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 $A \subseteq B \land B \subseteq C \Rightarrow A \subseteq C$
       (c) antisymmetric $A \subseteq B \land B \subseteq A \Rightarrow A = B$
    (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 , $\gcd(a, b)|\frac{ab}{\gcd(a,b)}$

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

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

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 $\Leftrightarrow \forall x_1, x_2 \in \mathbb{N}, f(x_1) \leq f(x_2)$.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, $\forall (g_1, g_2) \in \mathrm{Stab}(x)^2, g_1g_2^{-1}x = g_1x = x$, so $g_1g_2^{-1} \in \mathrm{Stab}(x)$. 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 $g = g_1s_1 = g_2s_2$, then $g_2 = g_1s_1\iota(s_2)$. Thus, for any $s \in \mathrm{Stab}(x), g_2s = g_1s_1\iota(s_2)s \in g_1\mathrm{Stab}(x)$.
    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 $g_1s_1 = g_2s_2, g_1x = g_1s_1x = g_2s_2x = g_2x$. 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) $e = \mathrm{Id}_E, f \circ f^{-1} = \mathrm{Id}_E$
    (2) $\sigma^0(x) = x$ and composition of mapping is associative.
    (3) Easy.
    (4) -

16. (1)