1 Basic Logic

1. truth value:

P	Q	$P \wedge \neg P$	$P \vee \neg P$	$(P \vee Q) \Rightarrow (P \wedge Q)$	$(P \Rightarrow Q) \Rightarrow (Q \Rightarrow P)$
T	T	F	T	T	T
F	T	F	T	F	F
T	F	F	T	F	T
F	F	F	T	T	T

Table 1: truth value table

2. (1)$Q \wedge \neg Q$ =F,$P \Rightarrow (Q \wedge \neg Q) = \neg P \vee$F$= \neg P$
(2)$(P \wedge \neg Q) \Rightarrow Q = \neg P \vee Q \vee Q = \neg P \vee Q = P \Rightarrow Q$

3. (1)$P \wedge Q \Rightarrow R$
(2)$Q \Rightarrow P$
(3)$P \Leftarrow Q$

4. We denote that "bear is smart" as P,"bear is lazy" as Q, then "bear is not smart" can be denoted as $\neg P$. We have $(P \wedge Q \vee (\neg P)) \wedge P$,it's equivalent to $P \wedge Q$,then Q must be true .

6. We denote "At door 1,2,3" as P, Q, R ,one of them is true ,while we can get another information:one of $\neg P, \neg Q, Q$ is true. Due to "not Q then $\neg Q$",we can infer that $\neg P$ is false.(We can confirm while $Q = R$ =false,it can satisfies the requirements of the question)
so the treasure is behind the Door 1!

7. We denote ... can leads to the capital as P, Q, R, then $P \wedge (R \Rightarrow Q) = (\neg P) \wedge (\neg R) = P \wedge (\neg Q)$ =False. Combine the first and the third formula $P \wedge (\neg R \vee Q \vee \neg Q) = P$ =False, then from the second $\neg R$ =False. We are not sure about the stone path ,but we are sure that the dirt path can lead to capital.

8. Denote "$a + 1 == 0$" as P ,$b + 1 == 0$ as Q,then $ab + a + b \neq -1 = (a + 1)(b + 1) == 0 = \neg P \wedge \neg Q$

9. (1)Use the proof by contradiction.Not losing generality ,we assume that $a = 1$,

4 Ordering

1. $\frac{7}{13} < \frac{6}{11}$

2. If $ab < 0, a^2+b^2 > 0 > ab$.If $ab \geq 0, a^2+b^2 \geq 2ab \geq ab$.Thus, $a^2+b^2 \geq ab$.

3. Let $c = 1000000001$,then $a = (c+1)^2, b = (c-7)(c+7), a-b = 2c+50 > 0$.So $a > b$.

4. $\frac{2+\sqrt{3}}{2-\sqrt{3}} = 7 + 4\sqrt{3}$

5. (1) $x \in \,]-8, 2[$
   (2) $x \in \,]\frac{2}{3}, 6[$
   (3) $x \in \,]-2, 4[$

6. $x \in [-2, \frac{3+\sqrt{13}}{2}]$

7. (1) 0.
   (2) -1.
   (3) No.

8.
$$A^{\mathrm{u}} = \{x \in \mathbb{R} | \sqrt{2} \leq x\}, A^{\mathrm{l}} = \{x \in \mathbb{R} | -\sqrt{2} \geq x\}$$
$$\sup A = \sqrt{2}, \inf A = -\sqrt{2}$$
$$B^{\mathrm{u}} = \{x \in \mathbb{R} | x \geq 1\}, B^{\mathrm{l}} = \{x \in \mathbb{R} | x \leq 0\}$$
$$\sup B = 1, \inf B = 0$$

9. 2.

10. Cauchy's inequality.n^2

11. (1) (a) reflexive:$A \subseteq A$
   (b) transitive $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$
   (c) antisymmetric $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$
   (2) Denote $\bigcup_{i \in I} A_i$ as A
   $\forall i \in I, A_i \subseteq A$,so $A \in (A_i)^{\mathrm{u}}_{i \in I}$.$\forall B \in (A_i)^{\mathrm{u}}_{i \in I}, \forall i \in I, A_i \subseteq B$, so $A \subseteq B, A = \min(A_i)^{\mathrm{u}}_{i \in I}, \sup(A_i)_{i \in I} = A$.Similarly,$\inf(A_i)_{i \in I} = \cap_{i \in I} A_i$

12. The following is about induction,we skip it.

22. (1) (a) reflexive:$\forall n \in \mathbb{N}, n|n$
   (b) transitive:If $a|b, b|c$, where $(a, b, c) \in \mathbb{N}^3$,then $\exists (m, n) \in \mathbb{N}^2$ such that $b = am, c = nb$, so $c = (nm)a$, which leads to $a|c$.
   (c) antisymmetric:Let $a = mb, b = na, (m, n) \in \mathbb{N}^2$
   Then $1 = mn, m = n = 1$.Hence $a = b$
   Therefore $(\mathbb{N}, |)$ is a partially ordered set.

(2) Obvious.

(3) $\forall n \in \mathbb{N}, 1|n$.1 is the least element.

(4) $\forall n \in \mathbb{N}, n|0$.0 is the greatest element.

(5) If there exists a $n \in \mathbb{N}, n \neq 0$, such that $\forall a \in A, a|n$, then $a \leq n$.That contradicts to A is infinite.Thus n can only be 0.$\sup_{(\mathbb{N},|)} A = 0$

(6) (a) $\forall a \in A, a|n$,where,$n = \prod_{x \in A} x$,so $n \in M(A)$.

(b) Suppose $\exists n \in M(A), n_0 \nmid n$ we can write $n = dn_0 + r$,where $d, r \in \mathbb{N}, 0 < r < n_0$.Claim $r \in M(A)$:Take $x \in A$, since $n, n_0 \in M(A), \exists s, s_0 \in \mathbb{N}, xs = n, xs_0 = n_0$,then $xs = dxs_0 + r, x|r$,so$r \in M(A)$.That contradicts to the fact that n_0 is the least number in $M(A)$.

(c) $\sup A = n_0$

(7) (a) Let $x = \sum_{i=1}^{k} a_i n_i, y = \sum_{j=1}^{t} b_j m_j, \sum_{i=1}^{k} a_i n_i + \sum_{j=1}^{t} b_j m_j \in A\mathbb{Z}$.

(b) $\sum_{i=1}^{k} a_i (yn_i) \in A\mathbb{Z}$

(c) $\forall a \in A$, let $k = 1, a_1 = a, n_1 = 1$,we have $a \in A\mathbb{Z}$.$A \cap (\mathbb{N} \backslash \{0\}) \neq \varnothing$,hence,$(A\mathbb{Z}) \cap (\mathbb{N} \backslash \{0\}) \neq \varnothing$.

(d) $\{d\} \subseteq A\mathbb{Z}$.By (b), we have $d\mathbb{Z} \subseteq A\mathbb{Z}$.If $A\mathbb{Z} \nsubseteq d\mathbb{Z}$,then $\exists x = \sum a_i x_i \notin d\mathbb{Z}$,i.e. $d \nmid x$.Write $x = dm + r$,where $m, n \in \mathbb{N}, 0 < r < d$.$r = x - dm = \sum a_i x_i + (-m)d \in A\mathbb{Z}$. But that's impossible.Hence $A\mathbb{Z} \subseteq d\mathbb{Z}, A\mathbb{Z} = d\mathbb{Z}$.

(e) By (d),$A\mathbb{Z} = d\mathbb{Z}$,by (c),$A \subseteq A\mathbb{Z} \Rightarrow A \subseteq d\mathbb{Z}$,i.e. $d|a, \forall a \in A \Rightarrow d$ is a lower bound of A.Take another lower bound d' of A.$d'|a, \forall a \in A \Rightarrow d|y, \forall y \in A\mathbb{Z} = d\mathbb{Z} \Rightarrow d'|d \Rightarrow d$ is the greatest lower bound of A.i.e.$\inf A = d$.

(8) If A is empty, it is easy to check $\gcd(A) = 0, \operatorname{lcm}(A) = 1$.Assume $A =\neq \varnothing$.If $A = \{0\}$, then easy to check $\gcd(A) = \operatorname{lcm}(A) = 0$.Set $A' = \{a \in A | a \neq 0\} \subseteq A, A' \neq \varnothing$.By (7)-(e),$A'$ has infimum d. d is also the infimum of A.By (5),(6)-(c),A' has a supremum D.d is also the supremum of A.

(9) $A = \{a, b\}$,by (7)-(d)(e),$A\mathbb{Z} = d\mathbb{Z} \Rightarrow d \in A\mathbb{Z} \Rightarrow \exists m, n$ such that $d = ma + nb$ (Bézout Lemma)

(10) $\frac{ab}{\gcd(a,b)} = a\frac{b}{\gcd(a,b)} = b\frac{a}{\gcd(a,b)} \Rightarrow \frac{ab}{\gcd(a,b)}$ is an upper bound of $A = \{a, b\}$ under $(\mathbb{N}, |)$.Since $\operatorname{lcm}(a, b)$ is the least upper bound of A , $\gcd(a, b)|\frac{ab}{\gcd(a,b)}$

$$a = \frac{ab}{\operatorname{lcm}(a,b)} \frac{\text{lcm(a, b)}}{b}, b = \dots$$

$\frac{ab}{\text{lcm}(a,b)}$ is a lower bound of $A = \{a, \}$ under $(\mathbb{N}, |)$,gcd is the greatest $\ldots$
$\frac{ab}{\text{lcm}(a,b)} | \gcd(a, b), ab = \gcd(a, b)\text{lcm}(a, b)$.

23. (1) Obvious.

(2) $\forall x \in \varnothing, P(x)$ is true.There is no non-empty set can be the subset of $\varnothing$,$(\varnothing, \underline{\in})$ is true.

(3) $(\alpha, \underline{\in})$ is a well-ordered set since it is a subset of $(\alpha \cup \{\alpha\}, \underline{\in})$. $\forall x \in \alpha \cup \{\alpha\}$,if $x = \alpha, x \subseteq (\alpha \cup \{\alpha\})$;if $x \in \alpha, x \subseteq \alpha \subseteq (\alpha \cup \{\alpha\})$.So α is ordinal.

(4) $\forall x \in \alpha, x\underline{\in}\alpha, \forall A \subseteq \alpha, \min(A) \in \alpha \subseteq (\alpha \cup \{\alpha\})$,so $(\alpha \cup \{\alpha\}, \underline{\in})$ is well ordered.$\forall x \in \alpha \cup \{\alpha\}$,if $x = \alpha$,$\alpha \subseteq \alpha \cup \{\alpha\}$;If $x \in \alpha$,since α is ordinal, $x \subseteq \alpha \subseteq \alpha \cup \{\alpha\}$.Thus $\alpha \cup \{\alpha\}$ is an ordinal.
Obviously,

$$\alpha \subseteq \bigcup_{x \in \alpha \cup \{\alpha\}} x$$

Conversely,$\forall y \in x, x \in \alpha \cup \{\alpha\}$,if $x = \alpha$,then $y \in \alpha$.If $x \in \alpha$,since α is ordinal,$y \in x \subseteq \alpha, y \in \alpha$.Hence,

$$\alpha \supseteq \bigcup_{x \in \alpha \cup \{\alpha\}} x$$

Therefore,

$$\alpha = \bigcup_{x \in \alpha \cup \{\alpha\}} x$$

(5)

$$\alpha = \bigcup_{x \in \alpha \cup \{\alpha\}} x = \bigcup_{x \in \beta \cup \{\beta\}} x = \beta$$

(6) If $x = \alpha \vee y = \alpha$,easy.If $x, y \in \alpha$,since $(\alpha, \underline{\in})$ is well ordered, consider $\{x, y\} \subseteq \alpha, x\underline{\in}y \vee y\underline{\in}x$.

(7) $\forall x \in \alpha, x \subseteq \alpha$, since $(\alpha, \underline{\in})$ is well ordered, $(x, \underline{\in})$ is well ordered.$\forall y \in x, z \in x$,by transitive $z \in x, y \subseteq x$.Therefore,all elements of α are ordinals.

(8) Take $x \in \beta$,denote $X := \{\, y \in \alpha | y\underline{\in}x \,\}$.Take $y \in X$,since $y\underline{\in}x\underline{\in}\beta$,by transitivity,$y\underline{\in}\beta$.If $y = \beta, \beta \in x \wedge x \in \beta$,contradicts to axiom of foundation.So $y \in \beta, X \subseteq \beta$.

(9) If $\beta \in \alpha \cup \{\alpha\}$ and $\beta \neq \alpha, \beta \subseteq \alpha$.By (8),$\beta$ is an initial segment of α. If β is an initial segment of α

24. (1) $\Rightarrow$:Let $\alpha = A \cup \{A\}$ for an ordinal A.By (4) of 23.

$$A = \bigcup_{x \in A \cup \{A\}} x = \bigcup_{x \in \alpha} x \subseteq \alpha$$

$\Leftarrow$: Let $U = \cup_{x \in \alpha} x$,claim that $\alpha = U \cup \{U\}$ (to be continue to check)

(2) -

(3) N.T.S. $\forall x \in \varnothing \cup \{\varnothing\}$,$x$ is not a limit ordinal.$\Rightarrow$ $x = \varnothing$, which is not a limit ordinal by definition.

(4) $\alpha = n$ is a natural number $\Leftrightarrow$ $\forall x \in \alpha \cup \{\alpha\}, x$ is not limit.N.T.S $\alpha + 1$ is not $\mathbb{N}$, i.e. $\forall x \in \alpha \cup \{\alpha\} \cup \{\alpha \cup \{\alpha\}\}, x$ is not limit.Whether $x \in \alpha \cup \{\alpha\}$ or $x = \alpha \cup \{\alpha\}$, it's right.

(5) -

(6) $\alpha = n$ natural number .$\forall x \in \alpha + 1, x$ is not limit. N.T.S $\forall y \in \alpha, \forall z \in y + 1, z$ is not limit.$z \in y + 1 \nsubseteq \alpha + 1 \Rightarrow z \in \alpha + 1 \Rightarrow z$ is not a limit ordinal.

(7) -

(8) -

(9) f increasing $\Leftrightarrow$ $\forall x_1, x_2 \in \mathbb{N}, f(x_1) \le f(x_2)$.Prove by induction.Claim $f(0) = 0$.Pf.:If not ,then $f(0) \ne 0 \Rightarrow f(0) \ge 1$.By increasing,$\forall n > 0, f(n) \ge f(0) \ge 1$.$\forall n \in \mathbb{N}, f(n) \ne 0, f$ is not surjective.Claim:If $f(n) = n, \forall n \ge m$, then $f(m+1) = m+1$.Pf. $f(m+1) \ge f(m) = m$ .If $f(m + a) = m = f(m) \Rightarrow f$ is not injective.If $f(m + 1) > m + 1$,then $\forall i > m + 1, f(i) \ge f(m + 1) > m + 1$.

5 Group

1. It is communicative and associative.

2. It's communicative, but not associative.

3. (1) $1 + 3(x * y) = 1 + 3x + 3y + 9xy = (1 + 3x)(1 + 3y)$

   (2) Easy to prove it's communicative. $(x*y)*z = x+y+z+3xy+3yz+3zx + 9xyz$, x, y, z are in the same position. Then it's associative.

   (3) $\forall x \in \mathbb{R}, (x * 0) = (0 * x) = x$, so $e = 0$ is the neutral element in the semigroup.

   (4) $\forall x \ne -\frac{1}{3}, y = -\frac{x}{1+3x}$ satisfies $(x * y) = 0 = e$.

4. (1) Easy. $e = 0$.

(2) $\forall (x,y) \in \mathbb{R}^2_{>0}, \sqrt{x^2+y^2} > 0 = e$. So none of the non-zero element is invertible.

5. (1) Easy to check it is close.
   (2) Composition of mapping is associative, so it's a semigroup.
   (3) $\forall i \in \{1,2,3,4\}, f_1 \circ f_i = f_i = f_i \circ f_1$. So it is a monoid.
   (4) $\forall i \in \{1,2,3,4\}, f_i \circ f_i = f_1$. So it is a group.

6. (1) $e = (1,0), (\frac{1}{a}, -\frac{x}{a})$ is the inverse of (a,x).
   (2) Not communicative.
   (3) Easy.

7. (1) Not close.
   (2) Not close.
   (3) $e = 1$ is the neutral element. $\forall (x,y) \in H^2$, let $x = \frac{q}{p}, y = \frac{t}{s}, \iota(y) = \frac{s}{t}$, then $x \cdot \iota(y) = \frac{qs}{pt} \in H$. So $(H, \cdot)$ is a group.
   (4) $\forall \sigma \in H, \sigma(x) = x \Rightarrow x = \sigma^{-1}(\sigma(x)) = \sigma^{-1}(x)$, so $\sigma^{-1} \in H$. Since we've known H is monoid, H is a group.

8. We denote $G := \{a + b\sqrt{2} \mid (a,b) \in \mathbb{Z}^2\}$. Take two elements $x = a+b\sqrt{2}, y = c+d\sqrt{2}$ from G, $x \cdot y = (ac+2bd)+(ad+bc)\sqrt{2} \in G$. The neutral element $e = 1$ also in G, so it is a submonoid of $(\mathbb{R}, \cdot)$.

9. $\forall z \in \mu_n(\mathbb{C}), \iota(z) = z^{-1}$. $\forall (z_1, z_2) \in \mu_n(\mathbb{C})^2, (z_1 z_2^{-1})^n = z_1^n (z_2^n)^{-1} = 1$, thus $z_1 \iota(z_2) \in \mu_n(\mathbb{C})$. Therefore $\mu_n(\mathbb{C})$ is a subgroup of $(\mathbb{C}^\times, \cdot)$.

10. (1) Neutral element $e = 1$ is in $G := \{x + y\sqrt{3} \mid x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1\}$. If $x + y\sqrt{3}$ is an element of G, then $(x+y\sqrt{3})(x-y\sqrt{3}) = 1$, since $x \geq 0, x+y\sqrt{3}$ and $x - y\sqrt{3}$ can not both be negative. Then they are both positive, so they are both in $\mathbb{R}_{>0}$. Moreover, They are inverse of each other. $(x+y\sqrt{3})(z-w\sqrt{3}) = xz - 3yw + (zy - xw)\sqrt{3}, x > \sqrt{3}y, z > \sqrt{3}w \Rightarrow xz - 3yw > 0$. So $xz - 3yw \in \mathbb{N}$. $(x+y\sqrt{3})(z-w\sqrt{3}) \in G$. Therefore, it is a subgroup of $(\mathbb{R}_{>0}, \times)$.
    (2) Easy.
    (3) $\frac{97}{56} - \sqrt{3} = \frac{1}{(97+56\sqrt{3})56}$.

11. (1) $\forall (n,m) \in \mathbb{Z}^2, (-1)^n(-1)^m = (-1)^{n+m}$.
    (2) Easy.
    (3) Easy.

12. (1) Easy to check $e \in \mathrm{Stab}(x)$. $\forall g \in \mathrm{Stab}(x), x = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$. So $g^{-1} \in \mathrm{Stab}(x)$. Moreover, $\forall (g_1, g_2) \in \mathrm{Stab}(x)^2, g_1 g_2^{-1} x = g_1 x = x$, so $g_1 g_2^{-1} \in \mathrm{Stab}(x)$. Therefore, $\mathrm{Stab}(x)$ is a subgroup of G.

    (2) Claim that: if $\exists g \in G$, $g \in g_1\mathrm{Stab}(x) \wedge g \in g_2\mathrm{Stab}(x)$, then $g_1\mathrm{Stab}(x) = g_2\mathrm{Stab}(x)$. Let $g = g_1 s_1 = g_2 s_2$, then $g_2 = g_1 s_1 \iota(s_2)$. Thus, for any $s \in \mathrm{Stab}(x), g_2 s = g_1 s_1 \iota(s_2) s \in g_1\mathrm{Stab}(x)$.
    So $g_2\mathrm{Stab}(x) \subseteq g_1\mathrm{Stab}(x)$. resp. we have $g_2\mathrm{Stab}(x) \supseteq g_1\mathrm{Stab}(x)$. Hence $g_2\mathrm{Stab}(x) = g_1\mathrm{Stab}(x)$. If $g_1 s_1 = g_2 s_2, g_1 x = g_1 s_1 x = g_2 s_2 x = g_2 x$. Therefore, they map at the same gx.

    (3) By definition, $\forall g \in G, |\mathrm{Stab}(x)| = |g\mathrm{Stab}(x)|$.(Lagrange Theorem)

13. (1) 1.

    (2) By definition, $n \in N(a)$. Hence, $\min(N(a)) \leq n$.

    (3) Let $p, q \leq \mathrm{ord}(a), 0 \leq p < q$. Suppose that $a^p = a^q$, then $e = a^{q-p}, (q-p) \in N(a), q - p < \mathrm{ord}(N(a))$, contradiction. Thus they are distinct.

    (4) Let $f : (\mathbb{Z}, +) \to (G, *)$ be the homomorphism, $f(1) = a$, then $\forall n \in \mathbb{Z}, a * f(n) = f(n+1)$.

        (a) Suppose $\langle a \rangle$ is finite. If $\forall n, m \in \mathbb{Z}, f(n) \neq f(m)$, then the image is not finite, contradiction. Take $f(n) = f(m), n < m$, then $a^{m-n} = 1$. Thus $\mathrm{ord}(a) \leq m - n$ is finite.

        (b) Suppose $\mathrm{ord}(a)$ is finite. Then $\forall n \in \mathbb{Z}, f(n + \mathrm{ord}(a)) = f(n) \in \{f(i) \mid i \in \mathbb{N}, 1 \leq i \leq \mathrm{ord}(a)\}$

    (5) By (4)(b), $|\langle a \rangle| \leq \mathrm{ord}(a)$. By (4)(a),$|\langle a \rangle| \geq \mathrm{ord}(a)$.

14. (1) By comm. law $(ab)^N = a^N b^N = e, \mathrm{ab} \leq N$ is finite.

    (2) -

    (3) -

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.

17. Let $E = \{1, 2, \dots, n\}$, $\forall \sigma \in \mathfrak{S}_E$,

$$\prod_{i \neq j \in E} [\sigma(i) - \sigma(j)] = \prod_{i \neq j \in E} (i - j)$$

$$\prod_{i \neq j \in E} (i-j)[(\sigma \circ \pi)(i) - (\sigma \circ \pi)(j)] = \prod_{i \neq j \in E} [\sigma(i) - \sigma(j)][\pi(i) - \pi(j)]$$

$$\prod_{i < j \in E} (i-j)[(\sigma \circ \pi)(i) - (\sigma \circ \pi)(j)] = \prod_{i < j \in E} [\sigma(i) - \sigma(j)][\pi(i) - \pi(j)]$$

$$\prod_{i < j \in E} \frac{[(\sigma \circ \pi)(i) - (\sigma \circ \pi)(j)]}{i-j} = \prod_{i < j \in E} \frac{\sigma(i) - \sigma(j)}{i-j} \prod_{i < j \in E} \frac{\pi(i) - \pi(j)}{i-j}$$

Hence, sgn is a homomorphism.

18. By 16. $\forall \sigma \in \mathfrak{S}_E$, it can be represented by the composition of transpositions τ_i, where,

$$\tau_i : E \longrightarrow E,$$

$$\tau_i(x) = \begin{cases} x & , \quad x \in E \setminus \{i, \mathrm{mod}(i,n)+1\} \\ \mathrm{mod}(x,n)+1 & , \quad x = i \\ \mathrm{mod}(x-2,n)+1 & , \quad x = \mathrm{mod}(i,n)+1 \end{cases}$$

Easy to check that $\tau_i \circ \tau_i = \mathrm{Id}_E$. So $\forall f$ be a homomorphism, , $f(\tau_i)f(\tau_i) = 1, f(\tau_i) = \pm 1$. Then $\forall \sigma \in \mathfrak{S}_E, f(\sigma) = \pm 1$.

Remark. $f = -1$ corresponds to the sgn in 17.

6 Rings and Modules

1. (1) First, we check that it is a monoid.
   One has it is closed. For any $(x_1, x_2) \in \mathbb{Z}^2, (x_1, x_2) * (1, 0) = (x_1, x_2)$. So $(1, 0)$ is the neutral element.

   (2) Second, check that it is commutative.
   For any $(x_1, x_2), (y_1, y_2) \in \mathbb{Z}^2, (x_1, x_2) * (y_1, y_2) = (x_1 y_1 + r x_2 y_2, x_1 y_2 + x_2 y_1) = (y_1 x_1 + r y_2 x_2, y_1 x_2 + y_2 x_1) = (y_1, y_2) * (x_1, x_2)$.

   (3) Third, check that it is distributive.
   For any $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in \mathbb{Z}^3, (x_1, x_2) * ((y_1, y_2) + (z_1, z_2)) = (x_1(y_1 + z_1) + r x_2(y_2 + z_2), x_1(y_2 + z_2) + x_2(y_1 + z_1)) = (x_1, x_2) * (y_1, y_2) + (x_1, x_2) * (z_1, z_2)$.

2. (1) Associativity is NOT valid in general.

   (2) Just verify.

3. Let $e_i = (0, \ldots, 1, \ldots, 0)$

4. 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

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

5. 10.

(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 $\sum_{n\in\mathbb{N}} a_n T^n \in k[[T]]$,

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

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

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

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

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

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

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

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

$$\sum_{i=0}^{n} a_i b_{n-i} = \sum_{t=n}^{0} a_{n-t} b_t = \sum_{t=0}^{n} b_t a_{n-t}.$$

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 $g = \sum_{n\in\mathbb{N}} b_nT^n$ 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
$$b_{n+1} = \left(\mathbb{1} - \sum_{i=1}^{n+1}(a_ib_{n+1-i})\right)a_0^{-1},$$
then,
$$\sum_{i=0}^{n+1}(a_ib_{n+1-i}) = \mathbb{1}.$$
Hence $g = \sum_{n\in\mathbb{N}} b_nT^n$ is the inverse of f.

(6) Follow the algorithm in (5), we can easily get the result.
$$(1 - aT)^{-1} = \sum_{n\in\mathbb{N}} a^nT^n.$$

(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 $f' = \sum_{n\in\mathbb{N}} b_nT^n$, let $a_n = b_{n-1}(n-1)^{-1},\ n \neq 0,\ D[\sum_{n\in\mathbb{N}} a_nT^n] = f'$. Therefore D is a surjective k-linear mapping.

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

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

(10)

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

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

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

6. 15.

(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 $\{k \in \mathbb{N}^* \mid k \leq n\}$ satisfies $\gcd(k, p_i) = p_i \neq 1$. So, there are $n(1 - \frac{1}{p_i})$ elements in $\{k \in \mathbb{N}^* \mid k \leq n\}$ 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.