Section A

MA10209 2016-17

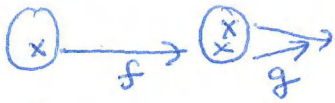
1 (a) F
(b) T
(c) F
(d) F
(e) F
(f) F
(g) T
(h) T
(i) F
(j) F

10 x 1 = [10]

---

2 (a) Yes, if f is not injective $\exists\, x, y \in A$ such that $f(x) = f(y)$ but $x \neq y$. [2]

Then $h(x) = g(f(x)) = g(f(y)) = h(y)$ so h would not be injective.

(b) No  or [2]

say $f: \{1\} \to \{1,2\}$ is defined by $f(1) = 1$
& $g: \{1,2\} \to \{1\}$ is defined by $g(1) = g(2) = 1$.
Then $h: \{1\} \to \{1\}$ is the identity map (& so injective) but $g(1) = g(2)$ so g is not injective.

(c) Yes. If $c \in C$, $\exists\, b \in B$ s.t. $g(b) = c$ since g is surjective. Now $\exists\, a \in A$ s.t. $f(a) = b$ since f is surjective. Now $h(a) = g(f(a)) = g(b) = c$. Therefore h is surjective. [2]

(d) No.  [2]

$A = B = C = \{1,2,3\}$; $f = g$; $f(1) = 2$, $f(2) = 3$ & $f(3) = 3$.
Notice $h(x) = 1$ for $x \in \{1,2,3\}$ so is a constant map, but neither f nor g is a constant map.

(e) No.  or $A = C = \{1\}$, $B = \{1,2\}$,

$f(1) = 1$, $g(1) = 1$ & $g(2) = 1$; h bijective but neither f nor g is bijective. [2]

3 (a) $247 = 1 \times 221 + 26$
$221 = 8 \times 26 + \boxed{13}$
$26 = 2 \times 13 + 0$

$\gcd(221, 247) = 13$ [4]

(b) $13 = 1 \cdot 221 - 8 \cdot 26$
$= 1 \cdot 221 - 8\,(247 - 221)$
$= 9 \cdot 221 - 8 \cdot 247$

& $\lambda = 9$ & $\mu = -8$ will work. [4]

(c) $221 = 13 \times 17$, $247 = 13 \times 19$

so $221 \times 10^{10} = 13 \times 17 \times 2^{10} \times 5^{10}$
& $247 \times 11^{11} = 13 \times 19 \times 11^{11}$ } prime factorizations

by Fundamental Thm of Arithmetic we can read off $\gcd(221 \times 10^{10}, 247 \times 11^{11}) = 13$. [2]

---

4. (a) If $x \in G$ & e is the identity element of H (& so of G) we have

$x = e \cdot x \in Hx$ & $x = x \cdot e \in xH$ [2]

so $x \in xH \cap Hx \neq \emptyset$.

(b) $G = S_3$. $H = \langle (12) \rangle = \{e, (12)\}$.

let $y = (23)$. Notice $(12)(23) = (123)$ [2]
& $(23)(12) = (132)$

Now $yH = \{(23), (132)\}$
& $Hy = \{(23), (123)\}$ so $yH \neq Hy$.

(c) e is the identity element of G (& H).

Notice $eH = H = He$ so $e \in K \neq \emptyset$.

Suppose that $x, y \in K$, then $(xy)K = x(yK)$

$= x(Ky) = (xK)y = (Kx)y = K(xy)$.

Therefore $xy \in K$.

Now suppose that $x \in K$, so $xK = Kx$,

$\Rightarrow (x^{-1}(xK))x^{-1} = (x^{-1}(Kx))x^{-1}$ [3]

(brackets unimportant by associativity)

so $(e \cdot K)x^{-1} = (x^{-1}K) \cdot e$ i.e. $Kx^{-1} = x^{-1}K$.

Therefore $x^{-1} \in K$ & so K is a subgroup of G.

(d) $x \in xH \cap Hx$ (see (a))

so $x \in Hy \cap Hx$.

Now if Hy & Hx are right cosets with non-trivial intersection, then they are equal [3]

so $Hx = Hy$

Section B

5 (a) If $n \in \mathbb{N}$, then $\varphi(n) = \left|\{ m \mid m \in \mathbb{Z}, 0 \leq m < n, \gcd(m,n) = 1 \}\right|$ [2]

(but also accept $\varphi(n) = n \prod_{\substack{p \text{ prime} \\ p \mid n}} (1 - 1/p)$. [2]

(b) $[m]$ has a multiplicative inverse in $\mathbb{Z}_n$ iff $\gcd(m,n) = 1$. Therefore $|\mathbb{Z}_n^\circ| = \varphi(n)$ [3]

where $\mathbb{Z}_n^\circ$ denotes the group of units of $\mathbb{Z}_n$.

(c) $8085 = 3 \times 5 \times 7^2 \times 11$ so $\varphi(8085) = 2 \times 4 \times 42 \times 10 = 3360$

(d) If p is prime & $p \mid m$ then $\varphi(p) \mid 4$ so $p = 2, 3$ or 5. [3]

Thus $m = 5$ or $5 \nmid m$; $m = 12$ or $3 \nmid m$; otherwise m is a power of 2 & so $m = 8$. Therefore $m \in \{12, 5, 8\}$.

6. (a) Suppose that m & n are coprime positive integers, and that a, b are integers. The pair of congruences $x \equiv a \bmod m$ & $x \equiv b \bmod n$ have a solution $x_0 \in \mathbb{Z}$. Moreover, the set of all possible solutions is $\{x_0 + kmn \mid k \in \mathbb{Z}\}$ i.e. the set of solutions of the single congruence $x \equiv x_0 \bmod mn$. [3]

(4)

(b) $m_1, \ldots, m_k$ are pairwise coprime positive integers & $a_1, \ldots, a_k$ are integers. Let $M = \prod_{i=1}^{k} m_i$.

The system of k congruences $x \equiv a_i \bmod m_i$ $(i = 1, \ldots, k)$ has an integer solution x_0 & the set of all solutions is $\{x_0 + kM \mid k \in \mathbb{Z}\}$ i.e. the set of solutions of the single congruence $x \equiv x_0 \bmod M$. [3]

(b) Let (p_i) denote the sequence of prime numbers in increasing size. Let $b = 10^9$.

Let $m_i = \prod_{j=(i-1)b+1}^{ib} p_j$ $\quad (i = 1, \ldots, b)$

(so m_1 is the product of the first billion primes; m_2 is the product of the next billion primes etc).

The m_i are pairwise coprime so the quantities m_i^b are also pairwise coprime.

By CRT there is a (positive) integer x_0 such is a solution to all congruences $x \equiv -i \bmod m_i^b$ for $i = 1, \ldots, b$. Then $x_0 + 1, \ldots, x_0 + b$ is the required sequence. [4]