

代数序論A (第14回・2010/07/15) 小テスト

学籍番号		氏名	
------	--	----	--

[1] (同値関係) 集合  $X$  の2つの元の間定義された関係  $\sim$  が、次の3つの条件を満たすとき、この関係  $\sim$  を同値関係という。

(1) 反射律  $x \sim x (\forall x \in X)$ ,

(2) 対称律  $x \sim y$  ならば  $y \sim x (\forall x, y \in X)$ ,

(3) 推移律  $(\forall x, y, z \in X)$ ,

定理 . 集合  $X$  に同値関係  $\sim$  を定めると、同値類  $C(a) = [a]$  によって  $X$  の類別が得られる .

[2]  $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \dots, [m-1]\}$  を考える . 但し、 $[a] = a + m\mathbb{Z} = \{a + mn \mid n \in \mathbb{Z}\} = \bar{a}$  である . ここで、集合  $\mathbb{Z}/m\mathbb{Z}$  に2つの演算、加法  $+$  と乗法  $\cdot$  を以下の様に定義する .

$$[a] + [b] := [a + b], \quad [a] \cdot [b] := \boxed{\phantom{0}}$$

この同値類に対して定義された演算  $(+, \cdot)$  が、代表元の取り方に依らずに定まっていること、すなわち  $[a] = [a']$  かつ  $[b] = [b']$  ならば  $[a + b] = [a' + b']$  及び  $[ab] = [a'b']$  が成り立つことを、

w から始まる英単語1つを用いて、演算は  $\phantom{0}$  であるという .

[3]  $(\mathbb{Z}/m\mathbb{Z}, \cdot)$  に対して、 $\bar{a} = [a]$  として、演算表を書いてみる :

	$m = 2$			$m = 3$			$m = 4$				$m = 5$					$m = 6$										
	$\cdot$	$\bar{0}$	$\bar{1}$	$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$		
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$		
	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$		
	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	
	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	
	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

よって、 $m = 2, 3, 4, 5, 6$  のうち、 $\mathbb{Z}/m\mathbb{Z}$  が体となる  $m$  は  $\phantom{0}$  である .

[4]  $(\mathbb{Z}/m\mathbb{Z})^\times := \{[a] \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1\}$  に対して、 $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$  は位数  $\varphi(m)$  の可換群をなす . 群  $((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$  を既約剰余類群、 $\varphi(m)$  を  $\phantom{0}$  関数と呼ぶ .

$\varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6, \varphi(8) = 4, \varphi(9) = \boxed{\phantom{0}}$  .

[5] (オイラーの定理) 整数  $m \geq 2$  と  $\gcd(a, m) = 1$  なる整数  $a \in \mathbb{Z}$  に対して、以下が成り立つ :

$$a^{\varphi(m)} \equiv 1 \pmod{m} .$$

素数  $p$  に対して、 $m = p$  の場合、 $\varphi(m) = \boxed{\phantom{0}}$  であるから、オイラー (1707-1783) の

定理はある数学者 (1601-1665) の名前が付いた  $\phantom{0}$  の小定理の拡張になっている .

(1)  $2^{13}$  を 13 で割った余りは  $\phantom{0}$  , (2)  $5^{13}$  を 12 で割った余りは  $\phantom{0}$  .