

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 75.

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 $|G| = 75 = 3 \cdot 5^2$. Since there are 6 divisors of 75; hence G has 6 subgroups. **(5 points)**

b) For each subgroup of G list its size and *one* generator in the form a^ℓ , where $0 \leq \ell < 75$.

Solution: If d is a positive divisor of $n = 75$ then $|\langle a^d \rangle| = n/d$ and therefore $|\langle a^{n/d} \rangle| = d$.

size	a generator
1	$a^{75} = a^0 = e$
3	a^{25}
5	a^{15}
15	a^5
25	a^3
75	$a^1 = a$

(6 points).

c) List *all* generators of the subgroup of G of order 15 in the form a^ℓ , where $0 \leq \ell < 75$.

Solution: The integers $1 \leq k \leq 15$ which are relatively prime to 15 are: 1, 2, 4, 7, 8, 11, 13, 14. Thus the generators of the subgroup of order 15 of G are

$$(a^5)^1 = a^5, \quad (a^5)^2 = a^{10}, \quad (a^5)^4 = a^{20}, \quad (a^5)^7 = a^{35},$$

$$(a^5)^8 = a^{40}, \quad (a^5)^{11} = a^{55}, \quad (a^5)^{13} = a^{65}, \quad (a^5)^{14} = a^{70}. \quad \text{(7 points)}$$

d) Find a divisor d of 75 such that $\langle a^{-400} \rangle = \langle a^d \rangle$ and list the distinct elements of $\langle a^{-400} \rangle$ as a^ℓ , where $0 \leq \ell < 75$.

Solution: The greatest common divisor of -400 and 75 is 25. Therefore we may take

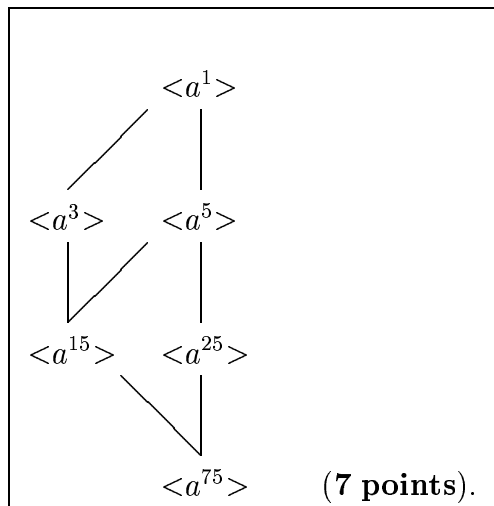
$d = 25$ **(2 points)** and thus

$$\langle a^{-400} \rangle = \langle a^{25} \rangle = \{e, a^{25}, a^{50}\}. \quad \text{(3 points)}$$

Note: $d = -25$ works just as well.

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

Solution: If d, d' are divisors of $n = 75$ then $\langle a^d \rangle \subseteq \langle a^{d'} \rangle$ if and only if d' divides d .



2. (20 pts.) Consider the permutation $f = (1\ 6\ 3\ 4)(2\ 5\ 7)(1\ 6\ 5)(5\ 6\ 10\ 9\ 8)$ of S_{10} .

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

Solution: $f = (1\ 3\ 4)(2\ 5\ 7)(6\ 10\ 9\ 8)$, or any rearrangement of these cycles. (5 points)

b) Write f as a product of transpositions.

Solution: Using our cyclic decomposition we have

$$f = (1\ 4)(1\ 3)(2\ 7)(2\ 5)(6\ 8)(6\ 9)(6\ 10) \quad (5 \text{ points})$$

for example, or $f = (3\ 4)(1\ 4)(5\ 7)(2\ 7)(9\ 8)(10\ 8)(6\ 8)$. One can go back and replace the cycles in the definition of f and write

$$f = (1\ 4)(1\ 3)(1\ 6)(2\ 7)(2\ 5)(1\ 5)(1\ 6)(5\ 8)(5\ 9)(5\ 10)(5\ 6)$$

or

$$f = (3\ 4)(6\ 4)(1\ 4)(5\ 7)(2\ 7)(6\ 5)(1\ 5)(9\ 8)(10\ 8)(6\ 8)(5\ 8)$$

as well.

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

Solution: Since f is the product of an odd number of 2-cycles it follows that f is *odd*.

Thus f is not 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, which are 3, 3, 4, and is therefore **12. (5 points)**

3. (25 pts.) Let $G = \langle a \rangle$ be a finite cyclic group and suppose that $f : G \rightarrow G'$ is a group homomorphism. [Hint: For parts a) and b) you may use the following: If G is any group and $g \in G$ has finite order, then $g^m = e$ if and only if $|g|$ divides m .]

a) Show that $f(a)$ has finite order and $|f(a)|$ divides $|a|$.

Solution: Let $n = |a|$. Then $e = a^n$; thus by definition of order and the hint

$e = f(e) = f(a^n) = f(a)^n$ implies that $f(a)$ has finite order and $|f(a)|$ divides n . **(3 points)**

b) Suppose that $b \in G'$ has finite order and $|b|$ divides $|a|$. Show that the rule $\phi : G \rightarrow G'$ given by $\phi(a^\ell) = b^\ell$ for all $\ell \in \mathbf{Z}$ is a *well-defined* group homomorphism. (Well-defined means that $a^\ell = a^{\ell'}$ implies $b^\ell = b^{\ell'}$.)

Solution: Suppose that $b \in G'$ has finite order and $|b|$ divides $|a|$. Define ϕ as above. Then ϕ is *well-defined*. For if $a^\ell = a^{\ell'}$ then $|a|$ divides $\ell - \ell'$. Since $|b|$ divides $|a|$ it follows that $|b|$ divides $\ell - \ell'$ as well. As a consequence $b^\ell = b^{\ell'}$. **(3 points)**

The fact that ϕ is a homomorphism follows by the calculation

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

for all integers k, m .

c) Suppose that $|G| = 60$ and $G' = \langle c \rangle$ is cyclic of order 175. Determine all group homomorphisms $\phi : G \rightarrow G'$.

Solution: By parts a) and b) it is a matter of finding $b \in G'$ such that $|b|$ divides 60. Then $\phi(a) = b$ determines a homomorphism $f : G \rightarrow G'$; thus $\phi(a^\ell) = b^\ell$ for all $\ell \in \mathbf{Z}$.

By Lagrange's Theorem $|b|$ divides 175. Thus $|b|$ divides 60, 175 which is the case if and only if $|b| = 1$ or 5. Thus

$$b = e, c^{35}, c^{70}, c^{135}, \text{ or } c^{140}. \quad \mathbf{(11 \text{ points})}$$

4. (25 pts.) Consider the subgroup $H = \langle (1\ 2\ 4) \rangle$ of A_4 .

a) What is the number of left cosets of H in A_4 ? In S_4 ?

Solution: $|H| = 3$. Thus H has $|S_4|/|H| = 24/3 =$ 8 left cosets in S_4 (3 points)
and $|A_4|/|H| = 12/3 =$ 4 left cosets in A_4 (3 points).

b) Write the elements of $(1\ 3)H$ as products of disjoint cycles.

Solution: Since $H = \{\text{Id}, (1\ 2\ 4), (1\ 2\ 4)^2 = (1\ 4\ 2)\}$ we have

$$(1\ 3)H = \{(1\ 3)\text{Id}, (1\ 3)(1\ 2\ 4), (1\ 3)(1\ 4\ 2)\}$$

$$= \{(1\ 3), (1\ 2\ 4\ 3), (1\ 4\ 2\ 3)\}. \quad \text{(12 points)}$$

c) Determine whether or not H is a normal subgroup of S_4 .

Solution: $(1\ 2\ 4)(1\ 3) = (1\ 3\ 2\ 4) \notin (1\ 3)H$. Therefore

H is not a normal subgroup of S_4 . (7 points)

5. (25 pts.) Consider the group $G = \mathbf{Z}_{16} \oplus \mathbf{Z}_6$.

a) Find all elements of G of order 6.

Solution: Let $(a, b) \in G$. Then the order of (a, b) is $\text{lcm}(|a|, |b|)$. Since $|a| = 1, 2, 4, 8,$ or 16 and $|b| = 1, 2, 3,$ or 6 , it follows that $\text{lcm}(|a|, |b|) = 6$ if and only if $|a| = 1$ and $|b| = 6$, or $|a| = 2$ and $|b| = 3, 6$. (3 points) The elements of order 6 are thus $(0, 1), (0, 5); (8, 2), (8, 4); (8, 1), (8, 5)$. (6 points)

b) Find a cyclic subgroup of G of order 12 and list its elements.

Solution: Since $4 \in \mathbf{Z}_{16}$ has order 4 and $2 \in \mathbf{Z}_6$ has order 3, by our comments in the solution of part a) we see that $(4, 2)$ is an element of G of order 12. Thus

$$\langle (4, 2) \rangle = \{(0, 0), (4, 2), (8, 4), (12, 0), (0, 2), (4, 4), (8, 0), (12, 2), (0, 4), (4, 0), (8, 2), (12, 4)\} \quad \text{(7 points)}$$

provides an example.

c) Find a non-cyclic subgroup of G of order 12.

Solution: $H = \langle 8 \rangle \oplus \langle 1 \rangle$ as $\langle 8 \rangle \subseteq \mathbf{Z}_{16}$ has order 2 and $\langle 1 \rangle \subseteq \mathbf{Z}_6$ has order 6, and thus $|H| = |\langle 8 \rangle| |\langle 1 \rangle| = 2 \cdot 6 = 12$. By our comments in the solution of part a) the order of any element of H divides 6. Therefore H is not cyclic. (5 points)

- d) Now regard $R = \mathbf{Z}_{16} \oplus \mathbf{Z}_6$ as a ring. Given that $U(R) = U(\mathbf{Z}_{16}) \oplus U(\mathbf{Z}_6)$, find the order of $U(R)$.

Solution: Generally the elements of $U(\mathbf{Z}_n)$ are the integers $1 \leq k \leq n$ which are relatively prime to n . Thus $|U(\mathbf{Z}_{16})| = |\{1, 3, 5, 7, 9, 11, 13, 15\}| = 8$ and $|U(\mathbf{Z}_6)| = |\{1, 5\}| = 2$. Therefore $|U(R)| = |U(\mathbf{Z}_{16}) \oplus U(\mathbf{Z}_6)| = |U(\mathbf{Z}_{16})| |U(\mathbf{Z}_6)| = 8 \cdot 2 =$
16 (4 points)

6. (25 pts.) Consider the subset $R = \{m + n\sqrt{5} \mid m, n \in \mathbf{Z}\}$ of the field of real numbers \mathbf{R} .
- a) Determine whether or not R is an additive subgroup of \mathbf{R} .

Solution: $0 = 0 + 0\sqrt{5} \in R$; thus $R \neq \emptyset$ (**2 points**). Suppose that $x, x' \in R$. Then $x = m + n\sqrt{5}$ and $x' = m' + n'\sqrt{5}$ for some $m, m', n, n' \in \mathbf{Z}$. Therefore

$$x - x' = (m + n\sqrt{5}) - (m' + n'\sqrt{5}) = (m - m') + (n - n')\sqrt{5} \in R.$$

We use the fact that \mathbf{Z} is an additive subgroup of \mathbf{R} . Thus R is an additive subgroup of \mathbf{R} . (**7 points**)

- b) Determine whether or not R is a subring of \mathbf{R} .

Solution: By part a) R is an additive subgroup of \mathbf{R} . Continuing with our notation from part a), the calculation

$$xx' = (m + n\sqrt{5})(m' + n'\sqrt{5}) = (mm' + 5nn') + (mn' + m'n)\sqrt{5} \in R$$

shows that R is a subring of \mathbf{R} . We use the fact that \mathbf{Z} is a commutative subring of \mathbf{R} for this calculation. (**8 points**)

- c) Determine whether or not R is a subfield of \mathbf{R} . [Hint: You may use the fact that $r + s\sqrt{5} = r' + s'\sqrt{5}$, where $r, r', s, s' \in \mathbf{Q}$, implies that $r = r'$ and $s = s'$. This follows from the fact that $\sqrt{5}$ is not rational.]

Solution: If R were a subfield of \mathbf{R} then $\sqrt{5}$ would have a multiplicative inverse in R . But

$$1 + 0\sqrt{5} = 1 = (m + n\sqrt{5})\sqrt{5} = 5n + m\sqrt{5}$$

implies that $5n = 1$ and $m = 0$ by the hint. Since 5 does not have a multiplicative inverse in \mathbf{Z} we conclude that $\sqrt{5}$ does not have a multiplicative inverse in R . Thus R is not a subfield of \mathbf{R} . (**8 points**)

7. (25 pts.) Let R be a ring. For non-empty subsets S_1, \dots, S_n of R define

$$S_1 + \dots + S_n = \{s_1 + \dots + s_n \mid s_i \in S_i \text{ for all } 1 \leq i \leq n\}.$$

- a) Define ideal of R .

Solution: An ideal of R is an additive subgroup I of R such that $ra, ar \in I$ for all $r \in R$ and $a \in I$. **(5 points)**

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

Solution: Since I, J are ideals of R they are additive subgroups of R . Therefore $I, J \neq \emptyset$. This means $I + J \neq \emptyset$. **(2 points)**

Now let $x, x' \in I + J$. Then $x = a + b$ and $x' = a' + b'$ where $a, a' \in I$ and $b, b' \in J$. Since I, J are additive subgroups of R , by the 1-Step subgroup Test $a - a' \in I$ and $a - b' \in J$. Therefore

$$x - x' = (a + b) - (a' + b') = (a - a') + (b - b') \in I + J.$$

We have used the associative and commutative axioms for addition implicitly in the preceding calculation. By the 1-Step Subgroup Test $I + J$ is an additive subgroup of R . **(4 points)**

Now suppose that $r \in R$. Since I and J are ideals of R the products $ra, ar \in I$ and $rb, br \in J$. Therefore $rx = r(a+b) = ra+rb \in I+J$ and $xr = (a+b)r = ar+br \in I+J$. This completes the proof that $I + J$ is an ideal of R . **(4 points)**

- c) Suppose that I_1, \dots, I_n are ideals of R . Show, by induction, that $I_1 + \dots + I_n$ is an ideal of R .

Solution: Suppose that $n = 1$, Then the sum is I_1 by convention. By assumption I_1 is an ideal of R . **(5 points)** Now suppose that $n \geq 2$. Then $I_1 + \dots + I_n = (I_1 + \dots + I_{n-1}) + I_n$. By our induction hypothesis $I_1 + \dots + I_{n-1}$ is an ideal of R . By part b) the sum of two ideals of R is an ideal of R . Therefore $I_1 + \dots + I_n$ is an ideal of R . **(5 points)**

8. (25 pts.) Let R be a ring with unity 1 and suppose that I is an ideal of R .

- a) Show that $1 \in I$ implies $I = R$.

Solution: Let $r \in R$. Since $1 \in I$, and I is an ideal of R , the product $r1 \in I$. Therefore $r = r1 \in I$ from which we conclude that $R \subseteq I$. Thus $I = R$ as $I \subseteq R$. **(10 points)**

- b) Now let $R = \mathbf{R}[x]$ and suppose that $x^3 - 6x - 1, x^2 + 3x + 1 \in I$. Show that $I = R$. [Hint: You might find the Division Algorithm useful in finding other elements in I].

Solution: Suppose that $f(x), g(x) \in I$ and $q(x), r(x) \in R$ satisfy $f(x) = q(x)g(x) + r(x)$. Since I is an ideal of R we conclude that $r(x) = f(x) + (-q(x))g(x) \in I$. **(5 points)**

By assumption $x^3 - 6x - 1, x^2 + 3x + 1 \in I$. By the Division Algorithm

$$x^3 - 6x - 1 = (x - 3)(x^2 + 3x + 1) + (2x + 2), \quad (\mathbf{5 \text{ points}})$$

from which we conclude that $2x + 2 \in I$. By the same we have

$$x^2 + 3x + 1 = \left(\frac{1}{2}x + 1\right)(2x + 2) + (-1)$$

from which we conclude that $-1 \in I$. Therefore $1 = -(-1) \in I$ since the latter is an additive subgroup of R . By part a) it follows that $I = R$. (**5 points**)