Homework

Ding Yaoyao, 516030910572

2017-09-29

Exercise 1-4

Additional

Problem: If $N = n_1 n_2$, and $gcd(n_1, n_2) = 1$, then $Z_n^* \cong Z_{n_1}^* \times Z_{n_2}^*$.

Proof:

- Define the map φ: $Z_n^* \to Z_{n_1}^* \times Z_{n_2}^*$ by $\varphi(x) = (x\ mod\ n_1, x\ mod\ n_2)$.
- φ is injective: If $(x\ mod\ n_1, x\ mod\ n_2) = (y\ mod\ n_1, y\ mod\ n_2)$, then $n_1 \mid x - y$ and $n_2 \mid x - y$. Beacuse n_1 and n_2 are co-prime, $n_1 n_2 \mid x - y$, which means $n \mid x - y$. Thus $x = y$(when $x, y \in [0, n)$).
- φ is surjective: For all $(x_1, x_2) \in Z_{n_1}^* \times Z_{n_2}^*$, exist $x \in Z_n^*$ such that $x\ mod\ n_1 = x_1$ and $x\ mod\ n_2 = x_2$ by the Chinese Remainder Theorem(when $gcd(n_1, n_2) = 1$).
- φ is homomorphic: $\varphi(xy) = (xy\ mod\ n_1, xy\ mod\ n_2)$
  $= ((x\ mod\ n_1)(y\ mod\ n_1)\ mod\ n_1, (x\ mod\ n_2)(y\ mod\ n_2)\ mod\ n_2)$
  $= (x\ mod\ n_1, x\ mod\ n_2)(y\ mod\ n_1, y\ mod\ n_2)$
  $= \varphi(x)\varphi(y)$.

Above all, $Z_n^* \cong Z_{n_1}^* \times Z_{n_2}^*$.

3

- $\Rightarrow$: For all $x \in G$, exist $y \in G$ such that $y^{-1} = x$. So ϕ is surjective. If $\phi(x) = \phi(y)$(i.e. $x^{-1} = y^{-1}$), we have $x = y$. So ϕ is injective. Beacuse group G is an abelian group, we have:
  $$\phi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \phi(x)\phi(y)$$
  Then ϕ is homomorphic. Above all, ϕ is an isomorphism(exactly automorphism).
- $\Leftarrow$: Beacuse ϕ is an isomorphism, we have:
  $$xy = ((xy)^{-1})^{-1} = \phi((xy)^{-1}) = \phi(y^{-1}x^{-1}) = \phi(y^{-1})\phi(x^{-1}) = yx$$
  (for all $x, y \in G$). So group G is an abelian group.

4

- injective: If $\phi(x) = \phi(y)$, then $axa^{-1} = aya^{-1}$. By the cancellation law of group, we get $x = y$.
- surjective: For all $x \in G$, exist $y = a^{-1}xa \in G$ such that $aya^{-1} = x$.
- homomorphic: $\phi(xy) = a^{-1}xya = a^{-1}x(aa^{-1})ya = (a^{-1}xa)(a^{-1}ya) = \phi(x)\phi(y)$.

Above all, ϕ is an isomorphism(also called inner automorphism).

6

$H = \langle 1 \rangle, G = \langle 2 \rangle, R = \langle 4 \rangle$($\langle k \rangle$ means group $(\{kn \mid n \in \mathbb{Z}\}, +)$).

It's obvious that $\langle 4 \rangle < \langle 2 \rangle < \langle 1 \rangle$ and $\langle 2 \rangle \cong \langle 2 \rangle$(by the identity isomorphism). And I only need to prove $\langle 1 \rangle \cong \langle 4 \rangle$.

Let's define the mapping ϕ: $\langle 1 \rangle \to \langle 4 \rangle$ as $\phi(x) = 4x$ for all $x \in \mathbb{Z}$.

- injective: If $\phi(x) = \phi(y)$, then $4x = 4y$. We can get $x = y$.
- surjective: For all $x \in \langle 4 \rangle$, by the definition of $\langle 4 \rangle$, exist $y \in \mathbb{Z}$ such that $4y = x$(i.e. $\phi(y) = x$).
- homomorphic: $phi(x + y) = 4(x + y) = 4x + 4y = \phi(x) + \phi(y)$.

Above all, ϕ is an isomorphism, which means $\langle 1 \rangle \cong \langle 4 \rangle$.

Exercise 1-5

1

Table 1: Z_7

n	0	1	2	3	4	5	6
ord	1	7	7	7	7	7	7

Table 2: Z_8

n	0	1	2	3	4	5	6	7
ord	1	8	4	8	2	8	4	8

Table 3: Z_{10}

n	0	1	2	3	4	5	6	7	8	9
ord	1	10	5	10	5	2	5	10	5	10

Table 4: Z_{14}

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
ord	1	14	7	14	7	14	7	2	7	14	7	14	7	14

Table 5: Z_{15}

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ord	1	15	15	5	15	3	5	15	15	5	3	15	5	15	15

Table 6: Z_{18}

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
ord	1	18	9	6	9	18	3	18	9	2	9	18	3	18	9	6	9	18

5

$U(n)$ is an cyclic group for all $n \in \mathbb{Z}^+$.

The generators:

- $U(8)$:$e^{2\pi i\frac{1}{8}}$, $e^{2\pi i\frac{3}{8}}$, $e^{2\pi i\frac{5}{8}}$, $e^{2\pi i\frac{7}{8}}$
- $U(9)$:$e^{2\pi i\frac{1}{9}}$, $e^{2\pi i\frac{2}{9}}$, $e^{2\pi i\frac{4}{9}}$, $e^{2\pi i\frac{5}{9}}$, $e^{2\pi i\frac{7}{9}}$, $e^{2\pi i\frac{8}{9}}$
- $U(10)$:$e^{2\pi i\frac{1}{10}}$, $e^{2\pi i\frac{3}{10}}$, $e^{2\pi i\frac{7}{10}}$, $e^{2\pi i\frac{9}{10}}$
- $U(13)$:$e^{2\pi i\frac{1}{13}}$, $e^{2\pi i\frac{2}{13}}$, $e^{2\pi i\frac{3}{13}}$, $e^{2\pi i\frac{4}{13}}$, $e^{2\pi i\frac{5}{13}}$, $e^{2\pi i\frac{6}{13}}$, $e^{2\pi i\frac{7}{13}}$, $e^{2\pi i\frac{8}{13}}$, $e^{2\pi i\frac{9}{13}}$, $e^{2\pi i\frac{10}{13}}$, $e^{2\pi i\frac{11}{13}}$, $e^{2\pi i\frac{12}{13}}$
- $U(14)$:$e^{2\pi i\frac{1}{14}}$, $e^{2\pi i\frac{3}{14}}$, $e^{2\pi i\frac{5}{14}}$, $e^{2\pi i\frac{9}{14}}$, $e^{2\pi i\frac{11}{14}}$, $e^{2\pi i\frac{13}{14}}$
- $U(21)$:$e^{2\pi i\frac{1}{21}}$, $e^{2\pi i\frac{2}{21}}$, $e^{2\pi i\frac{4}{21}}$, $e^{2\pi i\frac{5}{21}}$, $e^{2\pi i\frac{8}{21}}$, $e^{2\pi i\frac{10}{21}}$, $e^{2\pi i\frac{11}{21}}$, $e^{2\pi i\frac{13}{21}}$, $e^{2\pi i\frac{16}{21}}$, $e^{2\pi i\frac{17}{21}}$, $e^{2\pi i\frac{19}{21}}$, $e^{2\pi i\frac{20}{21}}$

12

We only need to prove:

$$(gag^{-1})^r = e \Longleftrightarrow a^r = e$$

- $\Rightarrow$: If $(gag^{-1})^r = ga^r g^{-1} = e$, we have $ga^r = g$, which means $a^r = e$.

- $\Leftarrow$: $(gag^{-1})^r = ga^r g^{-1} = gg^{-1} = e$.