VE203 Assigment 3

Liu Yihao 515370910207

Exercise 3.1

i) (i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in S$

(ii) $1 \in S$ satisfies $a \cdot 1 = 1 \cdot a = a$ for all $a \in S$

(iii) $|z| = 1 \Rightarrow z = x + yi(x^2 + y^2 = 1)$ for every $a = x + yi \in S$ there exists an element $a^{-1} = x - yi \in S$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$

So it is proved.

ii) (i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in S$

(ii) $1 \in S$ satisfies $a \cdot 1 = 1 \cdot a = a$ for all $a \in S$

(iii) $z^n = 1 \Rightarrow |z|^n = 1 \Rightarrow |z| = 1 \Rightarrow z = x + yi(x^2 + y^2 = 1)$
for every $a = x + yi \in S$ $(x^2 + y^2 = 1)$ there exists an element $a^{-1} = x - yi \in S$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$

So it is proved.

Exercise 3.2

i) (i) $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ for all $A, B, C \in S$

(ii)

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$E \in S$ satisfies $A \cdot E = E \cdot A = A$ for all $A \in S$

(iii)

$$A^T = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \text{ When } \varphi = -\varphi_0$$

$$A \cdot A^T = \begin{pmatrix} \cos^2\varphi + \sin^2\varphi & 0 \\ 0 & \cos^2\varphi + \sin^2\varphi \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

for every $A \in S$ there exists an element $A^{-1} = A^T \in S$ such that $A \cdot A^{-1} = A^{-1} \cdot A = E$

So it is proved.

ii) (a) (i) $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ for all $A, B, C \in SL$

(ii)

$$E = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

$E \in SL$ satisfies $A \cdot E = E \cdot A = A$ for all $A \in SL$

(iii)

$$det(A) = det(A^T) = 1$$

$$A \cdot A^T = E$$

for every $A \in SL$ there exists an element $A^{-1} = A^T \in SL$ such that $A \cdot A^{-1} = A^{-1} \cdot A = E$

So it is proved.

(b) (i) $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ for all $A, B, C \in O$

(ii)

$$E = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

$E \in O$ satisfies $A \cdot E = E \cdot A = A$ for all $A \in O$

(iii)

$$A \cdot A^T = E$$

for every $A \in O$ there exists an element $A^{-1} = A^T \in O$ such that $A \cdot A^{-1} = A^{-1} \cdot A = E$

So it is proved.

(c) (i) $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ for all $A, B, C \in SO$

(ii)

$$E = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

$E \in SO$ satisfies $A \cdot E = E \cdot A = A$ for all $A \in SO$

(iii)

$$det(A) = det(A^T) = 1$$

$$A \cdot A^T = E$$

for every $A \in O$ there exists an element $A^{-1} = A^T \in SO$ such that $A \cdot A^{-1} = A^{-1} \cdot A = E$

So it is proved.

Exercise 3.3

i) reflexive: $2|a - a$ is true for all $a \in Z$
symmetric: if $2|a - b$ is true, then $2|b - a$ is true for all $a, b \in Z$
transitive: if $2|a - b$ and $2|b - c$ is true, then $2|a - b + b - c$ is true, so $2|a - c$ is true for all $a, b, c \in Z$

ii) $\{2Z, 2Z + 1\}$

iii) Let $m_1, m_2 = m_1 + 2a \in m$, $n_1, n_2 = n_1 + 2b \in n$, $2|n_1 - n_2$, $2|m_1 - m_2$

$$2|n_1 - n_2 + m_1 - m_2 \Longleftrightarrow 2|(m_1 + n_1) - (m_2 + n_2)$$

$$[m] + [n] := [m + n]$$

$$m_1n_1 - m_2n_2 = -4ab - 2m_1b - 2n_1a$$
$$2| -4ab - 2m_1b - 2n_1a$$
$$[m] \cdot [n] := [m \cdot n]$$

Exercise 3.4

Suppose $c = gcd(a, b)$, then $a = cm$, $b = cn$ where $m, n \in N^*$ and $gcd(m, n) = 0$
$n = ax + by = (mx + ny)c$ where $mx + ny \in Z$
So all elements in T is integer multiples of $gcd(a, b)$
According to Theorem 1.6.7, $c|a$ and $c|b$ implies $c|(ax + by)$ for any $x, y \in Z$ So it is proved.

Exercise 3.5

When $n = 3k$, $n^2 = 3(3k^2)$, which is divided
When $n = 3k + 1$, $n^2 = 3(3k^2 + 2k) + 1$
When $n = 3k + 2$, $n^2 = 3(3k^2 + 4k + 1) + 1$
So it is proved.

Exercise 3.6

Suppose $c = gcd(a, a + n)$, then $a = qb$, $a + n = qc$
$n = q(c - b)$, so c divides n
When $n = 1$, $gcd(a, a + 1)$ divides 1, so a and $a + 1$ are always relatively prime.

Exercise 3.7

i)

$$72 = 1 \cdot 56 + 16$$
$$56 = 3 \cdot 16 + 8$$
$$16 = 8 \cdot 2 + 0$$

$$d = gcd(56, 72) = 8$$
$$8 = 56 - 3 \cdot (72 - 56) = 4 \cdot 56 - 3 \cdot 72$$
$$20 \cdot 56 - 15 \cdot 72 = 40$$
$$x = 20 + \frac{72}{8}t = 20 + 9t$$
$$y = 15 - \frac{56}{8}t = 20 - 7t$$

ii)

$$439 = 5 \cdot 84 + 19$$
$$84 = 4 \cdot 19 + 8$$
$$19 = 2 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$

$$d = gcd(84, 439) = 1$$
$$1 = 3-2 = 3-(8-2\cdot3) = -8+3(19-2\cdot8) = 3\cdot19-7(84-4\cdot19) = -7\cdot84+31(439-5\cdot84) = 31\cdot439-162\cdot84$$
$$-25272 \cdot 84 - (-4836) \cdot 439 = 156$$
$$x = -25272 + 439t$$
$$y = -4836 + 84t$$

Exercise 3.8

i) Since $gcd(a, b) = 1|c$, we can apply Theorem 1.6.26
The general solution of $ax + by = c$ is

$$x = x_0 + \frac{b}{d}$$
$$y = y_0 - \frac{a}{d}$$

where x_0, y_0 is a solution to $ax + by = c$
Let $b' = -b$, the general solution of $ax - by = c$ is

$$x = -x_0 - \frac{b}{d}$$
$$y = -y_0 - \frac{a}{d}$$

ii)

$$158 = 2 \cdot 57 + 44$$
$$57 = 1 \cdot 44 + 13$$
$$44 = 3 \cdot 13 + 5$$
$$13 = 2 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$

$$d = gcd(158, 57) = 1$$
$$1 = -5+2(13-2\cdot5) = 2\cdot13-5(44-3\cdot13) = -5\cdot44+17(57-44) = 17\cdot57-22\cdot(158-2\cdot57) = -22\cdot158+61\cdot57$$
$$-154 \cdot 158 - (-427) \cdot 57 = 7$$
$$x = -154 + 57t$$
$$y = -4276 + 158t$$

Exercise 3.9

i) Suppose $a = 3k_1 + 1$, $b = 3k_2 + 1$, then

$$ab = (3k_1 + 1)(3k_2 + 1) = 3(3k_1k_2 + k_1 + k_2) + 1$$

Suppose a member of the set in not a prime, the number can be expressed by two members of the set. If either of the factor numbers isn't a prime, it can be expressed by another two members of the set. This procedure will last until all of the factor numbers are prime, so the number is a product of primes.

ii)

$$100 = 10 \cdot 10 = 4 \cdot 25$$

Exercise 3.10

i) $(4k + 3)|4 \cdot (3 \cdot 7 \cdots p)$, which means $4k + 3|d + 1$
Suppose there exist a prime of form $(4k + 3)|d$, $gcd(d, d + 1) \geqslant 4k + 3$, but according to Exercise 3.6, $gcd(d, d + 1) = 1$, so it is impossible, no prime of this form divides d

ii) $d = 4 \cdot (3 \cdot 7 \cdots (p - 1)) + 3$, which is in the form of $4k + 3$
According to i), no prime of the form $4k+3$ divides d, so if it can be divided, the factors of d can only be $4k+1$ (since it is an odd number). Suppose $a = 4k_1+1, b = 4k_2+1$, $ab = 4(4k_1k_2+k_1+k_2)+1$, which is in the form of $4k + 1$. So the product of numbers in the form of $4k + 1$ will never be in the form of $4k + 3$. It suggests that d, which is in the form of $4k + 3$, can't be divided by $4k + 1$

iii) According to i),ii), d is an odd and no odd prime numbers divides d, which means d is a prime number. Since $d > p$, we can choose d as a prime number to form another $d' = 4 \cdot (3 \cdot 7 \cdots d)$, and d' is also a prime number. Repeat the procedure infinitely and we can get infinite number of primes of the form $4k + 3$