FAA HW (Group & Ring)

Jiete XUE

September 21, 2025

15. (1) We know that the composition of mapping is associative. And easy to check that in this case, the composition is closed. $e = \mathrm{Id}_E, f \circ f^{-1} = \mathrm{Id}_E$. Hence $\mathcal{S}_E$ equipped with composition of mapping forms a group.

    (2) $\sigma^0(x) = x$. $\phi_\sigma(n + m, x) = \sigma^{(n+m)}(x) = \sigma^n \circ \sigma^m(x) = \phi_\sigma(n, x) \circ \phi_\sigma(m, x)$. So ϕ_σ defines a left action of $\mathbb{Z}$ on E.

    (3) $\forall \sigma^n(x) \in \mathrm{Orb}_\sigma(x), \sigma(\sigma^n(x)) = \sigma \circ \sigma^n(x) = \sigma^{n+1}(x) \in \mathrm{Orb}_\sigma(x)$. Hence $\sigma(\mathrm{Orb}_\sigma(x)) \subseteq \mathrm{Orb}_\sigma(x)$.

    (4) We claim that x, y both in a same orbit is a equivalence relation. Reflexivity: $x \in \mathrm{Orb}_\sigma(x) \Leftrightarrow x \in \mathrm{Orb}_\sigma(x)$. Transitivity: $x \sim y \Rightarrow \exists n \in \mathbb{Z}, \sigma^n(x) = y, y \sim z \Rightarrow \exists m \in \mathbb{Z}, \sigma^m(y) = z$. Thus $\sigma^{n+m}(x) = z, x \sim z$. Symmetry: $x \sim y \Rightarrow \exists n \in \mathbb{Z}, \sigma^n(x) = y, \sigma^{-n}(y) = x$. Hence $y \sim x$. Therefore, if $x \in O_i$, then $x \notin O_j, i \neq j$. So $\sigma_i(x) = \sigma(x), \sigma_j(x) = x, i \neq j$. $\forall x \in E, \sigma_1 \dots \sigma_n(x) = \sigma(x)$, hence $\sigma = \sigma_1 \dots \sigma_n$.

16. (1) By definition.

    (2) Let n be the largest cardinal of its orbits and O be the orbit that has more than one element. Then for any element x in any other orbit, $\sigma(x) = x$. Moreover, $\forall m \in \mathbb{Z}, \sigma^m(x) = x$. While n is the order of σ on O, for any $x \in E$, $\sigma^n(x) = x$, n is the order of σ. This relation is NOT hold generally. If there exists two orbits O_1, O_2 , there cardinal are n, m and $m > n > 1, \gcd(n, m) = 1$, then for the element $x \in O_1$, $\sigma^m(x) \neq x$. So m is not the order of σ.

    (3) For any $y \notin \mathrm{Orb(x)}, \sigma(y) = y = \tau_{x_i, x_{i+1}},\ i \in \{0, \dots, p-1\}$.

    $$\tau_{x_i, x_{i+1}}(\tau_{x_{i+1}, x_{i+2}}(\dots(x_i))) = \tau_{x_i, x_{i+1}}(x_i) = x_{i+1},$$

    $$\tau_{x_1, x_2}(\dots(\tau_{x_{i-1}, x_i}(x_{i+1}))) = x_{i+1}.$$

    Hence, $\forall i \in \{0, \dots, p-1\},\ \sigma(x_i) = \tau_{x_1, x_2} \dots \tau_{x_{p-2}, x_{p-1}}(x_i)$. Therefore,

    $$\sigma = \tau_{x_1, x_2} \dots \tau_{x_{p-2}, x_{p-1}}.$$

(4) Take O_i from $\langle\sigma\rangle\backslash E$, let

$$\sigma_i(x) := \begin{cases} \sigma(x) & \text{if } x \in O_i \\ x & \text{if } x \notin O_i \end{cases}.$$

Similarly to (3), we can get $\sigma = \sigma_1 \dots \sigma_n$, where $n = \mathrm{Card}[\langle\sigma\rangle\backslash E]$. Since σ_i is the composition of transpositions, any $\sigma \in \mathcal{S}_E$ can be written in the form of composition of transpositions.

5. Let

$$f : \mathbb{Q} \longrightarrow \mathbb{Q}$$

be a automorphism. Then

$$f(1) = 1.$$

For any $n \in \mathbb{N}$,

$$f(n) = f\left(\sum_{i=1}^{n} 1\right) = \sum_{i=1}^{n} f(1) = nf(1) = n.$$

$$0 = f(0) = f(n + (-n)) = f(n) + f(-n) = n + f(-n).$$

So, $f(-n) = -n$. Let $(n, m) \in \mathbb{Z}$,

$$f(n) = f(m)f(\frac{n}{m}),$$

$$f(\frac{n}{m}) = \frac{n}{m}.$$

Therefore, for any $x \in \mathbb{Q}$, $f(x) = x$, which means

$$f = \mathrm{Id}_{\mathbb{Q}}.$$

11. (1)

$$\left(\sum_{n\in\mathbb{N}} a_n T^n\right) \dagger \left(\sum_{n\in\mathbb{N}} b_n T^n\right) = \sum_{n\in\mathbb{N}} (a_n + b_n) T^n$$

$$= \sum_{n\in\mathbb{N}} (b_n + a_n) T^n = \left(\sum_{n\in\mathbb{N}} b_n T^n\right) \dagger \left(\sum_{n\in\mathbb{N}} a_n T^n\right).$$

So $\dagger$ is a communitative composition law.
For any $\sum_{n\in\mathbb{N}} a_n T^n \in k[[T]]$,

$$\left(\sum_{n\in\mathbb{N}} a_n T^n\right) \dagger \sum_{n\in\mathbb{N}} 0T^n = \left(\sum_{n\in\mathbb{N}} a_n T^n\right).$$

So $\sum_{n\in\mathbb{N}} 0T^n$ is the neutral element of $k[[T]]$.
For any $\sum_{n\in\mathbb{N}} a_n T^n \in k[[T]]$,

$$\left(\sum_{n\in\mathbb{N}} a_n T^n\right) \dagger \left(\sum_{n\in\mathbb{N}} -a_n T^n\right) = \sum_{n\in\mathbb{N}} 0T^n,$$

$$\left(\sum_{n\in\mathbb{N}} -a_nT^n\right) \dagger \left(\sum_{n\in\mathbb{N}} a_nT^n\right) = \sum_{n\in\mathbb{N}} 0T^n.$$

Therefore, $k[[T]]$ equipped with $\dagger$ forms a communitative group.

(2) Note that, for any $\sum_{n\in\mathbb{N}} a_nT^n \in k[[T]]$,

$$\left(\sum_{n\in\mathbb{N}} a_nT^n\right) * \sum_{n\in\mathbb{N}} \mathbb{1}T^n = \sum_{n\in\mathbb{N}} \left(\sum_{i=0}^{n} a_i\mathbb{1}T^n\right) = \sum_{n\in\mathbb{N}} a_nT^n.$$

Hence $\sum_{n\in\mathbb{N}} eT^n$ is the neutral element of $k[[T]]$. One has

$$\sum_{i=0}^{n} a_ib_{n-i} = \sum_{t=n}^{0} a_{n-t}b_t = \sum_{t=0}^{n} b_ta_{n-t}.$$

Thus, $*$ is communitative. Therefore, what given is a communitative monoid.

(3)

$$a_i = a\delta_{i,n}, b_i = b\delta_{i,m}.$$

$$(aT^n)(bT^m) = \sum_{k\in\mathbb{N}}\sum_{i=0}^{k} ab\delta_{i,n}\delta_{k-i,m}T^k = abT^{n+m}.$$

(4) We only need to check it's distributive.

$$\begin{aligned}
&\left(\sum_{n\in\mathbb{N}} a_nT^n\right) * \left[\left(\sum_{n\in\mathbb{N}} b_nT^n\right) \dagger \left(\sum_{n\in\mathbb{N}} c_nT^n\right)\right] \\
=&\left(\sum_{n\in\mathbb{N}} \left(\sum_{i=0}^{n} a_i(b_{n-i} + c_{n-i})\right) T^n\right) \\
=&\left(\sum_{n\in\mathbb{N}} \left(\sum_{i=0}^{n} a_ib_{n-i}T^n + \sum_{i=0}^{n} a_ic_{n-i}T^n\right)\right) \\
=&\left(\sum_{n\in\mathbb{N}}\sum_{i=0}^{n} a_ib_{n-i}T^n\right) \dagger \left(\sum_{n\in\mathbb{N}}\sum_{i=0}^{n} a_ic_{n-i}T^n\right) \\
=&\left(\sum_{n\in\mathbb{N}} a_nT^n\right) * \left(\sum_{n\in\mathbb{N}} b_nT^n\right) \dagger \left(\sum_{n\in\mathbb{N}} a_nT^n\right) * \left(\sum_{n\in\mathbb{N}} c_nT^n\right).
\end{aligned}$$

(5) (a) Suppose f is invertible, and $g = \sum\limits_{n\in\mathbb{N}} b_nT^n$ be its inverse, then by (2), $(b_i)_{i\in\mathbb{N}}$ satisfies:

$$\sum_{i=0}^{n} a_ib_{n-i} = \mathbb{1}, \forall n \in \mathbb{N}.$$

Take $n = 0$, we obtain a_0 must be invertible.

(b) Suppose a_0 is invertible. For any $n \in \mathbb{N}$, let

$$b_{n+1} = \left(\mathbb{1} - \sum_{i=1}^{n+1}(a_i b_{n+1-i})\right) a_0^{-1},$$

then,

$$\sum_{i=0}^{n+1}(a_i b_{n+1-i}) = \mathbb{1}.$$

Hence $g = \sum\limits_{n\in\mathbb{N}} b_n T^n$ is the inverse of f.

(6) Follow the algorithm in (5), we can easily get the result.

$$(1 - aT)^{-1} = \sum_{n\in\mathbb{N}} a^n T^n.$$

(7) -

(8) k is communitative. We claim that D is a homomorphism.

$$\begin{aligned} D(f_1) \dagger D(f_2) &= \left(\sum_{n\in\mathbb{N}}(n+1)a_{1,(n+1)}T^n\right) \dagger \left(\sum_{n\in\mathbb{N}}(n+1)a_{2,(n+1)}T^n\right) \\ &= \sum_{n\in\mathbb{N}}(n+1)(a_{1,(n+1)} + a_{2,(n+1)})T^n \\ &= D\left(f_1' \dagger f_2'\right). \end{aligned}$$

$$D\left(\sum_{n\in\mathbb{N}} 0T^n\right) = \sum_{n\in\mathbb{N}}(n+1)0T^n = \sum_{n\in\mathbb{N}} 0T^n.$$

Then we prove it is surjective. For any $f' = \sum_{n\in\mathbb{N}} b_n T^n$, let $a_n = b_{n-1}(n-1)^{-1}$, $n \neq 0$, $D[\sum_{n\in\mathbb{N}} a_n T^n] = f'$. Therefore D is a surjective k-linear mapping.

(9) Let $f = \sum\limits_{n\in\mathbb{N}} a_n T^n \in \ker(D)$, then for any $n \in \mathbb{N}, a_{n+1} = 0$. Thus,

$$\ker(D) = k.$$

(10)

$$a_{n+1} = a_n(n+1)^{-1}.$$

$$a_n = a_0 \prod_{i=0} n(i+1)^{-1}.$$

$$f = \sum_{n\in\mathbb{N}} a_0 \prod_{i=0} n(i+1)^{-1}T^n, \ \forall a_0 \in k.$$

16. (1) (a) (i)$\Rightarrow$ (ii): Let $\bar{b}$ be the inverse of $\bar{a}$. If $\bar{a}\bar{c} = 0$, then

$$0 = \bar{b}0 = \bar{b}(\bar{a}\bar{c}) = (\bar{b}\bar{a})\bar{c} = \bar{c}.$$

Hence $\bar{a}$ is not a zero divisor.

(b) (ii)$\Rightarrow$ (iii): We prove by contradiction. Assume $\gcd(a, n) = k, 1 < k < n$.Then

$$\bar{a}\frac{\bar{n}}{k} = 0.$$

That is contradicts to the fact that $\bar{a}$ is not a zero divisor.

(c) (iii)$\Rightarrow$ (i):

(2) By (1) (i)$\Rightarrow$ (iii), $(\mathbb{Z}/n\mathbb{Z})^\times \subseteq \{k \mid k \in [0, n-1], \gcd(k, n) = 1\}$.
By (1) (iii)$\Rightarrow$ (i), $\{k \mid k \in [0, n-1], \gcd(n, k) = 1\} \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$.
Hence $\{k \mid k \in [0, n-1], \gcd(n, k) = 1\} = (\mathbb{Z}/n\mathbb{Z})^\times$.

$$\phi(n) = \#\{k \mid k \in [0, n-1], \gcd(n, k) = 1\}.$$

(3) Suppose $\bar{\alpha}$ is invertible and let $\bar{\beta}$ be its inverse. Then,

$$\forall k \in \mathbb{N}, \bar{k} = k\bar{\beta}\bar{\alpha} = (k\beta)\bar{\alpha}.$$

So $\mathbb{Z}/n\mathbb{Z} = \{k\alpha\}_{k\in\mathbb{Z}}$.
Conversely, if $\mathbb{Z}/n\mathbb{Z} = \{k\alpha\}_{k\in\mathbb{Z}}$, then there exists $k \in \mathbb{Z}$ such that $\bar{k}\bar{\alpha} = 1$, which means $\bar{k}$ is $\bar{\alpha}$'s inverse. Thus, $\bar{\alpha}$ is invertible.

(4) -

(5) $\{x \mid x = a^n, n \in \mathbb{Z}\}$ forms a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. By Lagrange theorem, its order is a divisor of n. So $\bar{a}^{\phi(n)} = 1, a^{\phi(n)} \equiv 1(\mod n)$.

(6) There are $\frac{n}{p_i}$ elements in $\{k \in \mathbb{N}^* \mid k \le n\}$ satisfies $\gcd(k, p_i) = p_i \ne 1$. So, there are $n(1 - \frac{1}{p_i})$ elements in $\{k \in \mathbb{N}^* \mid k \le n\}$ satisfies $\gcd(k, p_i) = 1$. By (4),

$$\phi(n) = n\prod_{i=1}^{k}(1 - \frac{1}{p_i}).$$

(7) By definition of prime number, for any $n \in \mathbb{N}^*, n < p, \gcd(n, p) = 1$, so $\phi(p) = p - 1$. By (1), any element in $\mathbb{Z}/p\mathbb{Z}$ except 0 is invertible. For any $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}, \bar{a}\bar{b} = \overline{ab} = \overline{ba} = \bar{b}\bar{a}$. So $\mathbb{Z}/p\mathbb{Z}$ is commutative. Therefore $\mathbb{Z}/p\mathbb{Z}$ is a field.