VE 203 HW 3 周浩然 5180219011039

Ex 3.1 i) Let $z = \cos t + i\sin t$

then $a = \cos t_1 + i\sin t_1$

$b = \cos t_2 + i\sin t_2$

$c = \cos t_3 + i\sin t_3$

① associativity: $a\cdot(b\cdot c) = (\cos t_1 + i\sin t_1)(\cos t_2\cos t_3 + i\cos t_2\sin t_3 + i\sin t_2\cos t_3 - \sin t_2\sin t_3)$

$= (\cos t_1 + i\sin t_1)(\cos(t_2+t_3) + i\sin(t_2+t_3))$

$= \cos(t_1+t_2+t_3) + i\sin(t_1+t_2+t_3)$

$(a\cdot b)\cdot c = (\cos t_1\cos t_2 + i\cos t_1\sin t_2 + i\sin t_1\cos t_2 - \sin t_1\sin t_2)\cdot(\cos t_3 + i\sin t_3)$

$= (\cos(t_1+t_2) + i\sin(t_1+t_2))(\cos t_3 + i\sin t_3)$

$= \cos(t_1+t_2+t_3) + i\sin(t_1+t_2+t_3)$

Therefore $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

② unit element: $e = 1$

$a\cdot e = e\cdot a = \cos t_1 + i\sin t_1 = a$

③ inverse: $a^{-1} = \cos(-t_1) + i\sin(-t_1) = \cos(t_1) - i\sin t_1$

$a\cdot a^{-1} = a^{-1}\cdot a = \cos^2(t_1) + \sin^2(t_1) = 1$

Therefore, S is a group.

ii) Let $z = e^{i\frac{2\pi}{n}t}$

Then $a = e^{i\frac{2\pi}{n}t_1}$

$b = e^{i\frac{2\pi}{n}t_2}$

$c = e^{i\frac{2\pi}{n}t_3}$

① associativity: $a\cdot(b\cdot c) = e^{i\frac{2\pi}{n}t_1}\left(e^{i\frac{2\pi}{n}(t_2+t_3)}\right) = e^{i\frac{2\pi}{n}(t_1+t_2+t_3)}$

$(a\cdot b)\cdot c = e^{i\frac{2\pi}{n}(t_1+t_2)}\cdot e^{i\frac{2\pi}{n}t_3} = e^{i\frac{2\pi}{n}(t_1+t_2+t_3)}$

Therefore $a\cdot(b\cdot c) = (a\cdot b)\cdot c$

② unit element. $e = 1$

$a\cdot e = e\cdot a = e^{i\frac{2\pi}{n}t_1} = a$

③ inverse: $a^{-1} = e^{i\frac{2\pi}{n}(-t_1)}$

$a\cdot a^{-1} = a^{-1}\cdot a = e^{i\frac{2\pi}{n}(t_1-t_1)} = e^0 = 1$

Therefore, S(n) is a group.

Ex 3.2 i) ① associativity. $A(a)\times(A(b)\times A(c)) = \begin{pmatrix}\cos a & -\sin a\\ \sin a & \cos a\end{pmatrix}\times\left(\begin{pmatrix}\cos b & -\sin b\\ \sin b & \cos b\end{pmatrix}\times\begin{pmatrix}\cos c & -\sin c\\ \sin c & \cos c\end{pmatrix}\right)$

$= \begin{pmatrix}\cos a & -\sin a\\ \sin a & \cos a\end{pmatrix}\times\begin{pmatrix}\cos b\cos c - \sin b\sin c & -\cos b\sin c - \sin b\cos c\\ \sin b\cos c + \cos b\sin c & -\sin b\sin c + \cos b\cos c\end{pmatrix}$

$= \begin{pmatrix}\cos a & -\sin a\\ \sin a & \cos a\end{pmatrix}\times\begin{pmatrix}\cos(b+c) & -\sin(b+c)\\ \sin(b+c) & \cos(b+c)\end{pmatrix}$

$= \begin{pmatrix}\cos(a+b+c) & -\sin(a+b+c)\\ \sin(a+b+c) & \cos(a+b+c)\end{pmatrix}$

$(A(a)\times A(b))\times A(c) = \left(\begin{pmatrix}\cos a & -\sin a\\ \sin a & \cos a\end{pmatrix}\times\begin{pmatrix}\cos b & -\sin b\\ \sin b & \cos b\end{pmatrix}\right)\times\begin{pmatrix}\cos c & -\sin c\\ \sin c & \cos c\end{pmatrix}$

$= \begin{pmatrix}\cos a\cos b - \sin a\sin b & -\cos a\sin b - \sin a\cos b\\ \sin a\cos b + \cos a\sin b & -\sin a\sin b + \cos a\cos b\end{pmatrix}\times\begin{pmatrix}\cos c & -\sin c\\ \sin c & \cos c\end{pmatrix}$

$$= \begin{pmatrix} \cos(a+b) & -\sin(a+b) \\ \sin(a+b) & \cos(a+b) \end{pmatrix} \times \begin{pmatrix} \cos c & -\sin c \\ \sin c & \cos c \end{pmatrix}$$

$$= \begin{pmatrix} \cos(a+b+c) & -\sin(a+b+c) \\ \sin(a+b+c) & \cos(a+b+c) \end{pmatrix}$$

Therefore $A(a) \times (A(b) \times A(c)) = (A(a) \times A(b)) \times A(c)$

② unit element $e = A(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$A(a) \times A(0) = A(0) \times A(a) = \begin{pmatrix} \cos a & -\sin a \\ \sin a & \cos a \end{pmatrix} = A(a)$$

③ inverse: $a^{-1} = A(-a) = \begin{pmatrix} \cos a & \sin a \\ -\sin a & \cos a \end{pmatrix}$

$$A(a) \times A(-a) = A(-a) \times A(a) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$$

Therefore, S is a group

ii) (a)(b)(c) ① associativity, we will prove the general associativity of matrix multiplication.

A: $m \times n$ matrix, B: $n \times r$ matrix C: $r \times s$ matrix

Let $D = AB$, $E = B \times C$

then $d_{il} = \sum_{k=1}^{n} a_{ik} b_{kl}$ $\quad e_{kj} = \sum_{l=1}^{r} b_{kl} c_{lj}$

The (i,j) entry of DC is $\sum_{l=1}^{r} d_{il} c_{lj} = \sum_{l=1}^{r} \left(\sum_{k=1}^{n} a_{ik} b_{kl} \right) c_{lj}$

The (i,j) entry of AE is $\sum_{k=1}^{n} a_{ik} e_{kj} = \sum_{k=1}^{n} a_{ik} \left(\sum_{l=1}^{r} b_{kl} c_{lj} \right)$

Since $\sum_{l=1}^{r} \left(\sum_{k=1}^{n} a_{ik} b_{kl} \right) c_{lj} = \sum_{l=1}^{r} \left(\sum_{k=1}^{n} a_{ik} b_{kl} c_{lj} \right) = \sum_{k=1}^{n} a_{ik} \left(\sum_{l=1}^{r} b_{kl} c_{lj} \right)$,

we have $(A \times B) \times C = D \times C = A \times E = A \times (B \times C)$ (blog.csdn.net)

(a). ② unit element. $e = \mathbb{1} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in SL(n, \mathbb{R})$

$$A \times e = e \times A = A.$$

③ inverse: $\det A = 1 \neq 0$, then we can have A^{-1}

$\det A \cdot \det A^{-1} = 1 \Rightarrow \det A^{-1} = 1$

$A \cdot A^{-1} = A^{-1} \cdot A = e$

(b). ② unit element: $e = \mathbb{1} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in O(n, \mathbb{R})$

$$A \times e = e \times A = A$$

③ inverse: $A \times A^{-1} = A^{-1} \times A = e$

Therefore, there exists the inverse

(C). ② unit elemet: $e = \mathbb{1} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

$$A \times e = e \times A = A$$

③ inverse: Since $\det A = 1 \neq 0$, then we have A^{-1}

$A \times A^{-1} = A^{-1} \times A = e$

$\det(A \times A^{-1}) = \det A \det A^{-1} = 1 \Rightarrow \det A^{-1} = 1$

Ex 3.3 i) ① reflexive: $a \sim a \Leftrightarrow 2 \mid (a-a) \Leftrightarrow 2 \mid 0$, true

② symmetric: $m \sim n \Leftrightarrow 2 \mid (n-m) \Leftrightarrow n-m = 2k$

then $m-n = -2k \Leftrightarrow 2 \mid (m-n) \Leftrightarrow n \sim m$

③ transitive: $a \sim b \Leftrightarrow 2 \mid (b-a) \Leftrightarrow b-a = 2p$

$b \sim c \Leftrightarrow 2 \mid (c-b) \Leftrightarrow c-b = 2q$

$(b-a)+(c-b) = c-a = 2(p+q) \Leftrightarrow 2 \mid (c-a) \Leftrightarrow a \sim c$

ii) $n-m = 2k$, then m and n are both odd or even.

$$\mathbb{Z}_2 = \left\{ \{n \mid n = 2k+1, k \in \mathbb{Z}\}, \{n \mid n = 2k, k \in \mathbb{Z}\} \right\} = \{[0], [1]\}$$

iii) For $[m]+[n] = [m+n]$:

$[m'] = [m] \Rightarrow m'$ and m are both odd or even $\Rightarrow m'-m = 2p$

$[n'] = [n] \Rightarrow n'$ and n are both odd or even $\Rightarrow n'-n = 2q$

$m'-m+n'-n = (m'+n')-(m+n) = 2(p+q)$

Then $m'+n'$ and $m+n$ are both odd or even, meaning $[m'+n'] = [m+n]$

Therefore, it is indepedent of the representatives m and n of each class.

For $[m] \cdot [n] = [m \cdot n]$:

$[m'] = [m] \Rightarrow m'$ and m are both odd or even $\Rightarrow m'-m = 2p \Rightarrow m' = m+2p$

$[n'] = [n] \Rightarrow n'$ and n are both odd or even $\Rightarrow n'-n = 2q \Rightarrow n' = n+2q$

$m' \cdot n' = (m+2p)(n+2q) = mn+2mq+2pn+4pq$

$m' \cdot n' - mn = 2(mq+pn+2pq) \Rightarrow m' \cdot n'$ and $m \cdot n$ are both odd or even $\Rightarrow [m'n'] = [mn]$

Therefore, it is indepedent of the representatives m and n of each class.

iv). Since $\mathbb{Z}_2 = \{[0], [1]\}$,

we can have $[0] \neq [1]$

$\mathbb{Z}_2 \setminus \{0\} = \{[1]\}$, $[1] \cdot [1] = [1]$, so there is the a^{-1} element.

Therefre, $(\mathbb{Z}_2, +, \cdot)$ is a field.

Ex3.4 By Bézout's lemma, we have: $\exists\ x_0, y_0 \in \mathbb{Z}$ s.t. $ax_0 + by_0 = \gcd(a,b)$

Then we multiply m on both sides, $amx_0 + bmy_0 = m\cdot\gcd(a,b)$, $m \in \mathbb{Z}$

Let $x = mx_0$, $y = my_0$, then $ax + by = m\cdot\gcd(a,b)$.

Since $m \in \mathbb{Z}$, we have $x, y \in \mathbb{Z}$ and $m\cdot\gcd(a,b)$ can be all integer multiplies of $\gcd(a,b)$.

Therefore, we can prove it.

Ex3.5 For any n, we can express it as $n = 3m+1$ or $n = 3m+2$ or $n = 3m$

① $n = 3m+1$, $n^2 = 9m^2+6m+1 = 3(3m^2+2m)+1 = 3k+1$

② $n = 3m+2$, $n^2 = 9m^2+12m+4 = 3(3m^2+4m+1)+1 = 3k+1$

③ $n = 3m$, $n^2 = 9m^2 = 3(3m^2) = 3k$

Therefore, for any $n \in \mathbb{N}$, there exists $k \in \mathbb{N}$ such that either $n^2 = 3k$ or $n^2 = 3k+1$

Ex3.6 ① $n = 0$, $\gcd(a,a) = a$ and a divides 0 is true.

② $n \neq 0$, Since $a+n = a\times 1 + n$, by lemma 1.6.20,

$\gcd(a+n, a) = \gcd(a, n)$

Also $\gcd(a, a+n) = \gcd(a+n, a)$, we have $\gcd(a, a+n) = \gcd(a, n)$

Since $\gcd(a,n)$ divides n, $\gcd(a, a+n)$ must divides n.

When $n = 1$, $\gcd(a, a+1)$ divides 1, meaning $\gcd(a, a+1) = 1$.

Therefore, a and $a+1$ are alway relative prime.

Ex3.7 i) $72 = 1\times 56 + 16$

$56 = 3\times 16 + 8$

$16 = 2\times 8 + 0$

then $\gcd(72, 56) = 8$. Since $8 \mid 40$, a solution exists.

$8 = 56 - 16\times 3$

$= (72-16) - 16\times 3$

$= 72 - 4\times(72-56)$

$= -3\times 72 + 4\times 56$

$72\times(-15) + 56\times 20 = 40$

Therefore, $x = 20 + \frac{72}{8}t = 20 + 9t$

$y = -15 - \frac{56}{8}t = -15 - 7t$

for $t \in \mathbb{Z}$

ii) $-439 = -6\times 84 + 65$

$84 = 1\times 65 + 19$

$65 = 3\times 19 + 8$

$19 = 2\times 8 + 3$

$8 = 2\times 3 + 2$

$3 = 1\times 2 + 1$

$2 = 2\times 1 + 0$

so $\gcd(84, -439) = 1$. Since $1 \mid 156$, a solution exists.

$1 = 3 - 2$

$= (19 - 8\times 2) - 2$

$= 19 - 9\times 2$

$= 84 - 65 - 9\times(8 - 2\times 3)$

$= 84 + 439 - 6\times 84 - 9\times(65 - 3\times 19) + 18\times(19 - 2\times 8)$

$= -5\times 84 + 439 - 9\times(6\times 84 - 439) + 27\times 19 + 18\times 19 - 36\times(65 - 3\times 19)$

$= -59\times 84 + 10\times 439 + 153\times(84 - 65) - 36\times(6\times 84 - 439)$

$= -127\times 84 + 46\times 439 - 153\times(6\times 84 - 439)$

$= -1040\times 84 + 199\times 439$

$= (-199)\times(-439) - 1040\times 84$

Therefore, $84\times(-162240) - 439\times(-31044) = 156$

$x = -162240 - \frac{439}{1}t = -162240 - 439t$

$y = -31044 - \frac{84}{1}t = -31044 - 84t$

for $t \in \mathbb{Z}$

Ex3.8 i) Since $\gcd(a,b) = 1$, $\exists\, x_0, y_0$ such that $ax_0 + by_0 = 1$

Then $acx_0 + bcy_0 = c \Rightarrow acx_0 - b(-cy_0) = c$

Let $x = cx_0$, $y = -cy_0 \Rightarrow ax - by = c$

$x = cx_0 + bt$

$y = -cy_0 + at$

for $t \in \mathbb{Z}$

Therefore, there exists infinitely many solutions.

ii) $158 = 2\times 57 + 44$

$57 = 1\times 44 + 13$

$44 = 3\times 13 + 5$

$13 = 2\times 5 + 3$

$5 = 1\times 3 + 2$

$3 = 1\times 2 + 1$

$2 = 2\times 1 + 0$

so $\gcd(158, 57) = 1$

$1 = 3 - 2$

$= 3 - (5 - 3)$

$= 3\times 2 - 5$

$= (13 - 2\times 5)\times 2 - 5$

$= 13\times 2 - 5\times 5$

$= 13\times 2 - (44 - 3\times 13)\times 5$

$= 13\times 17 - 44\times 5$

$= (57 - 44)\times 17 - 44\times 5$

$= 57\times 17 - 44\times 22$

$= 57\times 17 - (158 - 2\times 57)\times 22$

$= 57\times 61 - 22\times 158$

$158\times(-154) - 57\times(-427) = 7$

$x = -154 + 57t$

$y = -427 + 158t$

for $t \in \mathbb{Z}$

Ex 3.9 i) Suppose there are numbers such that they're neither prime nor a product of primes.

By well-ordering principle, there exists a smallest one, denoted as x.

Then, x can be expressed as a product with at least one integer that is not prime.

For the integer that is not prime, it can be expressed as product of primes.

Then x can be expressed as product of primes, which is a contradiction.

Therefore, any number of S is either prime or a product of primes.

ii) $100 = 10 \times 10 = 4 \times 25$

Ex 3.10 i) Suppose $(4k+3) \mid d$.

Then $(4k+3) \times a = 4 \times (3 \times 7 \cdots P) - 1$, where $a \in \mathbb{Z}$.

Since $4k+3 \in D$, then

$$a = 4 \times \underbrace{(3 \times 7 \times \cdots \times P)}_{\text{without } 4k+3.} - \frac{1}{4k+3}$$

We know $\frac{1}{4k+3}$ can not be an integer.

So the right hand side is not an integer while the left hand side is an integer.

There is contradiction.

Therefore, no prime of the form $4k+3$ divides d.

ii). Suppose $(4k+1) \mid d$

Then $(4k+1) \times a = 4(3 \times 7 \times \cdots P) - 1$

① $a = 4n$ or $4n+2$.

$(4k+1) \times a$ is even while $4(3 \times 7 \times \cdots \times P) - 1$ is odd.

Therefore, $a = 4n$ or $4n+2$ can't be true.

② $a = 4n+1$

$(4k+1)(4n+1) = 16kn + 4(k+n) + 1 = 4(3 \times 7 \times \cdots \times P) - 1$

$4(3 \times 7 \times \cdots \times P - (k+n) - 4kn) = 2$

$3 \times 7 \times \cdots \times P - (k+n) - 4kn = \frac{1}{2}$

Left hand side is integer while right hand side is not integer.

Therefore, $a = 4n+1$ can't be true.

③ $a = 4n+3$

$$(4k+1) = 4 \cdot \underbrace{(3 \cdot 7 \cdot \cdots \cdot P)}_{\text{without } 4n+3} - \frac{1}{4n+3}$$

Left hand side is integer while right hand side is not integer.

Therefore, $a = 4n+3$ can't be true.

Therefore, no such a statisfies. So d can't be divided by $4k+1$.

iii) If it is finite, then there is a largest one, denoted as P.

$d = 4(3 \cdot 7 \cdots P) - 1$ is odd, then it can't be divided by even numbers.

Also, d can't be divided by $4k+1$ and $4k+3$, then d is prime number.

$d = 4(3 \cdot 7 \cdots P) - 1 = 4(3 \cdot 7 \cdot \cdots \cdot P - 1) + 3 > P$, also d is the prime number of the form $4n+3$.

so p is not the largest one, contradiction. Therefore, there is an infinite number of primes of the form $4n+3$