

In most cases the answer is given with a *very* detailed justification.

1. (30 pts.) Let $G = \langle a \rangle$ be a cyclic group of order 66.

a) How many subgroups does G have?

Solution: The correspondence $H \mapsto |H|$ describes a bijection between the set of subgroups of G and the set of divisors of $|G| = 66 = 2 \cdot 3 \cdot 11$. Since there are 8 divisors of 66; hence G has 8 subgroups. **(5 points)**

b) For each subgroup of G list its size and *one* generator.

Solution: If d is a positive divisor of $n = 66$ then $|\langle a^d \rangle| = n/d$ and therefore $|\langle a^{n/d} \rangle| = d$.

size	a generator
1	$a^{30} = e$
2	a^{33}
3	a^{22}
6	a^{11}
11	a^6
22	a^3
33	a^2
66	$a^1 = a$

(6 points).

c) List *all* generators of the subgroup of G of order 6.

Solution: The integers $1 \leq k \leq 6$ which are relatively prime to 6 are: 1, 5. Thus the generators of the subgroup of order 6 of G are

$$\boxed{(a^{11})^1 = a^{11}, \quad (a^{11})^5 = a^{55}. \quad \text{(5 points)}}$$

d) Find a divisor d of 66 such that $\langle a^{-42} \rangle = \langle a^d \rangle$ and list the distinct elements of $\langle a^{-42} \rangle$.

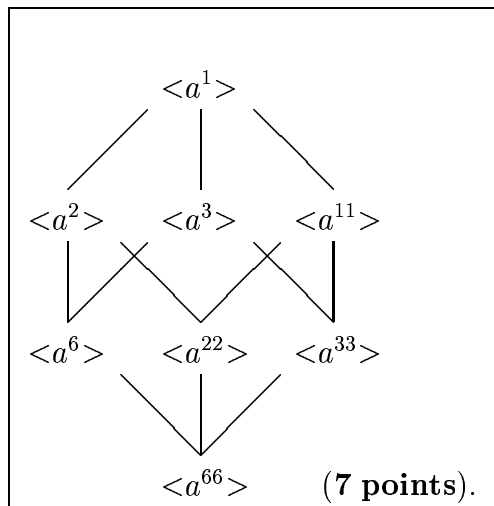
Solution: The greatest common divisor of -42 and 66 is 6. Therefore we may take $d = 6$ **(2 points)** and thus

$$\boxed{\langle a^{-42} \rangle = \langle a^6 \rangle = \{e, a^6, a^{12}, a^{18}, a^{24}, a^{30}, a^{36}, a^{42}, a^{48}, a^{54}, a^{60}\}. \quad \text{(5 points).}}$$

Note: $d = -6$ works just as well.

e) Write down the lattice of all subgroups of G .

Solution: If d, d' are divisors of $n = 66$ then $\langle a^d \rangle \subseteq \langle a^{d'} \rangle$ if and only if d' divides d .



2. (20 pts.) Consider the permutation $f = (1\ 3\ 2\ 4\ 9\ 8\ 6\ 5\ 7)(4\ 7)(6\ 9)$ of S_9 .

a) Write f as a product of *disjoint* cycles.

Solution: $f = (1\ 3\ 2\ 4)(5\ 7\ 9)(6\ 8)$, or any rearrangement of these cycles. (5 points)

b) Write f as a product of transpositions.

Solution: Using our cyclic decomposition we have

$$f = (1\ 4)(1\ 2)(1\ 3)(5\ 9)(5\ 7)(6\ 8) \quad (5 \text{ points}).$$

One can go back and replace the cycles in the definition of f and write

$$f = (1\ 7)(1\ 5)(1\ 6)(1\ 8)(1\ 9)(1\ 4)(1\ 2)(1\ 3)(4\ 7)(6\ 9)$$

as well.

c) Is f even? You must justify your answer.

Solution: Since f is the product of an even number of 2-cycles it follows that f is even. (5 points)

d) What is the order of f ?

Solution: The order of f is the least common multiple of its disjoint cycle lengths and is therefore 12. (5 points)

3. (25 pts.) Let $G = \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a, b \in \mathbf{R} \right\}$.

a) Show that G is a subgroup of $\text{GL}(3, \mathbf{R})$.

Solution: We first note that

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & a' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & a+a' \\ 0 & 1 & b+b' \\ 0 & 0 & 1 \end{pmatrix} \quad (1)$$

for all $a, a', b, b' \in \mathbf{R}$. In particular

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & -a \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix}$$

for all $a, b \in \mathbf{R}$. Thus for

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & a' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} \in G$$

we have

$$\boxed{\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & a' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & a-a' \\ 0 & 1 & b-b' \\ 0 & 0 & 1 \end{pmatrix} \in G. \quad (13 \text{ points})}$$

Since $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in G$, here $a = b = 0$, it follows that G is non-empty. **(2 points)**

Thus G is a subgroup of $\text{GL}(3, \mathbf{R})$.

b) Show that $\mathbf{R} \oplus \mathbf{R} \simeq G$, where \mathbf{R} is regarded as a group under addition.

Solution: Define $f : \mathbf{R} \oplus \mathbf{R} \rightarrow G$ by

$$f((a, b)) = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

for all $(a, b) \in \mathbf{R} \oplus \mathbf{R}$. Then f is onto by definition. **(2 points)** Since two matrices of the same dimensions are equal if and only if their corresponding components are equal, it follows that f is one-one. **(2 points)**

Suppose that $(a, b), (a', b') \in \mathbf{R} \oplus \mathbf{R}$. Then $f((a, b) + (a', b')) = f((a + a', b + b'))$ is the right hand side of (1) and $f((a, b)f((a', b')))$ is the left hand side of the same. Therefore $f((a, b) + (a', b')) = f((a, b)f((a', b'))$ (6 points) which completes our proof that f is an isomorphism.

4. (25 pts.) Let G, G' be finite groups where $G = \langle a \rangle$ is cyclic of order n .

- a) For $b \in G'$, show that $f : G \rightarrow G'$ given by $f(a^m) = b^m$ is a well-defined group homomorphism if and only if $|b|$ divides n .

Solution: Suppose that f described above is a homomorphism. Then

$$e = f(e) = f(a^n) = f(a)^n = b^n \text{ implies that } |b| \text{ divides } n. \text{ (3 points)}$$

Conversely, suppose that $b \in G'$ and $|b|$ divides n . Define f as above. Then f is well-defined. For if $a^m = a^{m'}$ then n divides $m - m'$. Since $|b|$ divides n it follows that $|b|$ divides $m - m'$. As a consequence $b^m = b^{m'}$. (3 points)

The fact that f is a homomorphism follows by the calculation

$$f(a^k a^m) = f(a^{k+m}) = b^{k+m} = b^k b^m = f(a^k) f(a^m) \text{ (8 points)}$$

for all integers k, m .

- b) Find all group homomorphisms $f : \mathbf{Z}_{20} \rightarrow \mathbf{Z}_{32}$.

Solution: Here additive notation is used instead of multiplicative. We make take $a = 1$. By parts a) and b) it is a matter of finding $b \in \mathbf{Z}_{32}$ such that $|b|$ divides 20. Then $f(1) = b$ determines a homomorphism $f : \mathbf{Z}_{20} \rightarrow \mathbf{Z}_{32}$.

By Lagrange's Theorem $|b|$ divides 32. (This is more basically a result about cyclic groups.) Thus $|b|$ divides 20, 32 which means $|b| = 1, 2, \text{ or } 4$. Thus

$$b = 0, 16 \text{ or } 8, 24 \text{ and these all work. (11 points)}$$

5. (25 pts.) Consider ring $R = \mathbf{Z}_{12}$.

- a) List the nilpotent elements of R .

Solution: If a is a nilpotent element of $R = \mathbf{Z}_{12}$ if and only if 2, 3 divide a . Thus $a = 0, 6$ are the nilpotent elements of R . (6 points)

- b) List the *zero divisors* of R . For each zero divisor a list a non-zero $b \in R$ such that $ab = 0$.

Solution: Let $a, b \in R$. Then $ab = 0$ holds if and only if 12 divides the integer product ab . The list of zero divisors is $\boxed{2, 3, 4, 6, 8, 10. \quad (4 \text{ points})}$

a	b	
2	6	(5 points)
3	4	
4	3	
6	2	
8	3	
9	4	
10	6	

- c) List the units of R and write down a Cayley table for $U(R)$.

Solution: The units of R are those $a \in R$ which are relatively prime to 12. Thus $\boxed{U(R) = \{1, 5, 7, 11\}. \quad (4 \text{ points})}$ A Cayley table for $U(R)$ is

	1	5	7	11	
1	1	5	7	11	(6 points)
5	5	1	11	7	
7	7	11	1	5	
11	11	7	5	1	

6. (25 pts.) Consider the subset $R = \{a + bi \mid a, b \in \mathbf{Z}\}$ of the field of complex numbers \mathbf{C} .

- a) Show that R is a subring of \mathbf{C} .

Solution: First of all $0 = 0 + 0i \in R$; therefore $\boxed{R \neq \emptyset. \quad (1 \text{ point})}$ Suppose that $a + bi, a' + b'i \in R$. Then $a, b, a', b' \in \mathbf{Z}$. Therefore $a - a', b - b' \in \mathbf{Z}$ and consequently

$$\boxed{(a + bi) - (a' + b'i) = (a - a') + (b - b')i \in R. \quad (4 \text{ points})}$$

We have shown that R is an additive subgroup of \mathbf{C} . Now $aa' - bb', ab' + a'b \in \mathbf{Z}$ as well. Therefore $\boxed{(a + bi)(a' + b'i) = (aa' - bb') + (ab' + a'b)i \in R. \quad (5 \text{ points})}$ This completes the proof that R is a subring of \mathbf{C} .

- b) Determine whether or not R a subfield of \mathbf{C} .

Solution: R is not a subfield of \mathbf{C} since,

$$\boxed{\text{for example, } (1 + i)^{-1} = \frac{1 - i}{1^2 + 1^2} = \frac{1}{2} - \frac{1}{2}i \notin R. \quad (8 \text{ points})}$$

- c) List the elements of $U(R)$. Is $U(R)$ a cyclic group? Justify your answer. [Hint: If z is a non-zero complex number then $1 = |zz^{-1}| = |z||z^{-1}|$, and thus $1 = |z|^2|z^{-1}|^2$.]

Solution: Suppose that $z = a + bi \in U(R)$. Then $|z|^2 = a^2 + b^2$ is a non-negative integer. By the hint $1 = |z|^2|z^{-1}|^2$ is the product of positive integers. Therefore $|z|^2 = 1$ which means $z = \pm 1$ or $z = \pm i$. Since $1^2 = (-1)^2 = 1$ and $i(-i) = -i^2 = 1$ these four elements are units. Thus $U(R) = \{1, -1, i, -i\}$. (4 points) Since

$$i^2 = -1, i^3 = i^2i = (-1)i = -i, i^4 = (i^2)^2 = (-1)^2 = 1$$

it follows that $U(R)$ is cyclic and generated by i . (3 points)

7. (25 pts.) Let $\phi : \mathbf{C} \rightarrow M(2, \mathbf{R})$ be the one-one function from the field of complex numbers to the ring of 2×2 matrices with real coefficients defined by $\phi(a + bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

- a) Show that ϕ is a ring homomorphism.

Solution: Let $a + bi, a' + b'i \in \mathbf{C}$. The calculations

$$\begin{aligned} \phi((a + bi) + (a' + b'i)) &= \phi((a + a') + (b + b')i) \\ &= \begin{pmatrix} a + a' & -b - b' \\ b + b' & a + a' \end{pmatrix} \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} \\ &= \phi(a + bi) + \phi(a' + b'i) \end{aligned}$$

show that $\phi((a + bi)(a' + b'i)) = \phi(a + bi)\phi(a' + b'i)$ (6 points) and

$$\begin{aligned} \phi((a + bi)(a' + b'i)) &= \phi((aa' - bb') + (ab' + a'b)i) \\ &= \begin{pmatrix} aa' - bb' & -ab' - a'b \\ ab' + a'b & aa' - bb' \end{pmatrix} \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} \\ &= \phi(a + bi)\phi(a' + b'i) \end{aligned}$$

show that $\phi((a + bi)(a' + b'i)) = \phi(a + bi)\phi(a' + b'i)$ (6 points); hence ϕ is a ring homomorphism.

- b) Compute $(3 + 2i)^{-1}$. Use the answer and ϕ to find $\begin{pmatrix} 3 & -2 \\ 2 & 3 \end{pmatrix}^{-1}$.

Solution: $(3 + 2i)^{-1} = \frac{3 - 2i}{3^2 + 2^2} = \frac{3}{13} - \frac{2}{13}i$. Since

$\phi(z^{-1}) = \phi(z)^{-1}$ for all non-zero $z \in \mathbf{C}$ (4 points), it follows that

$$\begin{pmatrix} 3 & -2 \\ 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{3}{13} & -(-\frac{2}{13}) \\ -\frac{2}{13} & \frac{3}{13} \end{pmatrix} = \begin{pmatrix} \frac{3}{13} & \frac{2}{13} \\ -\frac{2}{13} & \frac{3}{13} \end{pmatrix}. \quad (3 \text{ points})$$

- c) Compute $(3 + 2i)^2$. Use the answer and ϕ to find $\begin{pmatrix} 3 & -2 \\ 2 & 3 \end{pmatrix}^2$.

Solution: $(3 + 2i)^2 = (3 + 2i)(3 + 2i) = 5 + 12i$. Since

$\phi(zz') = \phi(z)\phi(z')$ for all $z, z' \in \mathbf{C}$ (3 points) it follows that

$$\begin{pmatrix} 3 & -2 \\ 2 & 3 \end{pmatrix}^2 = \begin{pmatrix} 5 & -12 \\ 12 & 5 \end{pmatrix}. \quad (3 \text{ points})$$

8. (25 pts.) Let R be a ring.

- a) Define *ideal of R* .

Solution: An ideal of R is

an additive subgroup I of R which satisfies $ra, ar \in I$ for all $r \in R$ and $a \in I$. (7 points)

- b) Suppose that I, J are ideals of R . Show that $I \cap J$ is an ideal of R .

Solution: First of all $I \cap J$ is an additive subgroup of R . Since I, J are additive subgroups of R , $0 \in I, J$ and $a - b \in I, J$ for all $a, b \in I, J$. In particular $0 \in I \cap J$ which means $I \cap J \neq \emptyset$. (2 points)

Let $a, b \in I \cap J$. Then $a, b \in I, J$ so $a - b \in I, J$.

Therefore $a - b \in I \cap J$. (4 points) We have shown that $I \cap J$ is an additive subgroup of R . Let $r \in R$ and $a \in I \cap J$. Then $a \in I, J$. since I, J are ideals of R it follows

that $ra, ar \in I, J$. Therefore $ra, ar \in I \cap J$. (4 points)

- c) Let $R = \mathbf{R}[x]$, $I = \langle (x+1)(x-3) \rangle$, and $J = \langle (x-3)(x+5) \rangle$. Find an $f(x) \in \mathbf{R}[x]$ such that $I \cap J = \langle f(x) \rangle$. Justify your choice. [Hint: Recall that if $a_1, \dots, a_r \in \mathbf{R}$ are distinct roots of $f(x) \in \mathbf{R}[x]$ then $(x - a_1) \cdots (x - a_r)$ divides $f(x)$.]

Solution: Generally for $g(x) \in \mathbf{R}[x]$ the elements of $\langle g(x) \rangle$ are the multiples of $g(x)$. By the hint $I = \langle (x+1)(x-3) \rangle$ consists of all polynomials of $\mathbf{R}[x]$ which roots $-1, 3$ and as roots $J = \langle (x-3)(x+5) \rangle$ consists of all polynomials of $\mathbf{R}[x]$ which roots $3, -5$ and as roots. Therefore $I \cap J$ consists of all polynomials which have roots $-1, 3$ and $3, -5$, or roots $-1, 3, -5$.

By the hint again, and reasons cited, $I \cap J = \langle (x+1)(x-3)(x+5) \rangle$. (8 points)