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

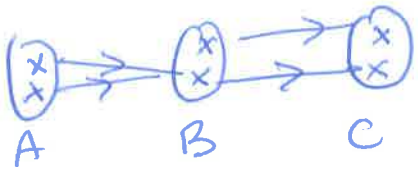
[10]

---

2 (a) Choose any $c \in C$. Now g is surjective so there is $b \in B$ such that $g(b) = c$. Also f is surjective so there is $a \in A$ such that $f(a) = b$. Now $(g \circ f)(a) = g(f(a))$ $= g(b) = c$. Therefore $g \circ f$ is surjective.

[2]

(b) Picture:



Let $A = B = C = \{1, 2\}$.

Define $f : A \to B$ by $f(1) = 1$ & $f(2) = 1$.

Define $g : B \to C$ by $g(1) = 1$ & $g(2) = 2$.

Now g is not a constant map but

$(g \circ f)(1) = (g \circ f)(2) = 1$.

[3]

(c) No, it does not follow. Conjure up f & g s.t. $g \circ f$ is injective but not surjective

eg $f : \mathbb{N} \to \mathbb{N}$ (identity map) $x \mapsto x$ $\forall x \in \mathbb{N}$ & $g : \mathbb{N} \to \mathbb{Z}$ (inclusion map) $x \mapsto x$ $\forall x \in \mathbb{N}$

so $A = B = \mathbb{N}$ & $C = \mathbb{Z}$; define $h : C \to A$ by $h(x) = x$ if $x > 0$ & $h(x) = 1729$ if $x \leq 0$. Then $h \circ g \circ f = Id_A$ but $g \circ f \circ h \neq Id_C$ (e.g. $g \circ f \circ h(-1) = 1729$. values so

[2]

(d) There are four maps, two of which (the constant maps) are neither injective nor surjective. The answer is therefore $4-2=2$. [3]

---

3 (a) $F^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$

(b) $F+I = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ $(= F^2)$

(c) $F^2 = F + I$ so $F^{-1}F^2 = F^{-1}F + F^{-1}I$

(note F^{-1} exists because $\det F = -1 \neq 0$)

$\therefore F = I + F^{-1}$ so $F^{-1} = F - I = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$.

(d) $F^3 = F^2 + F = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$

(e) $F^{10} = (F^5)^2 = (F^2 \cdot F^3)^2$

$= \left(\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} \right)^2 = \begin{pmatrix} 8 & 5 \\ 5 & 3 \end{pmatrix}^2 = \begin{pmatrix} 89 & 55 \\ 55 & 34 \end{pmatrix}$

5×[2]

---

4 Cycle type can only be $(***)$.

(a) There are $\binom{5}{3} \times 2 = 20$ 3-cycles.

(choose the three elts of the 3-cycle; write the smallest as the first entry, then two choices to complete..

[3]

4 (b) The 20 elements $(***)$ are all conjugate (*)

so $C_G((123))$ has order $\frac{120}{20} = 6$.

↑ centralizer of (123) = stabilizer of (123) when G acts on itself by conjugation.

These six elements commute with (123):

id, (123), $(123)^2 = (132)$, (45), $(123)(45)$ & $(132)(45)$ & so these are all elements which commute with (123). [3]

Justification of (*):

$(bc)(abc)(bc)^{-1} = (bc)(abc)(bc)$

$= (acb)$.

Therefore all 3-cycles are conjugate to their inverses. (**)

Also $(14)(123)(14)^{-1} = (14)(123)(14) = (234)$

& so if two 3-cycles have two elements in common they are conjugate (either way round - using **)

Also $(14)(25)(123)\left((14)(25)\right)^{-1} = (14)(25)(123)(14)(25)$

$= (345)$ so if two 3-cycles has one elements in common then they are conjugate (either way round by (*)).

∴ All 3-cycles are conjugate.

NB. Final part marked [was not required for full marks.

(c) There are 15 elements with this cycle shape; they are all conjugate ('routine'). [4]

Size of centralizer is $\frac{120}{15} = 8$.

Here they are: $1d$, (1324), $(1324)^2 = (12)(34)$,
$(1324)^3 = (1324)^{-1} = (1423)$,
(12), (34), $(13)(24)$, $(14)(23)$.

---

5 (a)
$$\begin{aligned} 8281 &= 3 \cdot 2210 + 1651 \\ 2210 &= 1 \cdot 1651 + 559 \\ 1651 &= 2 \cdot 559 + 533 \\ 559 &= 1 \cdot 533 + 26 \\ 533 &= 20 \cdot 26 + (13) \\ 26 &= 2 \cdot 13 + 0 \end{aligned}$$

gcd is 13 [2]

Now
$$\begin{aligned} 13 &= 533 - 20 \cdot 26 \\ &= 533 - 20(559 - 533) \\ &= 21 \cdot 533 - 20 \cdot 559 \\ &= 21 \cdot 1651 - 62 \cdot 559 \\ &= 83 \cdot 1651 - 62 \cdot 2210 \\ &= 83 \cdot 8281 - 331 \cdot 2210 \end{aligned}$$

[3]

(b) The set of all possible λ & μ is

$$\{(\lambda,\mu) = \{(83 + \tfrac{8281 \cdot 2210}{13 \cdot 8281} t, -331 - \tfrac{8281 \cdot 2210}{2210 \cdot 13} t) \mid t \in \mathbb{Z}\}$$

$$= \{(83 + 170t, -331 - 637t) \mid t \in \mathbb{Z}\}.$$

(see theory on a problem sheet).

5 (c) Squares in $\mathbb{Z}_{13}$: $0, 1, 4, 9, 3, 12, 10$

so -1 is a square; $-1 = 5^2 = 8^2$.

$$x^2 + 1 = x^2 - (-1) = x^2 - 5^2 = (x-5)(x+5)$$
$$= (x-5)(x-8)$$
in $\mathbb{Z}_{13}[x]$. [2]

(d). 2 is not a square in $\mathbb{Z}_{13}[x]$.

Suppose that x^2+2 factorized in $\mathbb{Z}_{13}[x]$ in a non-trivial way (into linear polynomials) (for contradiction).

$$x^2 + 2 = (ax+b)(cx+d)$$

so $acd = 1$ multiply by $\frac{1}{a} \cdot \frac{1}{c} (= 1)$. [3]

$$x^2 + 2 = \left(x + \frac{b}{a}\right)\left(x + \frac{d}{c}\right)$$
$$= (x - \alpha)(x - \beta);$$

so $x^2 + 2$ has a root $\alpha \in \mathbb{Z}_{13}$.

$\therefore \alpha^2 + 2 = 0 \quad \therefore \alpha^2 = -2$ which is impossible.

6 (a) if H is a subgroup of the finite group G, then $|H| \mid |G|$. [2]

(b) Lagrange $\Rightarrow$ if $x \in G$ & G is a finite group, then $x^{|G|} = id_G$.

Euler-Fermat $n \in \mathbb{N}$, G = group of units of $\mathbb{Z}_n$; $|G| = \varphi(n)$. [3]

$\therefore$ if $x \in G$, then $x^{\varphi(n)} = id$

(i.e. if $y \in \mathbb{Z}$ & $\gcd(n, y) = 1$, then $y^{\varphi(n)} \equiv 1 \mod n$).

If n is prime, Euler-Fermat becomes Fermat's Little Theorem.

(c) $2014 = 19 \times 106 = 19 \times 2 \times 53$ (all prime). [2]

$\therefore \varphi(2014) = \varphi(19)\varphi(2)\varphi(53)$

$= 18 \cdot 1 \cdot 52 = 936.$

(d) Euler-Fermat: $3^{936} \equiv 1 \mod 2014$ [3]

$\therefore 3^{1872} \equiv 1 \mod 2014$

$\therefore 3^{1875} \equiv 3^3 \cdot 3^{1872} \equiv 3^3 \equiv 27 \mod 2014$

$\therefore$ Answer is 27.

7. (a) $f = x^5 + x^4 + x^3 + x^2 + x + 1 \in \mathbb{R}[x]$

$(x-1)f = x^6 - 1 = (x^3-1)(x^3+1)$

$= (x-1)(x+1)(x^2+x+1)(x^2-x+1)$

$\mathbb{R}[x]$ is an integral domain so

$f = (x+1)(x^2+x+1)(x^2-x+1)$. [3]

three factors.

(b) $x+1$ irred because degree is 1.

both x^2+x+1 & x^2-x+1 have discriminant -3 and so no real roots & so no linear (real coeff) factors. They are therefore both irreducible. [3]

(c) $g_k = \sum_0^{k-1} x^i \in \mathbb{R}[x]$.

$\therefore (x-1) \mid g_k = x^k - 1$. [4]

Any root of g_k must be a root of x^k.

If k is even, there are two possibilities 1 & -1

If k is odd, only possibility is 1.

If k even; 1 not a root (by inspection)

$k-1$ is a root.

If k odd; 1 not a root (by inspection).

g_k has a root (-1) iff k is even.

8 (a) There are many. Here is one.

$$\alpha : \mathbb{N} \to \mathbb{Z}$$

$$2n \mapsto n \quad \text{if } n \in \mathbb{N}$$

$$2n-1 \mapsto -n+1 \quad \text{if } n \in \mathbb{N}. \qquad [3]$$

(b) Let the primes be $p_1, p_2, p_3, \ldots$ in ascending order $(2, 3, 5, \ldots)$.

Define a map f from S (the finite subsets of $\mathbb{N}$) to $\mathbb{N}$ [3]

by $f(X) = \prod_{x \in X} p_x$ if $X \neq \emptyset$

& $f(\emptyset) = 1$.

This map is injective by the fundamental theorem of arithmetic so S is in bijective correspondence with a subset of a countable set, and so is countable. [4]

(c) S in (b) is countable.

The ("complement in $\mathbb{N}^4$") map shows that complements of elts of S are countable.

Therefore moieties are uncountable, else $P(S)$ would be countable.