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

(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 , $\gcd(a, b) | \frac{ab}{\gcd(a,b)}$

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

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

23. (1) Obvious.

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

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

(4) $\forall x \in \alpha, x \subseteq \alpha, \forall A \subseteq \alpha, \min(A) \in \alpha \subseteq (\alpha \cup \{\alpha\})$,so $(\alpha \cup \{\alpha\}, \subseteq)$ 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 $(\alpha, \subseteq)$ is well ordered, consider $\{x, y\} \subseteq \alpha, x \subseteq y \vee y \subseteq x$.

(7) $\forall x \in \alpha, x \subseteq \alpha$, since $(\alpha, \subseteq)$ is well ordered, $(x, \subseteq)$ 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 $X := \{\, y \in \alpha | y \subseteq x \,\}$.Take $y \in X$,since $y \subseteq x \subseteq \beta$,by transitivity,$y \subseteq \beta$.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 $\Leftrightarrow \forall x_1, x_2 \in \mathbb{N}, f(x_1) \leq f(x_2)$.Prove by induction.Claim $f(0) = 0$.Pf.:If not ,then $f(0) \neq 0 \Rightarrow f(0) \geq 1$.By increasing,$\forall n > 0, f(n) \geq f(0) \geq 1$.$\forall n \in \mathbb{N}, f(n) \neq 0, f$ is not surjective.Claim:If $f(n) = n, \forall n \geq m$, then $f(m+1) = m+1$.Pf. $f(m+1) \geq f(m) = m$ .If $f(m + a) = m = f(m) \Rightarrow f$ is not injective.If $f(m + 1) > m + 1$,then $\forall i > m + 1, f(i) \geq f(m + 1) > m + 1$.

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) $\forall x \neq -\frac{1}{3}, y = -\frac{x}{1+3x}$ 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 $\langle \sigma \rangle \setminus E$, 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 $n = \mathrm{Card}[\langle \sigma \rangle \setminus E]$. 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,

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

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

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

6.1 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 $(x_1, x_2), (y_1, y_2) \in \mathbb{Z}^2, (x_1, x_2) * (y_1, y_2) = (x_1y_1 + rx_2y_2, x_1y_2 + x_2y_1) = (y_1x_1 + ry_2x_2, y_1x_2 + y_2x_1) = (y_1, y_2) * (x_1, x_2)$.

   (3) Third, check that it is distributive.
   For any $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in \mathbb{Z}^3, (x_1, x_2) * ((y_1, y_2) + (z_1, z_2)) = (x_1(y_1 + z_1) + rx_2(y_2 + z_2), x_1(y_2 + z_2) + x_2(y_1 + z_1)) = (x_1, x_2) * (y_1, y_2) + (x_1, x_2) * (z_1, z_2)$.

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

   (2) Just verify.

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

4. (1) $2x = (2x)^2 = 2x^2 + 2x = 2x + 2x \Rightarrow x = -x$. $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + b + ab + ba$. $\Rightarrow 0 = ab + ba = ab - ba \Rightarrow ab = ba$.

   (2) $x(x - 1) = 0$. If $x \neq 0$ and $x \neq 1$, then x is a zero divisor.

   (3) Assume there is a boolean ring that has three elements $0, 1, x$. If $x - 1 \neq 1$, then $x - 1 = x$, contradicts to $2x = 0$. Hence, $x - 1 = 1$, this contradicts to $1 + 1 = 0$. Therefore, A cannot have exactly 3 elements.

   (4) $1 + x = y, 1 + y = x, x + y = 1, xy = 0$.

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

6. 0 is the zero element and 1 is the unit element. Then all the natural number are in the subfield. It is a group with the composition law $+$, by inverse law $-$, and the identity element 0, all the integers are in the subfield. Similarly, all the rational numbers are in the subfield. So the only subfield of $\mathbb{Q}$ is $\mathbb{Q}$.

7. (1) $0 \in M$. Assume $M \cap \mathbb{N}_{>0} = \varnothing$, then for any non-zero elements $x, y \in M$, $x + y < 0$, that contradicts to x is invertible.
   (2) If there exists a element equals $kd + m, k \in \mathbb{Z}, m \in [1, d-1]$, then $kd + m + k(-d) = m < d \in M$. Contradiction!
   (3) By (2), $M \subseteq d\mathbb{Z}$. For any $nd \in d\mathbb{Z}, nd = \underbrace{d + d + \cdots + d}_{n \text{ copies}} \in d\mathbb{Z}$. So $d\mathbb{Z} \subseteq M$. Therefore, $M = d\mathbb{Z}$.

9. (1) We claim it is a left-A-module, then right-A-module follow the similar proof.First, it is a left action. For any $a \in A$, $ea = a$, where e is neutral element. By definition, $a(bc) = (ab)c$. Second, check it is a left A-module. For any $(a, b) \in A^2, (c, d) \in A^2, ac + bc = (a + b)c, ac + ad = a(c + d)$.

(2) If $[a_1]=[a_2],[b_1]=[b_2]$, then $a_1a_2^{-1}\in I,\ b_1b_2^{-1}\in I$. Hence $(a_1b_1)(a_2b_2)^{-1}=a_1(b_1b_2^{-1})a_2^{-1}\in I$. So it is well defined.
By definition it is closed. For any $a,b,c\in A$, $[a]([b][c])=[a][bc]=[a(bc)]=[(ab)c]=([a][b])[c]$. So it is associative. For any $a\in A,[a][1]=[a]=[1][a]$. So it determines a structure of monoid on A/I.

(3) Similarly, we can prove A/I equipped with additive law is well defined and forms a monoid. Then we only need to check that A/I is a group under induced $+$. For any $a\in A,[a]+[-a]=[a+(-a)]=[0]$, where 0 is the neutral element of $(A,+)$. Therefore, A/I becomes a unitary ring. For ant $(a,b)\in A,\pi(a)\pi(b)=[a][b]=[ab]=\pi(ab),\pi(1)=[1]$. So $\pi:A\to A/I$ is a homomorphism of monoids. $\pi(a)+\pi(b)=[a]+[b]=[a+b]\pi(a+b)$. So it is also a homomorphism of groups. Therefore, π is a homomorphism of rings.

(4) (a) For any $a\in A,x\in I,\ f(ax)=f(a)f(x)=f(a)0=0$. So $ax\in I$. Similarly, $xa\in I$. So I is an ideal of A.

(b) $\forall(x,y,z)\in A^3,f(x)\left(f(y)f(z)\right)=f(x)f(yz)=f(x(yz))=f((xy)z)=f(xy)f(z)=\left(f(x)f(y)\right)f(z)$. $f(x)f(1)=f(x\cdot1)=f(x)$. So $(\mathrm{Im}f,\cdot)$ is a monoid. Similarly, we can deduce that $(\mathrm{Im}(f),+)$ is a monoid, in addition, $f(x)+f(-x)=f(x-x)=f(0)=0$. So $f(-x)$ is the inverse of $f(x)$. So $\mathrm{Im}(f)$ is the subring of B.

(c) $\tilde{f}\left([x][y]\right)=f(xy)=f(x)f(y)=\tilde{f}\left([x]\right)\tilde{f}\left([y]\right)$. So it is a homomorphism. If $x,y\in A$ satisfy $x-y\in\ker f$, then $f(x)+f(-y)=f(x-y)=0$. Thus $f(x)=f(y)$. So $\tilde{f}$ is a injective homomorphism of unitary rings. Therefore, it forms a isomorphism.

(5) Let $f:\mathbb{Z}\to A$ be a mapping. $f(n)=n1_A$ is a homomorphism. If g is a homomorphism, then $f(1)=1_A,\ f(0)=0_A$. For any $n\in\mathbb{N},f(n)=f\left(\sum_{i=1}^n1\right)=\sum_{i=1}^nf(1)=\sum_{i=1}^n1_A$. For any ...

10. (1)

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

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

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

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

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

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

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

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

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

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

Hence $\mathbb{1}$ 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 $g = \sum_{n\in\mathbb{N}} b_n T^n$ be its inverse, then by (2), $(b_i)_{i\in\mathbb{N}}$ satisfies:

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

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 $g = \sum_{n\in\mathbb{N}} b_n T^n$ 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 $f = \sum_{n\in\mathbb{N}} a_n T^n \in \ker(D)$, then for any $n \in \mathbb{N}, a_{n+1} = 0$. Thus,

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

(10)

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

11. (1)

$$(a_n, b_n) \longmapsto \sum_{i=1}^{n} a_i b_{n-i}.$$

If $n > \deg(F)$, then

$$\sum_{i=1}^{n} a_i b_{n-i} = \sum_{i=\deg(F)}^{n} a_i b_{n-i}.$$

If $n < \deg(F) + \deg(G)$, then it will be 0. If $n = \deg(F) + \deg(G)$, then

$$\sum_{i=1}^{n} a_i b_{n-i} = a_{\deg(F)} b_{\deg(G)} \neq 0.$$

So $\deg(FG) = \deg(F) + \deg(G)$.

(2) Existence: If $\deg(F) < \deg(P)$ let $Q = 0, R = F$. If $\deg(F) > \deg(P)$, let $F_{i+1} = F_i - a_{\deg(F)} T^{\deg(F)-\deg(P)} P$, $(F_0 = F)$, then $\deg(F_{i+1}) < \deg(F_i)$. Then come to the first case.
Uniqueness: If $F = Q_1 P + R_1 = Q_2 P + R_2$. Then $(Q_1 - Q_2)P = R_2 - R_1$. If $Q_1 \neq Q_2$, then $\deg(Q_1 - Q_2) > 0, \deg((Q_1 - Q_2)P) > \deg(P) > \deg(R_1 - R_2)$. This contradicts to $\deg((Q_1 - Q_2)P) = \deg(R_2 - R_1)$. Thus $Q_1 = Q_2, \ R_1 = R_2$.

(3) By (2) $F = PQ + R$. R must be 0, or it will contradicts to $\deg(P)$ is the least. Let $\deg(P_1) = \deg(P_2)$ be the least. Then there exists $Q \in I \backslash \{0\}, \ P_1 Q = P_2$. Then $\deg(P_2) = \deg(P_1) + \deg(Q)$. So $\deg(Q)$ must be zero. Hence $Q = 1.$, we proved the uniqueness.

(4) Let P' be the minimal polynomial, since I is an ideal, $P = a^{-1}_{\deg(P')} P' \in I$. It is a monic polynomial.

(5) Easy.

12. (1) Let $Q = \sum_{n\in\mathbb{N}} b_n T^n$, then $(T-x)Q = -b_0 x + \sum_{n\in\mathbb{N}^*} (-x b_n + b_{n-1}) T^n$.

$$a_0 = -b_0 x, \ a_n = -x b_n + b_{n-1}.$$

It satisfies $P(0) = 0$ automatically.

(2) By (1), then can write in the form. $\deg(T - x_i) = 1$. By 11.(1),

$$d = \deg(P) = d_1 + d_2 + \cdots + d_n + \deg(P) \geq d_1 + \cdots + d_n.$$

(3) Suppose it has more the d root. Write it into (2) form. Then leads to a contradiction.

13. (1) $[T][T] = [P - 1] = [P] - I = I - I = 0$.

(2) Let $F = P_0Q_0 + R_0, Q_i = PQ_{i+1} + R_{i+1}$, $[F] = [PQ_0] + [R_0] = [P][Q_0] + [c_0 + b_0T] = [PQ_1] + [R_1] + b_0 i = \left([Q_n] + \sum_{i\in\mathbb{N}}^{n} b_i i\right)$ (Since $k[T]$ is formal, n is finite.)

(3) Let f be the mapping, f is injective. By (2), f is surjective. So it is a bijection. $[Q][R] = [QR] = [RQ] = [R][Q]$, hence it's communicative. $f(a, b) + f(c, d) = f(a + c, b + d)$, thus it is a homomorphism of group. $cf(a, b) = f(ca, cb)$. Therefore, f is a $\mathbb{R}$-linear bijection.

(4) -

(5) Easy. $\iota \circ \iota = \mathrm{Id} \Rightarrow$ bijection $\Rightarrow$ isomorphism.

(6) Easy

(7) $i = [T] = [-\iota(T)] = -i$.

(8) A bit confused.

(9) By communicative law.

(10) Find the inverse, and it is communicative.

(11) Easy.

(12) Emm.

(13) $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

14. (1) Addition: group, 0, Multiplication: monoid, 1.

(2) Let $P = T^2 - 2$, I be the ideal defined as

$$I := P\mathbb{R}[T].$$

Then we can prove: If we denote $[T]$ as $\sqrt{2}$, then $\left(\sqrt{2}\right)^2 = 2$. Then similar to 13.

(3) If $a^2-2b^2 = \pm 1$, then $\pm(a-b\sqrt{2})$ is the inverse of $a+b\sqrt{2}$. If $a+b\sqrt{2}$ is invertible, let $c+d\sqrt{2}$ be its inverse. Then $\left(ac + 2bd + (ad + bc)\sqrt{2}\right) = \pm 1$. Hence $ad + bc = 0$ **TO BE CONTINUE.**

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)⇒ (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)⇒ (i):

(2) By (1) (i)⇒ (iii), $(\mathbb{Z}/n\mathbb{Z})^\times \subseteq \{k \mid k \in [0, n-1], \gcd(k,n) = 1\}$. By (1) (iii)⇒ (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 $\gcd(k, p_i) = p_i \neq 1$. 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 $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}, \bar{a}\bar{b} = \bar{ab} = \bar{ba} = \bar{b}\bar{a}$. So $\mathbb{Z}/p\mathbb{Z}$ is commutative. Therefore $\mathbb{Z}/p\mathbb{Z}$ is a field.

7 Linear Algebra: Vectors and Matrices

6. (1) $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

(2) $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

(3) $A = \begin{pmatrix} \cos\left(\frac{2\pi}{3}\right) & \sin\left(\frac{2\pi}{3}\right) \\ -\sin\left(\frac{2\pi}{3}\right) & \cos\left(\frac{2\pi}{3}\right) \end{pmatrix}$.

8. (1) Easy

   (2) Easy

   (3) B is a non-zero solution. If X is the inverse of A, then $AX = I$. But $B(AX) = (BA)X = 0$. that contradicts to $BI = B$, for any non-zero matrix.

9. (1) $J^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Easy

   (2) Easy.

   (3) If $(a, b) = 0$, it is not invertible. If $(a, b) \neq 0$, easy to check $M\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ is its inverse.

11. (1) Easy.

    (2) Let x be 1 and 2, then we obtain $1 = a_n + b_n,\ 2^n = 2a_n + b_n$.. Hence $a_n = 2^n - 1,\ b_n = 2 - 2^n$.

    (3) $A^n = (A^2 - 3A + 2)\, Q(A) + (a_n A + b_n) = \ldots$.

12. For any $i, k, [b_i j], \sum_j a_{ij} b_{jk} = \sum_j b_{ij} a_{jk}$. Let $b_{ij} = \delta_{i,m}\delta_{j,n}$, then $a_{im}\delta_{k,n} = \delta_{i,m} a_{nk}$. So $a_{mn} = 0$, if $n \neq m$. $a_{mm} = a_{nn}$, for any m, n. So $a_{ij} = \lambda\delta_{i,j}$.

13. (2) Easy.

    (3) Easy.

14. Easy.

17. Easy.

18. (1) $a^{-1} = A$.

    (2) $A_\lambda\left(A + \lambda I_n\right) / \left(1 - \lambda^2\right) = I_n$

19. (1) Easy. $(I + A)(I - \frac{1}{2}A) = I + \frac{1}{2}A - \frac{1}{2}A^2 = I$.

    (2) $A(A - I) = 0$. If C is the inverse of A, then $0 = BA(A - I) = A - I$. So $A = I$. If $A = I$, then I is its inverse.