Instructions. Answer each of the questions on your own paper and be sure to show your work so that partial credit can be adequately assessed. Put your name on each page of your paper.

1. [**20 Points**] Let $G = \langle a \rangle$ be a cyclic group of order 45.

   (a) Compute the order of each of the following elements: (i) a^2 (ii) a^5 (iii) a^{27}

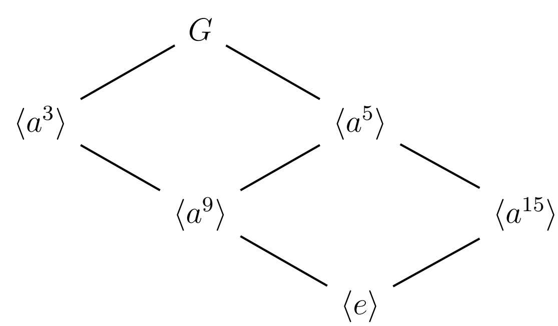
   ▶ **Solution.** The formula for the order of a power a^m of an element a of order n is $o(a^m) = \dfrac{n}{\gcd(m,\, n)}$. Hence, (i) $o(a^2) = \dfrac{45}{\gcd(2,\, 45)} = 45/1 = 45$, (ii) $o(a^5) = \dfrac{45}{\gcd(5,\, 45)} = 45/5 = 9$, (iii) $o(a^{27}) = \dfrac{45}{\gcd(27,\, 45)} = 45/9 = 5$. ◀

   (b) How many generators of G are there?

   ▶ **Solution.** a^m generates G if and only if $o(a^m) = 45$ if and only if $\gcd(m,\, 45) = 1$. Thus the number of generators of G is the Euler-φ function of 45, i.e. $\varphi(45) = \varphi(9)\varphi(5) = (3^2 - 3)(5 - 1) = 24$. ◀

   (c) Find all of the subgroups of G and draw the subgroup diagram for G.

   ▶ **Solution.** All of the subgroups of G are cyclic and there is a unique such subgroup for each divisor k of 45, namely $\langle a^{45/k} \rangle$. The divisors of 45 are 1, 3, 5, 9, 15, and 45 so the subgroups of G are $\langle a \rangle = G$, $\langle a^3 \rangle$, $\langle a^5 \rangle$, $\langle a^9 \rangle$, $\langle a^{15} \rangle$, and $\langle a^{45} \rangle = \langle e \rangle$. The subgroup diagram for G is



◀

2. [**25 Points**]

   (a) Complete the definition of *group homomorphism*: If G and G' are groups, a function $\varphi : G \to G'$ is a group homomorphism if

$$\boxed{\varphi(ab) = \varphi(a)\varphi(b) \text{ for all } a,\, b \in G.}$$

   (b) Give the definition of the *kernel* of a group homomorphism.

▶ **Solution.** $\mathrm{Ker}(\varphi) = \{x \in G \mid \varphi(x) = e\}$. ◀

(c) In each case determine whether $\varphi : G \to G_1$ is a group homomorphism. Use the definition you provided in part (a) to prove that your answer is correct.

i. $G = G_1 = \mathbb{Z}_7^*$, $\quad \varphi(a) = a^2$.

▶ **Solution.** $\varphi(ab) = (ab)^2 = abab = a^2b^2 = \varphi(a)\varphi(b)$, where the third equality is valid because $ba = ab$ for all choices of a, b in $\mathbb{Z}_7^*$. Hence, this φ is a group homomorphism. ◀

ii. $G = G_1 = S_3$, $\quad \varphi(a) = a^2$.

▶ **Solution.** In this case, $\varphi((1,\, 2)(1,\, 3)) = \varphi((1,\, 3,\, 2)) = (1,\, 3,\, 2)^2 = (1,\, 2,\, 3)$, while $\varphi((1,\, 2))\varphi((1,\, 3)) = (1,\, 2)^2(1,\, 3)^2 = (1)(1) = (1)$. Thus

$$\varphi((1,\, 2)(1,\, 3)) \neq \varphi((1,\, 2))\varphi((1,\, 3)),$$

and hence, this φ is not a group homomorphism. ◀

(d) For each function φ in part (c) that is a group homomorphism, find the kernel of φ, denoted $\mathrm{Ker}(\varphi)$, and the image $\varphi(G)$.

▶ **Solution.** The values of $\varphi : \mathbb{Z}_7^* \to \mathbb{Z}_7^*$ defined by $\varphi(a) = a^2$ are as follows:

a	1	2	3	4	5	6
$\varphi(a) = a^2$	1	4	2	2	4	1

From this table, $\mathrm{Ker}(\varphi) = \{1,\, 6\}$ and $\varphi(G) = \{1,\, 2,\, 4\}$. ◀

3. [**25 Points**] Recall that the dihedral group D_4 is defined by generators and relations as

$$\begin{aligned} D_4 &= \langle a,\, b | a^4 = e,\, b^2 = e,\, ba = a^{-1}b \rangle \\ &= \left\{e,\, a,\, a^2,\, a^3,\, b,\, ab,\, a^2b,\, a^3b\right\}. \end{aligned}$$

For convenience the multiplication table for D_4 is given here:

$\cdot$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

(a) List all of the *distinct* left cosets of the subgroup $H = \{e,\, a^2\}$ in D_4.

▶ **Solution.** $eH = H = \{e, a^2\}$, $aH = \{a, a^3\}$, $bH = \{b, a^2b\}$, and $abH = \{ab, ga^3b\}$. ◀

(b) Verify that H a normal subgroup of D_4? You may assume that H is a subgroup. It is only necessary to verify that H is *normal. Hint: Observe from the multiplication table that $a^2x = xa^2$ for all $x \in D_4$.*

▶ **Solution.** H is normal in D_4 provided $ghg^{-1} \in H$ for all $g \in D_4$ and $h \in H$. Since $geg^{-1} = e \in H$ and since $ga^2 = a^2g$ for all $g \in Q$ (by comparing the entries in the third row (a^2g) and third column (ga^2)), we have $ga^2g^{-1} = a^2 \in H$ for all $g \in Q$. Since $H = \{1, a^2\}$ we have shown that $ghg^{-1} = h \in H$ for all $h \in H$ and $g \in D^4$. Hence H is normal in D^4. ◀

(c) Write the multiplication table for the factor group D_4/H.

▶ **Solution.** The multiplication rule for cosets of a normal group N in a group G is $(cN)(dN) = (cd)N$, i.e., multiply the corresponding representatives. Thus, using the multiplication table for D_4 we have:

$\cdot$	H	aH	bH	abH
H	H	aH	bH	abH
aH	aH	H	abH	bH
bH	bH	abH	H	aH
abH	abH	bH	aH	H

◀

(d) Is D_4/H a cyclic group? Explain.

▶ **Solution.** D_4/H is not cyclic, since $|Q/H| = 4$ but every nonidentity element has order 2, as seen from the multiplication table above. Indeed, the table shows that $(xH)^2 = H$ for all cosets xH, and the identity of D_4/H is the coset H, so the square of every element of D_4/H is the identity. ◀

4. [**10 Points**] Compute the number of polynomials in $\mathbb{Z}_5[x]$ of degree 4.

▶ **Solution.** A polynomial of degree 4 over $\mathbb{Z}_5$ has the form

$$f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

where $a_4 \neq 0 \in \mathbb{Z}_4$, while each of the other coefficients can be any of the five elements of $\mathbb{Z}_5$. Since the coefficients can be assigned independently of each other, it follows that there are a total of $4 \cdot 5^4 = 2500$ possible polynomials of degree 4 in $\mathbb{Z}_5[x]$. ◀

5. [**20 Points**] Let $f(x) = x^3 - 1$ and let $g(x) = x^4 + x^3 + 2x^2 + x + 1$ be polynomials in $\mathbb{Z}_5[x]$.

(a) Use the Remainder Theorem to determine if $x - 2$ divides $g(x)$ in $\mathbb{Z}_5[x]$.

▶ **Solution.** The remainder theorem states that $x - 2$ divides $g(x)$ if and only if $g(2) = 0$. But

$$g(2) = 2^4 + 2^3 + 2 \cdot 2^2 + 2 + 1 = 35 \equiv 0 \pmod 5.$$

Hence $g(2) = 0 \in \mathbb{Z}_5$ so $x - 2$ divides $g(x)$. ◀

(b) Use Euclid's Algorithm to find $d(x) = \gcd(f(x), g(x))$.

▶ **Solution.** Use the division algorithm to get

$$x^4 + x^3 + 2x^2 + x + 1 = (x^3 - 1)(x + 1) + 2x^2 + 2x + 2,$$

and $x^3 - 1 = (2x^2 + 2x + 2)(3x + 3)$. Hence, the gcd of $x^3 - 1$ and $x^4 + x^3 + 2x^2 + x + 1$ is $x^2 + x + 1$ (remember that we defined gcd to be a monic polynomial). ◀

(c) Express $d(x)$ in the form $d(x) = a(x)f(x) + b(x)g(x)$, for polynomials $a(x)$, $b(x) \in \mathbb{Z}_5[x]$.

▶ **Solution.**

$$\begin{aligned} x^2 + x + 1 &= 3(2x^2 + 2x + 1) \\ &= 3(x^4 + x^3 + 2x^2 + x + 1 - (x + 1)(x^3 - 1)) \\ &= 3g(x) - 3(x + 1)f(x). \end{aligned}$$

◀