VE 203 Midterm 1 周雅凯 516021911039

Q1: ① When $n=0$, we have $2^0+(-1)^{0+1}=1+(-1)=0$, we can see that $3|0$.

② Then we need to show that $3|(2^{n+1}+(-1)^{n+1+1})$ if $3|(2^n+(-1)^{n+1})$.

i) if n is odd, then we need to show that $3|(2^{n+1}-1)$ if $3|(2^n+1)$.

Since $3|(2^n+1)$, we can denote: $2^n+1=3k$

Then $2^{n+1}-1=2(2^n+1)-3=2\times 3k-3=3(2k-1)$.

ii) if n is even, then we need to show that $3|(2^{n+1}+1)$ if $3|(2^n-1)$.

Since $3|(2^n-1)$, we can denote: $2^n-1=3k$

Then $2^{n+1}+1=2(2^n-1)+3=2\times 3k+3=3(2k+1)$.

Therefore, if $3|(2^n+(-1)^{n+1})$, we can have $3|(2^{n+1}+(-1)^{n+1+1})$.

Combining ① and ②, we can prove that $3|(2^n+(-1)^{n+1})$ for all $n\in\mathbb{N}$.

Q2. ① First prove $S\subset M$.

In particular, we show that if $s\in S$, then there exists n such that $s=1^n01^n$.

i) For $s=0$, we can choose $n=0$, so that $s=1^0 01^0=0$

ii) Assume that $s=1^n01^n$ for $n\in\mathbb{N}$.

Then $1s1=1^{n+1}01^{n+1}$.

Thus we can find $n'=n+1$, $n'\in\mathbb{N}$ such that $1s1$ can be written as $1^{n'}01^{n'}$.

This shows $S\subset M$.

② Then prove $M\subset S$.

In particular, we show that for all $n\in\mathbb{N}$, $1^n01^n\in S$

i) For $n=0$, $1^0 01^0=0\in S$

ii) Assume $1^n01^n\in S$, then $1^{n+1}01^{n+1}=11^n01^n1\in S$

Combining i), ii), we have for all $n\in\mathbb{N}$, $1^n01^n\in S$.

This shows $M\subset S$.

Therefore, $S=M$.

Q3.(a). ①, reflexive: For all $a\in\mathbb{Z}-\{0\}$, we have $a\cdot a>0$.

Therefore, it is reflexive.

②: symmetric: For all $a,b\in\mathbb{Z}-\{0\}$, if $a\sim b\Leftrightarrow a\cdot b>0\Leftrightarrow b\cdot a>0\Leftrightarrow b\sim a$

Therefore, it is symmetric

③: transitive: For all $a,b,c\in\mathbb{Z}$, if $a\sim b$, we have $a\cdot b>0$. If $b\sim c$, we have $b\cdot c>0$

$(a\cdot b)\cdot(b\cdot c)>0\Rightarrow acb^2>0$

Since $b\in\mathbb{Z}-\{0\}$, we have $b^2>0$.

From $acb^2>0$ and $b^2>0$, we have $ac>0\Leftrightarrow a\sim c$. Therefore, it is transitive.

Hence, this is an equivalence relation.

(b). It retains two of the required properties. It is not an equivalance relation.

① reflexive: $0\cdot 0=0\neq 0$. Therefore, it is not reflexive.

②symmetric: For all $a,b\in\mathbb{Z}$, if $a\sim b\Leftrightarrow a\cdot b>0\Leftrightarrow b\cdot a>0\Leftrightarrow b\sim a$

Therefore, it is symmetric

③transitive: For all $a,b,c\in\mathbb{Z}$, if $a\sim b$, we have $a\cdot b>0$. If $b\sim c$, we have $b\cdot c>0$

$(a\cdot b)\cdot(b\cdot c)>0\Rightarrow acb^2>0$

Since $b\in\mathbb{Z}$, we have $b^2\geq 0$. Also $acb^2>0$, therefore $b^2\neq 0$, meaning $b^2>0$.

From $acb^2>0$ and $b^2>0$, we have $ac>0\Leftrightarrow a\sim c$

Therefore, it is transitive.

Hence, it retains two of the required properties. It is not an equivalance relation.

(c). $x\sim y\Leftrightarrow xy>0$, therefore, x and y are both positive or negative. Hence $\{[\mathbb{Z}_+],[\mathbb{Z}_-]\}$

One fiber is positive number and the other fiber is negative number.

Q4.(a). Let $A, B, C \in P(M)$

① closure: $A \cap B = \{x : x \in A \wedge x \in B\} \in P(M)$

Therefore, $\cap$ is the operation that: $P(M) \times P(M) \to P(M)$

② associativity. $A \cap (B \cap C) = A \cap \{x : x \in B \wedge x \in C\}$

$= \{x : x \in A \wedge x \in B \wedge x \in C\}$

$= \{x : x \in A \wedge x \in B\} \cap C$

$= (A \cap B) \cap C$

③ unit element: $M \in P(M)$, $A \cap M = M \cap A = A$

④ inverse: there is no inverse A^{-1} such that $A \cap A^{-1} = A^{-1} \cap A = M$

⑤ commutativity: $A \cap B = \{x : x \in A \wedge x \in B\} = \{x : x \in B \wedge x \in A\} = B \cap A$

Therefore, $(P(M), \cap)$ is not a commutative group.

(b). ① closure: from the definition of $\Delta : P(M) \times P(M) \to P(M)$, we know it is closure.

② associativity: we take as granted the fact that it is associative.

③ unit element: $\phi \in P(M)$, $A \Delta \phi = (A \cap \phi^c) \cup (\phi \cap A^c) = A \cup \phi = A$

$\phi \Delta A = (\phi \cap A^c) \cup (A \cap \phi^c) = \phi \cup A = A$

$\Rightarrow A \Delta \phi = \phi \Delta A = A$

④ inverse: for every $A \in P(M)$, we can choose $A^{-1} = A$.

$A \Delta A^{-1} = A^{-1} \Delta A = A \Delta A = (A \cap A^c) \cup (A \cap A^c) = \phi \Rightarrow A^{-1} \Delta A = A \Delta A^{-1} = \phi$

⑥ commutativity. $A \Delta B = (A \cap B^c) \cup (B \cap A^c) = (B \cap A^c) \cup (A \cap B^c) = B \Delta A$

Therefore, $(P(M), \Delta)$ is a commutative group.

(c). ① closure:

From (a) and (b), we know both $\cap$ and Δ are closed.

② abelian group:

From (b), we know $(P(M), \Delta)$ is a commutative group, which is also called the abelian group.

③ multiplicative unit element:

From (a), we know there exist $M \in P(M)$ such that $A \cap M = M \cap A = A$

④ asociativity.

From (a), we know that $A \cap (B \cap C) = (A \cap B) \cap C$

⑤ distributivity.

$A \cap (B \Delta C) = A \cap [(B \cap C^c) \cup (C \cap B^c)] = (A \cap B \cap C^c) \cup (A \cap C \cap B^c)$

$(A \cap B) \Delta (A \cap C) = [(A \cap B) \cap (A \cap C)^c] \cup [(A \cap C) \cap (A \cap B)^c]$

$= [(A \cap B) \cap (A^c \cup C^c)] \cup [(A \cap C) \cap (A^c \cup B^c)]$

$= [(A \cap B \cap A^c) \cup (A \cap B \cap C^c)] \cup [(A \cap C \cap A^c) \cup (A \cap C \cap B^c)]$

$= [\phi \cup (A \cap B \cap C^c)] \cup [\phi \cup (A \cap C \cap B^c)]$

$= (A \cap B \cap C^c) \cup (A \cap C \cap B^c)$

Therefore: $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$

$(B \Delta C) \cap A = [(B \cap C^c) \cup (C \cap B^c)] \cap A = (B \cap C^c \cap A) \cup (C \cap B^c \cap A)$

$(B \cap A) \Delta (C \cap A) = [(B \cap A) \cap (C \cap A)^c] \cup [(C \cap A) \cap (B \cap A)^c]$

$= [(B \cap A) \cap (C^c \cup A^c)] \cup [(C \cap A) \cap (B^c \cup A^c)]$

$= [(B \cap A \cap C^c) \cup (B \cap A \cap A^c)] \cup [(C \cap A \cap B^c) \cup (C \cap A \cap A^c)]$

$= [(B \cap A \cap C^c) \cup \phi] \cup [(C \cap A \cap B^c) \cup \phi]$

$= (A \cap B \cap C^c) \cup (A \cap C \cap B^c)$

Therefore: $(B \Delta C) \cap A = (B \cap A) \Delta (C \cap A)$

⑥ commutative:

From (a) we know $A \cap B = B \cap A$

Therefore, it is a commutative ring.

$A \cap B = \phi \Rightarrow A = \phi$ or $B = \phi$

Therefore, it is an integral domain.

The unit element of Δ is ϕ and the unit element of $\cap$ is M,

For every $A \in P(M) \setminus \{\phi\}$, there is no A^{-1} such that $A \cap A^{-1} = M$.

Therefore, it is not a field.

Therefore, it is a commutative ring and an integral domain, but not a field.

Q5. $645 = 3 \cdot 5 \cdot 43$

Let $x \equiv 11^{644} \bmod 645$,

then $x \equiv 11^{644} \bmod 3$

$x \equiv 11^{644} \bmod 5$

$x \equiv 11^{644} \bmod 43$.

By Fermat's Little Theorem, we have:

$11^2 \equiv 1 \bmod 3$

$11^4 \equiv 1 \bmod 5$

$11^{42} \equiv 1 \bmod 43$

Therefore

$x \equiv 11^{644} \equiv (11^2)^{322} \equiv 1 \bmod 3$

$x \equiv 11^{644} \equiv (11^4)^{161} \equiv 1 \bmod 5$

$x \equiv 11^{644} \equiv 11^{42 \times 15 + 14} \equiv 11^{14} \equiv (11^2)^7 \equiv (35)^7 \equiv (35)^2 (35)^1 (35)^3 35 \equiv (21)^3 \cdot 35 \equiv 11 \cdot 21 \cdot 35 \equiv 1 \bmod 43$

$M = 3 \times 5 \times 43 = 645$

$m_1 = 215 \quad m_2 = 129 \quad m_3 = 15$

$$\begin{cases} 215\, y_1 \equiv 1 \bmod 3 \\ 129\, y_2 \equiv 1 \bmod 5 \\ 15\, y_3 \equiv 1 \bmod 43 \end{cases} \Rightarrow \begin{cases} y_1 = 2 \\ y_2 = 4 \\ y_3 = 23 \end{cases}$$

$11^{644} \equiv 2 \times 215 \times 1 + 4 \times 129 \times 1 + 15 \times 23 \times 1 \equiv 1291 \equiv 1 \bmod 645$