THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2023-24
Homework 1 Answer

Compulsory Part

1. A nontrivial abelian group A (written multiplicatively) is called **divisible** if for each element $a \in A$ and each nonzero integer k there is an element $x \in A$ such that $x^k = a$, i.e. each element has a k^{th} root in A.

   (a) Prove that the additive group of rational numbers, $\mathbb{Q}$, is divisible.

   (b) Prove that no finite abelian group is divisible.

   Proof. (a) For any $\frac{p}{q} \in \mathbb{Q}$ and $k \in \mathbb{Z}$, we have $k\frac{p}{kq} = \frac{p}{q}$. Thus it is divisible.

   (b) Let G be a finite divisible group of order m, then there is a non-trivial element g such that the order of g. Since G is divisible, there exists $f^m = g$. However $f^m = e$, this contradicts to our choice of g.

   $\square$

2. Let p be a prime and $\mathbb{F}_p$ the finite field with p elements. Compute the orders of the groups $\mathrm{GL}_n(\mathbb{F}_p)$ and $\mathrm{SL}_n(\mathbb{F}_p)$. (Important.)

   Answer. $|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)...(p^n - p^{n-1})$, and $|\mathrm{SL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)...(p^n - p^{n-1})/(p-1)$.

   The reason is that $\mathrm{GL}_n(\mathbb{F}_p) = \{M \mid M \in M_n(\mathbb{F}_p), \text{columns of } M \text{ are linearly independent}\}$. The first column has $p^n - 1$ choices. After choosing the first one, the second column has $p^n - p$ choices, and so on. The last column has $p^n - p^{n-1}$ choices.

   Note that $\det : \mathrm{GL}_n(\mathbb{F}_p) \to \mathbb{F}_p^\times$ is surjective, with kernel $\mathrm{SL}_n(\mathbb{F}_p)$. Therefore, $|\mathrm{SL}_n(\mathbb{F}_p)| = |\mathrm{GL}_n(\mathbb{F}_p)|/|\mathbb{F}_p^\times| = (p^n - 1)(p^n - p)...(p^n - p^{n-1})/(p-1)$.

3. Let G be a group of order pq, where p and q are primes. Show that every proper subgroup of G is cyclic.

   Proof. Let H be a proper subgroup of G, by Lagrange's theorem, it has order $1, p$ or q. If $|H| = 1$, then it is the trivial group, which is cyclic. If $|H| = p$ or q, since it has prime order, it is generated by any nonidentity element. So H is cyclic. $\square$

4. Let $H_1 \leq H_2 \leq H_3 \dots$ be an ascending chain of subgroups of a group G. Prove that the union $\cup_{i=1}^{\infty} H_i$ is a subgroup of G.

   Proof. Let $H = \cup_{i=1}^{\infty} H_i$. We prove that $H \leq G$.

   First, $e_G \in H_1 \subseteq H$. Second, take arbitrary $a, b \in H$. Then $a \in H_i$, $b \in H_j$ for some $i, j \geq 1$. Then $a, b \in H_{i+j}$. Therefore, $ab^{-1} \in H_{i+j} \subseteq H$.

   Therefore, $H \leq G$. $\square$

5. Let $H \leq K \leq G$. Show that $[G:H] = [G:K][K:H]$. (*Warning*: G, H and K may *not* be finite.)

   Proof. Note that $G = \bigsqcup_{i\in I} g_i K$, and $K = \bigsqcup_{j\in J} k_j H$ for some I, J, g_i, k_j (by axiom of choice). Then $G = \bigsqcup_{i\in I,\ j\in J} g_i k_j H$.
   Then $[G:H] = |I \times J| = |I||J| = [G:K][K:H]$. $\square$

6. Show that if H is a subgroup of index 2 in a group G, then $aH = Ha$ (as subsets in G) for all $a \in G$. (Warning: Again, G may not be finite.)

   Proof. Since $[G:H] = 2$, there are only two left cosets $\{H, aH\}$ and two right cosets $\{H, Ha\}$. Since cosets partition a group G, $aH \sqcup H = G = Ha \sqcup H$ and therefore $aH = G - H = Ha$. $\square$

7. Show that if a group G with identity e has finite order n, then $a^n = e$ for all $a \in G$.

   Proof. By Lagrange's theorem, the subgroup generated by an element a has order dividing $|G| = n$. The order of $\langle a \rangle$ is the same as $\operatorname{ord} a$. So $a^n = a^{k \operatorname{ord} a} = e$. $\square$

8. Show that any group homomorphism $\phi : G \to G'$, where $|G|$ is a prime number, must either be the trivial homomorphism or an injective map.

   Proof. Since $\ker \phi$ is a subgroup of G of prime order, $\ker \phi$ has order 1 or p. When it has order 1, it is injective. When it has order p, $\ker \phi = G$ and the map is trivial. $\square$

Optional Part

1. Recall that an element a of a group G with identity element e has **order** $r > 0$ if $a^r = e$ and no smaller positive power of a is the identity. Show that if G is a finite group with identity e and with an even number of elements, then there exists an order 2 element in G, i.e. there exists $a \neq e$ in G such that $a^2 = e$.

   Proof. Let $\sim$ be a relation on G defined by $g \sim h$ for $g, h \in G$ if and only if $g = h$ or $g = h^{-1}$. It is easy to verify that $\sim$ is an equivalence relation on G. Let $[g]$ be the equivalence class containing g for each $g \in G$. Then $|[g]| = \begin{cases} 1, & \text{if } \operatorname{ord}(g) = 1, 2, \\ 2, & \text{if } \operatorname{ord}(g) > 2. \end{cases}$.
   Since $|G|$ is even and $|G|$ is partitioned into equivalence classes by $\sim$, there must be an even number of equivalence classes that has size 1. Note that exactly one element $e \in G$ has order 1. Therefore there must be an element in G of order 2. $\square$

2. In Homework 1, we have seen that every finite group of even order contains an element of order 2. Using the Theorem of Lagrange, show that if n is odd, then an abelian group of order $2n$ contains precisely one element of order 2.

   Proof. Suppose there are two distinct elements a, b of order 2, then the subgroup generated by a, b is $\{e, a, b, ab\}$. It is a subgroup of order 4. But 4 does not divide $2n$ by assumption, so this would contradict Lagrange's theorem. $\square$

Remark. Can you find an nonabelian group of $2n$ elements containing more than 1 element of order 2?

3. Show that every group G with identity e and such that $x^2 = e$ for all $x \in G$ is abelian.

   Proof. Let $g, h \in G$ be arbitrary. Then $g^2 = h^2 = ghgh = 1$. Then $g^{-1}h^{-1}gh = ghgh = 1$. Therefore, $gh = hg$.

   Therefore, G is abelian. □

4. Prove that a cyclic group with *only one* generator can have at most 2 elements.

   Proof. Let G be a cyclic group with exactly one generator g. Then $G = \langle g \rangle$. Then $G = \langle g^{-1} \rangle$. Therefore, $g = g^{-1}$, and $\operatorname{ord}(g) = 1$ or 2. Then $|G| = \operatorname{ord}(g) = 1$ or 2. □

5. Show that a group with no proper nontrivial subgroups is cyclic.

   Proof. Let G be a group with no proper nontrivial subgroup. Let e denote the identity element in G.

   If $|G| = 1$. Then $G = \langle e \rangle$ is cyclic. If $|G| > 1$. Let $g \in G \backslash \{e\}$. Then $\langle g \rangle$ is a nontrivial subgroup of G, so it cannot be proper. Then $G = \langle g \rangle$, so G is cyclic. □

6. Show that a group which has only a finite number of subgroups must be a finite group.

   Proof. We prove the contrapositive. Suppose G is infinite.

   Case 1. Some $g \in G$ has infinite order. Then $\langle g^n \rangle$ are different subgroups of G for different $n \in \mathbb{Z}_{>0}$.

   Case 2. All $g \in G$ has finite order. Then $G = \bigcup\limits_{g \in G} \langle g \rangle$. But G is infinite, and each $\langle g \rangle$ is finite. Then there is an infinite number of distinct $\langle g \rangle$'s. Therefore, G has infinitely many subgroups.

   In either case, G has infinitely many subgroups. □

7. Let G be a group and suppose that an element $a \in G$ generates a cyclic subgroup of order 2 and is the *unique* such element. Show that $ax = xa$ for all $x \in G$. [*Hint:* Consider $(xax^{-1})^2$.]

   Proof. Note that a is the unique element in G of order 2. Let $x \in G$. Then $(xax^{-1})^2 = xa^2x^{-1} = xx^{-1} = e$. Also $xax^{-1} \neq e$ because otherwise $a = e$. Then $\operatorname{ord}(xax^{-1}) = 2$. Then $xax^{-1} = a$, and so $xa = ax$. □

8. Let n be an integer greater than or equal to 3. Show that the only element σ of S_n satisfying $\sigma g = g\sigma$ for all $g \in S_n$ is $\sigma = \iota$, the identity permutation. [*Hint:* First show that S_n is a nonabelian group for $n \geq 3$.]

Proof. Suppose $\sigma \in S_n$ satisfies $\sigma g = g\sigma$ for any $g \in S_n$.

Suppose σ is not the identity. Then $\sigma(i) \neq i$ for some $1 \leq i \leq n$. Let $j = \sigma(i)$. Since $n \geq 3$, we can find $1 \leq k \leq n$ distinct from i, j. Then $((j,k) \circ \sigma)(i) = k$, but $(\sigma \circ (j,k))(i)$. Therefore, $(j,k)\sigma \neq \sigma(j,k)$. Contradiction arises.

Therefore, $\sigma = \iota$, the identity permutation. □

9. Prove the following statements about S_n for $n \geq 3$:

   (a) Every permutation in S_n can be written as a product of at most $n-1$ transpositions.

   (b) Every permutation in S_n that is not a cycle can be written as a product of at most $n-2$ transpositions.

   (c) Every odd permutation in S_n can be written as a product of $2n+3$ transpositions, and every even permutation as a product of $2n+8$ transpositions.

Proof. (a) Note that a cycle $(x_1, x_2, ..., x_k)$ of length k can be written as a product of $k-1$ transpositions: $(x_1, x_2, ...x_k) = (x_1, x_2)(x_2, x_3)...(x_{k-1}, x_k)$. Also, a permutation in S_n can be written as a product of disjoint cycles. Let the lengths of the disjoint cycles be $l_1, l_2, ..., l_r$. Then $l_1 + ... + l_r \leq n$. Write each cycle as a product of transpositions. Then the number of transpositions used would be $l_1 - 1 + ... + l_r - 1 = l_1 + ... + l_r - r \leq n - r \leq n - 1$. (The identity permutation (1)=(1,2)(1,2). Better, it can be thought of as the product of 0 transpositions and thus, as a length 1 cycle, fall into the above discussion.)

(b) When $g \in S_n$ is not equal to any cycle, its cycle decomposition contain at least 2 cycles. Then $r \geq 2$ in (a). Thus the number of transpositions used is at most $n-2$.

(c) By (a), every odd permutation g is a product of $k \leq n \leq 2n+3$ transpositions, and k is odd because g is odd. Say $g = t_1...t_k$ is the product, where each t_i is a transposition. Then $g = t_1...t_k((1,2)(1,2))^{(2n+3-k)/2}$ is a product of $2n+3$ transposition. The case for even permutation is similiar.

□

10. Show that if $\sigma \in S_n$ is a cycle of odd length, then σ^2 is a cycle.

Proof. Let $\sigma = (x_1, ..., x_{2k-1})$ be a cycle of odd length, where $k \in \mathbb{Z}_{>0}$. Then $\sigma^2 = (x_1, x_3, x_5, ..., x_{2k-1}, x_2, x_4, ..., x_{2k-2})$ is a cycle. □

11. If n is odd and $n \geq 3$, show that the identity is the only element of D_n which commutes with all elements of D_n.

Proof. Recall that $D_n = \langle r, s \mid r^n = s^2 = rsrs = 1 \rangle = \{s^j r^i \mid 0 \leq i \leq n-1, j = 0, 1\}$.

Let $n \geq 3$. Suppose $g \in D_n$ commutes with all elements of D_n. Write $g = s^j r^i$, where $0 \leq i \leq n-1, j = 0, 1$. Then $s^j r^i s = s s^j r^i$. Then $r^i = s r^i s^{-1} = (srs^{-1})^i = (srs)^i = (r^{-1})^i = r^{-i}$. Therefore, $r^{2i} = 1$. But the order of r is n, so $n \mid 2i$. But n is odd, so $n \mid i$. Since $0 \leq i \leq n-1$, $i = 0$. Then $g = 1$ or s.

But the above discussion shows that s does not commute with $s^j r^i$ for $i \neq 0$. In particular s does not commute with r . Therefore, $g = 1$. □

12. Consider the group S_8.

    (a) What is the order of the cycle $(1, 4, 5, 7)$?

    (b) State a theorem suggested by part (a).

    (c) What is the order of $\sigma = (4, 5)(2, 3, 7)$? of $\tau = (1, 4)(3, 5, 7, 8)$?

    (d) Find the order of each of the permutations given in Exercises 2 below by looking at its decomposition into a product of disjoint cycles.

    (e) State a theorem suggested by parts (c) and (d). [*Hint:* The important words you are looking for are *least common multiple*.]

    Answer. (a) 4.

    (b) The order of a cycle is equal to its length.

    (c) The order of $\sigma = (4\ 5)(2\ 3\ 7)$ is 6. The order of $\tau = (1\ 4)(3\ 5\ 7\ 8)$ is 4.

    (d) The cycle decompositions of the permutations given in Exercises 10 through 12 are $(1\ 8)(3\ 6\ 4)(5\ 7), (1\ 3\ 4)(2\ 6)(5\ 8\ 7)$ and $(1\ 3\ 4\ 7\ 8\ 6\ 5\ 2)$ respectively, and their orders are $6, 6$ and 8 respectively.

    (e) The order of a permutation is equal to the least common multiple of the lengths of the cycles in its cycle decomposition.

13. Express the permutation of $\{1, 2, 3, 4, 5, 6, 7, 8\}$ as a product of disjoint cycles, and then as a product of transpositions:

    (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 \end{pmatrix}$

    (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 8 & 2 & 5 & 7 \end{pmatrix}$

    (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 7 & 2 & 5 & 8 & 6 \end{pmatrix}$

    Answer. (a) $(18)(364)(57) = (18)(36)(64)(57)$.

    (b) $(134)(26)(587) = (13)(34)(26)(58)(87)$.

    (c) $(13478652) = (13)(34)(47)(78)(86)(65)(52)$.

14. Find the maximum possible order for an element of S_6.

    Answer. The maximal order is $\text{lcm}(2, 3) = \text{lcm}(6) = 6$.

15. Find the maximum possible order for an element of S_{10}.

    Answer. The maximal order is $\text{lcm}(2, 3, 5) = 30$.

16. Complete the following with a condition involving n and r so that the resulting statement is a theorem:

    If σ is a cycle of length n, then σ^r is also a cycle of length n if and only if...

Answer. If σ is a cycle of length n, then σ^r is also a cycle of length n if and only if n and r are relatively prime.

Proof. We may assume that $\sigma = (1\ 2\ \cdots\ n)$.

($\Longleftarrow$) Suppose n and r are relatively prime. Then there are integers x and y such that $nx + ry = 1$. Hence, $(\sigma^r)^y = \sigma$ so that the list $\sigma^r(1), (\sigma^r)^2(1), (\sigma^r)^3(1), \ldots$ contains the same elements as what $\sigma(1), \sigma^2(1), \sigma^3(1), \ldots$ contains. They are $1, 2, 3, \ldots, n$. In other words, σ^r is a cycle of length n.

($\Longrightarrow$) Since σ^r is a cycle of length n, there is an integer y such that $(\sigma^r)^y(1) = \sigma(1)$. It follows that for any $i \in \{1, 2, \ldots, n\}$, $\sigma^{1-ry}(i) = \sigma^{1-ry}\sigma^{i-1}(1) = \sigma^{i-1}\sigma^{1-ry}(1) = \sigma^{i-1}(1) = i$. Hence $\sigma^{1-ry} = \mathrm{Id}$ and so $1 - ry$ is a multiple of n, which means that n and r are relatively prime.

A more constructive approach: Let $\overline{a}$ denote the only element in $(a + n\mathbb{Z}) \cap \{1, 2, ..., n\}$, the remainder of a divided by n in $\{1, 2, ..., n\}$. Then $\sigma^r(i) = \overline{i + r}$.

($\Longleftarrow$) Let r be relatively prime to n. Then $\times r : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a bijection. Then $\{\overline{r}, \overline{2r}, ..., \overline{nr}\} = \{1, 2, ..., n\}$. Then $(1, 2, ..., n)^r = (\overline{r}, \overline{2r}, ..., \overline{nr})$ is a cycle of length n.

($\Longrightarrow$) Suppose r is not relatively prime to n. Let $d = \gcd(r, n)$. Then $d > 1$, and $\gcd(r/d, n/d) = 1$. Then $\sigma^r = (\sigma^d)^{r/d} = ((1, d+1, ..., n-d+1)(2, d+2, ..., n-d+2)...(d, 2d, ..., n))^{r-d} = (1, d+1, ..., n-d+1)^{r/d}...(d, 2d, ..., n)^{r-d}$. Since each term is an r/d-th power of a cycle of length n/d and $\gcd(r/d, n/d) = 1$, by ($\Longleftarrow$), it is also a cycle of length n/d. These cycles $(i, d+i, ..., n-d+i)^{r/d}$ will again be disjoint for different i. Therefore, σ^r is the product of d-many disjoint cycles, each of length n/d.

Therefore σ^r is a cycle of length n if and only if $d = 1$. (The condition in blue is added in view of the case of $n \mid r$, where $\sigma^r = (1)$ is also a cycle.)

17. Show that S_n is generated by $\{(1, 2), (1, 2, 3, \ldots, n)\}$. (Important.)

    [*Hint:* Show that as r varies, $(1, 2, 3, \ldots, n)^r(1, 2)(1, 2, 3, \ldots, n)^{n-r}$ gives all the transpositions $(1, 2), (2, 3), (3, 4), \cdots, (n-1, n), (n, 1)$. Then show that any transposition is a product of some of these transpositions and use Corollary 9.12.]

    Proof. Let $G = \langle (1, 2), (1, 2, 3, ..., n) \rangle$ and we want to show that $G = S_n$.

    Note that $(1, 2, 3, \ldots, n)^r(1, 2)(1, 2, 3, \ldots, n)^{-r} = (r+1, r+2)$ for $0 \le r \le n-2$. Therefore, $\{(1, 2), (2, 3), (3, 4), \cdots, (n-1, n)\} \subseteq G$.

    Let $1 \le i < j \le n$. Fix i and we do induction on j to show that $(i, j) \in G$. If $j = i + 1$, then $(i, j) \in G$. If $(i, j) \in G$, then $(i, j+1) = (j, j+1)(i, j)(j, j+1) \in G$. By induction on j, $(i, j) \in G$ for all $i < j \le n$. Therefore, G contains all transpositions in S_n.

    By Compulsory Part 8(a), transpositions in S_n generate S_n. Therefore, $G = S_n$. □

18. Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

    Proof. If it is cyclic, suppose the generator is g, then there must exists $k \in \mathbb{Z}$ such that $g^k = (1, 0)$. Thus $g = (\frac{1}{k}, 0)$ cannot generate $(0, 1)$. □

19. Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic.

Answer. Consider the group $\{\frac{a}{2^n} | a, n \in \mathbb{Z}\}$ under addition, it is a subgroup of $\mathbb{Q}$. However for each r as a generator, $\frac{r}{2}$ cannot be expressed by r.

20. Let H and K be subgroups of a group G. Define a relation $\sim$ on G by $a \sim b$ if and only if $a = hbk$ for some $h \in H$ and some $k \in K$.

    (a) Prove that $\sim$ is an equivalence relation on G.

    (b) Describe the elements in the equivalence class containing $a \in G$. (These equivalence classes are called **double cosets**.)

    Proof. (a) The relation $\sim$ is reflexive because $a \sim a$ via $a = eae$ via $e \in H, K$.

    If $a \sim b$, assume $a = hbk$ for some h, k, then $b = h^{-1}ak^{-1}$, so $b \sim a$. Therefore $\sim$ is symmetric.

    If $a \sim b$ and $b \sim c$, then say $a = h_1bk_1$ and $b = h_2ck_2$, then $a = h_1h_2ck_2k_1$ for $h_1h_2 \in H$ and $k_2k_1 \in K$. Therefore $\sim$ is transitive.

    (b) The equivalence class containing $a \in G$ is given $[a] = \{hak \mid h \in H \text{ and } k \in K\}$.

    $\square$

21. Let H and K be subgroups of finite index in a group G, and suppose that $[G : H] = m$ and $[G : K] = n$. Prove that $\operatorname{lcm}(m, n) \leq [G : H \cap K] \leq mn$. Hence deduce that if m and n are relatively prime, then $[G : H \cap K] = [G : H][G : K]$.

    Proof. By result of question 4, since we have $H \cap K \leq H \leq G$ and $H \cap K \leq K \leq G$, the index $[G : H \cap K] = [G : H][H : H \cap K] = [G : K][K : H \cap K]$. Now m, n both divides $[G : H \cap K]$, therefore $\operatorname{lcm}(m, n)$ also divides $[G : H \cap K]$.

    Consider the set of left cosets $H/H \cap K$, for $h_1H \cap K \neq h_2H \cap K$, we have $h_1h_2^{-1} \notin H \cap K$. Since $h_1, h_2 \in H$ this implies that $h_1, h_2 \notin K$, so they define different left cosets of K: $h_1K \neq h_2K$. This shows that there are at least as many left cosets of K in G as left cosets of $H \cap K$ in H, i.e. $[H : H \cap K] \leq [G : K] = n$. So $[G : H \cap K] \leq mn$.

    When m and n are relatively prime, $\operatorname{lcm}(m, n) = mn$. Then $[G : H \cap K] = mn = [G : H][G : K]$. $\square$

22. Let $\phi : G \to G'$ be a homomorphism with kernel H and let $a \in G$. Prove the set equality $\{x \in G : \phi(x) = \phi(a)\} = Ha$.

    Proof. Let $x \in G$,

$$\begin{aligned}
\phi(x) = \phi(a) &\iff \phi(xa^{-1}) = 0 \\
&\iff xa^{-1} \in \ker \phi = H \\
&\iff Hxa^{-1} = H \\
&\iff Hx = Ha \\
&\iff x \in Ha
\end{aligned}$$

$\square$

23. Show that a nontrivial group which has no proper nontrivial subgroups must be finite and of prime order.

    Proof. Let G be a nontrivial group which has no proper nontrivial subgroups. Let $g \in G - \{e\}$ be arbitrary. Then $\langle g \rangle = G$ by assumption. Then G is cyclic. If $G \simeq \mathbb{Z}$, then $2\mathbb{Z}$ is a proper nontrivial subgroup. Then $G \simeq \mathbb{Z}_n$ for some $n \geq 2$. If n is not a prime, let $1 < d < n$ be a divisor of n, then $\langle d \rangle$ is a proper nontrivial subgroup. Therefore, $G \simeq \mathbb{Z}_p$ for some prime p, thus being finite of prime order. □

24. If A and B are groups, then their Cartesian product $A \times B$ is a group (called the **direct product** of A and B) using the componentwise defined operation. Is any subgroup of $A \times B$ of the form $C \times D$ where $C < A$ and $D < B$? Justify your assertion.

    Proof. Consider $\mathbb{Z} \times \mathbb{Z}$, then $(1,1)$ generates a subgroup that is not a product of two subgroups. This is because there are projection maps $C \times D \to C$ and $C \times D \to D$. So if $\langle (1,1) \rangle$ is a product, then $1 \in C$ and $1 \in D$. So $C \times D = \mathbb{Z} \times \mathbb{Z}$ but $\langle (1,1) \rangle \neq \mathbb{Z} \times \mathbb{Z}$. □

25. Prove, carefully and rigorously, that a finite cyclic group of order n has exactly one subgroup of each order d dividing n.

    Proof. Clearly there is a subgroup of order d in $\mathbb{Z}_n$ if we let an order d element generate a subgroup. This subgroup has $\phi(d)$ many generators by argument above, these are precisely all those elements of order d. Since every subgroup of cyclic group is cyclic, if there was another subgroup of order d, then there must be more than $\phi(d)$ many order d element, which is a contradiction. □

26. The **sign of an even permutation** is $+1$ and the **sign of an odd permutation** is -1. Observe that the map $\mathrm{sgn}_n : S_n \to \{1, -1\}$ defined by

    $$\mathrm{sgn}_n(\sigma) = \text{sign of } \sigma$$

    is a homomorphism of S_n onto the multiplicative group $\{1, -1\}$. What is the kernel?

    Answer. The kernel is A_n, the set of even permutations.

27. Let $\phi : G_1 \to G_2$ be a group homomorphism. Show that ϕ induces an order preserving one-to-one correspondence between the set of all subgroups of G_1 that contain $\ker \phi$ and the set of all subgroups of G_2 that are contained in $\mathrm{im}\, \phi$. (Very Important.)

    Proof. Let $S_1 = \{H \mid \ker(\phi) \leq H \leq G_1\}$, and let $S_2 = \{H' \mid H' \leq \mathrm{im}(\phi) \leq G_2\}$. We define a bijection between S_1 and S_2.

    For $H \leq H_1$, $\phi(H) \leq \mathrm{im}(\phi)$. For $H' \leq \mathrm{im}(\phi), \ker(\phi) \leq \phi^{-1}(H') \leq G_1$. Then we can define $\alpha : S_1 \to S_2$ by $\alpha(H) = \phi(H)$, and define $\beta : S_2 \to S_1$ by $\beta(H') = \phi^{-1}(H')$. We show that α and β are inverse functions of each other.

    Let $H \in S_1$, then $\beta \circ \alpha(H) = \phi^{-1} \circ \phi(H) = \{g \in G_1 \mid \phi(g) \in \phi(H)\} = H \ker(\phi) = H$ because $H \supseteq \ker(\phi)$. Let $H' \in S_2$, then $\alpha \circ \beta(H') = \phi \circ \phi^{-1}(H') = H' \cap \mathrm{im}(\phi) = H'$. Therefore $\alpha \circ \beta = \beta \circ \alpha = id$.

    Thus, we get a one-to-one correspondence induced by ϕ as required. □

28. Let G be a group, let $h, k \in G$ and let $\phi : \mathbb{Z} \times \mathbb{Z} \to G$ be defined by $\phi(m, n) = h^m k^n$. Give a necessary and sufficient condition, involving h and k, for ϕ to be a homomorphism. Prove your assertion.

    Answer. ϕ is a homomorphism if and only if $hk = kh$.

    Proof. ($\Rightarrow$) If ϕ is a homomorphism, then $hk = \phi(1,0)\phi(0,1) = \phi(1,1) = \phi(0,1)\phi(1,0) = kh$.
    ($\Leftarrow$) If $hk = kh$, then $\phi(m,n)\phi(p,q) = h^m k^n h^p k^q = h^{m+p} k^{n+q} = \phi(m+p, n+q)$. $\square$

29. Find a necessary and sufficient condition on G such that the map ϕ described in the preceding exercise is a homomorphism for all choices of $h, k \in G$.

    Answer. ϕ is a homomorphism for all h, k if and only if $hk = kh$ for all h, k, i.e. G is abelian.

30. Let G be a group, h be an element of G, and n be a positive integer. Let $\phi : \mathbb{Z}_n \to G$ be defined by $\phi(i) = h^i$ for $0 \leq i < n$. Give a necessary and sufficient condition (in terms of h and n) for ϕ to be a homomorphism. Prove your assertion.

    Answer. ϕ is a homomorphism if and only if $h^n = e$.

    Proof. ($\Rightarrow$) If ϕ is an homomorphism, then $\phi(n-1)\phi(1) = h^{n-1}h = \phi(0) = e$.
    ($\Leftarrow$) If $h^n = e$, then for $i + j < n$, $\phi(i+j) = h^{i+j} = h^i h^j = \phi(i)\phi(j)$. And if $i + j \geq n$, then $\phi(i+j) = \phi(i+j-n) = h^{i+j-n} = h^{i+j} = \phi(i)\phi(j)$. $\square$