b^m)^{-1} = (b^{-1})^m \in G$ .

Above all,  $H \leq G$ .

6

Because  $H$  is not empty,  $gHg^{-1}$  is not empty.

For all  $a, b \in gHg^{-1}$ , there are  $c, d \in H$  such that  $a = gcg^{-1}, b = gdg^{-1}$ .

Then  $a^{-1}b = (gcg^{-1})^{-1}gdg^{-1} = gc^{-1}g^{-1}gdg^{-1} = gc^{-1}dg^{-1}$ .

Because  $c^{-1}d \in H$ , we have  $a^{-1}b \in gHg^{-1}$ .

Finally, we get  $gHg^{-1} \leq G$ .

7

Because  $ea = ae, e \in C(a)$ . For all  $b, c \in C(a)$ , we have  $ba = ab$  and  $ca = ac$ .

Then  $b^{-1}c = (aba^{-1})^{-1}aca^{-1} = ab^{-1}a^{-1}aca^{-1} = ab^{-1}ca^{-1}$ , which imply that  $ab^{-1}c = b^{-1}ca, b^{-1} \in C(a)$ .

Above all,  $C(a) \leq G$ .

8

$g \in C(G) \Leftrightarrow \forall a \in G, ga = ag \Leftrightarrow \forall a \in G, g \in C(a) \Leftrightarrow g \in \bigcap_{a \in G} C(a)$ , then we have:

$$C(G) = \bigcap_{a \in G} C(a)$$

## 18

- $\langle m, n \rangle \subseteq \langle d \rangle$ :  $a \in \langle m, n \rangle \Rightarrow \exists k_1, k_2, a = k_1 m + k_2 n = (k_1 \frac{m}{d} + k_2 \frac{n}{d})d \Rightarrow a \in \langle d \rangle$ .
- $\langle d \rangle \subseteq \langle m, n \rangle$ : By the Euclid theorem,  $\exists k_1, k_2, d = k_1 m + k_2 n$ . If  $a \in \langle d \rangle$ , we have  $a = kd = k(k_1 m + k_2 n) = (kk_1)m + (kk_2)n$ , which means  $a \in \langle m, n \rangle$ .

Above all,  $\langle m, n \rangle = \langle d \rangle$ .

## 19

It's obvious that  $m = \pm n$  imply  $\langle m \rangle = \langle n \rangle$ , we only need to prove  $\langle m \rangle = \langle n \rangle \Rightarrow m = \pm n$ .

If  $\langle m \rangle = \langle n \rangle$ , we have  $m \in \langle m \rangle = \langle n \rangle$ .

There two cases:

- $m = 0$  or  $n = 0$ : we have  $\langle m \rangle = \langle n \rangle = 0$ , which means  $m = n = 0$ . So  $m = \pm n$ .
- $m \neq 0$  and  $n \neq 0$ :  $n \in \langle n \rangle = \langle m \rangle$ , which means  $m \mid n$ . We can get  $n \mid m$  by the same method.  $n \mid m$  and  $m \mid n$  means  $m = \pm n$ .