

Solutions to Homework 4

Problem 1. Let G be a group and a, b elements of G which commute, i.e. $ab = ba$. Suppose that a has order k and b has order l . We proved in class that:

1. the order of a^m is equal to $k/\gcd(k, m)$ for any integer m .
2. the order of ab divides $kl/\gcd(k, l)$ and $kl/\gcd(k, l)^2$ divides the order of ab . In particular, if k, l are relatively prime then ab has order kl .

- a) Prove that if d is a positive divisor of k then G has an element of order d .
- b) Prove that G has an element of order $\text{lcm}(k, l) = kl/\gcd(k, l)$ (warning: it does not have to be ab).
- c) Suppose that G is abelian and N is the smallest positive integer such that $g^N = e$ for every $g \in G$. Prove that G has an element of order N . Show a finite non-abelian group for which this is false.
- d) Let $f : G \rightarrow H$ be a homomorphism. Let $a \in G$ be an element of finite order k . Prove that $f(a)$ has also finite order, say m , and m divides k . Prove furthermore that a^n is in the kernel of f if and only if m divides n .

Solution. a) Consider $u = a^{k/d}$. Using the result 1. above we see that the order of u is equal to

$$\text{order of } u = \frac{k}{\gcd(k, k/d)} = \frac{k}{k/d} = d.$$

b) We start by working out a special case. Suppose that a has order $k = 24$ and b has order $l = 900$. We have $24 = 2^3 \cdot 3$, $900 = 2^2 \cdot 3^2 \cdot 5^2$, and $\text{lcm}(24, 900) = 2^3 \cdot 3^2 \cdot 5^2$. Using our solution to part a), $c_1 = a^3$ has order $2^3 = 8$, $c_2 = b^{100}$ has order 9, and $c_3 = b^{36}$ has order $5^2 = 25$. Since a and b commute, the elements c_1, c_2, c_3 commute with each other and have pairwise relatively prime orders. Using 2. we see that $c_1 c_2$ has order $8 \cdot 9$, and then again by 2., $(c_1 c_2) c_3$ has order $(8 \cdot 9) \cdot 25 = \text{lcm}(24, 900)$.

The general case follows the same idea. Write $\text{lcm}(k, l) = p_1^{e_1} \dots p_n^{e_n}$, where $p_1 < p_2 < \dots < p_n$ are prime numbers. Then for each $i = 1, 2, \dots, n$ we have $p_i^{e_i} | k$ or $p_i^{e_i} | l$. Let $c_i = a^{k/p_i^{e_i}}$ if $p_i^{e_i} \nmid l$ and $c_i = b^{l/p_i^{e_i}}$ otherwise. Then c_i has order $p_i^{e_i}$ and the elements $c_1, \dots, c_n$ commute with each other. Using 2. and a straightforward induction we see that $c_1 \dots c_t$ has order $p_1^{e_1} \dots p_t^{e_t}$ for $t = 1, \dots, n$. Thus $c_1 \dots c_n$ has order $p_1^{e_1} \dots p_n^{e_n} = \text{lcm}(k, l)$.

c) Let K be the largest possible order of elements in G and let $a \in G$ be of order K . Since $a^N = e$, we have $K | N$. We will show that $K = N$. Suppose to the contrary that $K < N$. Then there is an element $b \in G$ such that $b^K \neq e$. Thus the order L of b does not divide K , so $\text{lcm}(K, L) > K$. Since G is abelian, a and b commute and part b) tells us that G has an element of order $\text{lcm}(K, L)$, which is bigger than K . This clearly contradicts the definition of K . Thus we must have $K = N$.

Consider now the non-abelian group $S_3 = \{I, T, T^2, S, ST, ST^2\}$. Since T has order 3 and S has order 2, we have $3 | N$ and $2 | N$, so $6 | N$. On the other hand $a^6 = e$ for any $a \in S_3$, so $N = 6$. Clearly S_3 has no element of order 6: I has order 1, T, T^2 have order 3 and S, ST, ST^2 have order 2.

d) Since $a^k = e$, we see that $e = f(a^k) = f(a)^k$. This means that $f(a)$ has finite order m and m divides k .

Note that a^n is in the kernel of f if and only if $e = f(a^n) = f(a)^n$. On the other hand $f(a)^n = e$ if and only if m divides n , which completes the proof.

Problem 2. a) Let G be a group. For any element $g \in G$, let $c_g : G \rightarrow G$ be the conjugation by g map defined by $c_g(x) = gxg^{-1}$. Show that c_g is an automorphism of G . (It is called the **inner automorphism** induced by the element g or **the conjugation by g** automorphism.)

b) Show that the set $\{c_g : g \in G\}$ is a subgroup of $\text{Aut}G$. (This subgroup is called the **inner automorphism group** of G , denoted $\text{Inn}G$.)

c) Show that the map $g \mapsto c_g$ is a homomorphism from G to $\text{Aut}G$, whose image is the inner automorphism group $\text{Inn}G$ and whose kernel is the center $Z(G)$.

Solution: a) Since

$$c_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = c_g(x)c_g(y),$$

we see that c_g is a homomorphism. Note that $c_{g^{-1}}c_g$ and $c_gc_{g^{-1}}$ are both equal to the identity:

$$(c_gc_{g^{-1}})(x) = c_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = x$$

and similarly for $c_{g^{-1}}c_g$. Thus c_g is a bijection, hence an automorphism of G .

b) This will follow from c) since the image of a homomorphism is a subgroup (you can verify it directly though).

c) Note that

$$c_{ab}(x) = (ab)x(ab)^{-1} = abxb^{-1}a^{-1} = a(bxb^{-1})a^{-1} = c_a(c_b(x)) = (c_ac_b)(x).$$

Thus $c_{ab} = c_ac_b$ so our map is a homomorphism. Its image is $\text{Inn}G$ by the very definition of $\text{Inn}G$. The kernel of this homomorphism is

$$\begin{aligned} \{a \in G : c_a \text{ is the identity}\} &= \{a \in G : c_a(x) = x \text{ for all } x \in G\} = \\ &= \{a \in G : axa^{-1} = x \text{ for all } x \in G\} = Z(G). \end{aligned}$$

Problem 3. Let G and H be groups.

a) Prove that the maps $\pi_G : G \times H \rightarrow G$ and $\pi_H : G \times H \rightarrow H$ defined by $\pi_G(g, h) = g$ and $\pi_H(g, h) = h$ are homomorphisms. What are the kernels of these maps?

b) Suppose that $G = H$ and let $\Delta = \{(a, b) \in G \times G : a = b\}$. Prove that Δ is a subgroup of $G \times G$ which is isomorphic to G .

c) Let $f_1 : Q \rightarrow G$ and $f_2 : Q \rightarrow H$ be homomorphisms. Define $f : Q \rightarrow G \times H$ by $f(a) = (f_1(a), f_2(a))$. Prove that f is a homomorphism and that $\ker f = \ker f_1 \cap \ker f_2$.

Solution. a) We have

$$\pi_G((g, h)(a, b)) = \pi_G(ga, hb) = ga = \pi_G(g, h)\pi_G(a, b).$$

This shows that π_G is a homomorphism and same argument works for π_H . The kernel of π_G is the set of all pairs (g, h) such that $g = e$, so it is $\{e\} \times H$ (which is naturally isomorphic to H). Similarly, the kernel of π_H is $G \times \{e\}$.

b) Consider the map $f : G \longrightarrow G \times G$ defined by $f(g) = (g, g)$. Clearly Δ is the image of f . Note now that f is a homomorphism:

$$f(gh) = (gh, gh) = (g, g)(h, h) = f(g)f(h).$$

Since the image of a homomorphism is a subgroup, Δ is a subgroup. (Alternatively, you can just check directly that Δ is a subgroup). Since the kernel of f is trivial, we see that f gives an isomorphism between G and Δ .

c) We have

$$f(ab) = (f_1(ab), f_2(ab)) = (f_1(a)f_1(b), f_2(a)f_2(b)) = (f_1(a), f_2(a))(f_1(b), f_2(b)) = f(a)f(b)$$

so f is a homomorphism. Note that $f(a) = e$ iff $f_1(a) = e$ and $f_2(a) = e$. This means that $\ker f = \ker f_1 \cap \ker f_2$.

Problem 4. Consider the dihedral group $D_n = \{I, T, \dots, T^{n-1}, S, ST, \dots, ST^{n-1}\}$ of order $2n$. Let $f : D_n \longrightarrow A$ be a homomorphism, where A is an abelian group.

a) Prove that $T^2 \in \ker f$.

b) Prove that if n is odd then the image of f has either one or two elements. Give example of a homomorphism f with image of order 2.

c) Let n be even. Define a map $g : D_n \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$g(S^a T^b) = (a \bmod 2, b \bmod 2).$$

Prove that g is a surjective homomorphism and find its kernel.

d) Prove that if n is even then the image of f is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_2$ or the trivial group.

Solution: a) Recall that $TS = ST^{-1}$. Since f is a homomorphism and A is abelian, we have $f(TS) = f(T)f(S) = f(S)f(T)$ and $f(ST^{-1}) = f(S)f(T)^{-1}$. Thus $f(S)f(T) = f(S)f(T)^{-1}$ and consequently $f(T) = f(T)^{-1}$. This means that $f(T)^2 = e$, i.e. $f(T^2) = e$. Thus $T^2 \in \ker f$.

b) Suppose that $n = 2k - 1$ is odd. Then $T = TT^{2k-1} = T^{2k} = (T^2)^k \in \ker f$ by part a). Thus, $\ker f$ contains the subgroup $\langle T \rangle = \{I, T, T^2, \dots, T^{n-1}\}$. It follows that $f(T^i) = e$ and $f(ST^i) = f(S)$ for every i . Thus the image of f is equal to $\{e, f(S)\}$. If $f(S) = e$, the image has one element and if $f(S) \neq e$ the image has 2 elements.

To have a homomorphism with image consisting of 2 elements we can use several approaches. Recall that D_n can be considered as a subgroup of the group of 2×2 orthogonal matrices (i.e. isometries of $\mathbb{R}^2$). T is the rotation by $2\pi/n$ clockwise and S is the reflexion in the x -axis. Then the determinant gives a homomorphism from D_n to $\{1, -1\}$ and T is sent to 1 and S to -1 . Equivalently, one can consider D_n as a subgroup of permutations of the vertices of a regular n -gon. Then the sign of a permutation gives a homomorphism from D_n to $\{1, -1\}$, which coincides with the determinant above. Explicitly, this homomorphism can be described by the following formula

$$f(S^a T^b) = (-1)^a.$$

It is not hard to check directly, that f is indeed a homomorphism.

c) Note for integers a, b, a_1, b_1 we have $S^a T^b = S^{a_1} T^{b_1}$ if and only if $a \equiv a_1 \pmod{2}$ and $b \equiv b_1 \pmod{n}$. Since n is even, this implies that $b \equiv b_1 \pmod{2}$. Thus g is well defined. Recall that $(S^a T^b)(S^m T^k) = S^{a+m} T^{k+(-1)^m b}$. Since $k + (-1)^m b \equiv k + b \pmod{2}$ we see that

$$\begin{aligned} g((S^a T^b)(S^m T^k)) &= ((a+m) \pmod{2}, (k + (-1)^m b) \pmod{2}) = \\ ((a+m) \pmod{2}, (k+b) \pmod{2}) &= (a \pmod{2}, b \pmod{2}) + (m \pmod{2}, k \pmod{2}) = \\ &= g(S^a T^b)g(S^m T^k). \end{aligned}$$

This shows that g is a homomorphism. The kernel of g consists of $S^a T^b$ such that a and b are even, so $\ker g = \langle T^2 \rangle$. Now $g(S) = (1 + 2\mathbb{Z}, 0 + 2\mathbb{Z})$, $g(T) = (0 + 2\mathbb{Z}, 1 + 2\mathbb{Z})$, $g(ST) = (1 + 2\mathbb{Z}, 1 + 2\mathbb{Z})$, so g is surjective.

d) By a), we have $\langle T^2 \rangle \subseteq \ker f$. Thus the image of f is equal to the set $\{e = f(I), f(T), f(S), f(S)f(T)\}$. Let $g = f(T)$, $h = f(S)$. Then $g^2 = h^2 = e$ and $gh = hg$. If $g = h = e$ then the image is the trivial group. If g, h, gh are non-trivial and pairwise distinct then the image is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. In all other cases the image has 2 elements and therefore it is isomorphic to $\mathbb{Z}_2$.

Problem 5. a) Prove that the exponential function $f(x) = e^x$ is an isomorphism from the group of all real numbers with addition to the group of positive real numbers with multiplication.

b) Prove that the group all rational numbers with addition is not isomorphic to the group of positive rational numbers with multiplication.

c) Prove that the group $\mathbb{R}^\times$ of all non-zero real numbers with multiplication is not isomorphic to the group $\mathbb{R}_+^\times$ of all positive real numbers with multiplication. Prove that $\mathbb{R}^\times$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{R}_+^\times$.

d) Prove that every finitely generated subgroup of the group $\mathbb{Q}$ of rational numbers with addition is cyclic but $\mathbb{Q}$ is not cyclic.

Solution. a) Since $f(x+y) = e^{x+y} = e^x e^y = f(x)f(y)$, we see that f is a homomorphism. Since the exponential is a bijection from real numbers to positive real numbers, it is an isomorphism.

b) Let $\mathbb{Q}$ be the group of rational numbers with addition and let $\mathbb{Q}_+^\times$ denote the group of positive rational numbers with multiplication. Suppose that we have an isomorphism $f : \mathbb{Q} \rightarrow \mathbb{Q}_+^\times$. Then there is $a \in \mathbb{Q}$ such that $f(a) = 2$. Let $b = a/2$. Then $a = b + b$ so $2 = f(a) = f(b+b) = f(b)f(b) = f(b)^2$. However this means that $f(b) = \sqrt{2}$ and we know that $\sqrt{2}$ is not a rational number. This proves that f can not exist.

c) Suppose that $f : \mathbb{R}^\times \rightarrow \mathbb{R}_+^\times$ is an homomorphism. Then $f(-1)$ is a positive real number and $1 = f(1) = f((-1)(-1)) = f(-1)f(-1) = f(-1)^2$. This means that $f(-1) = 1 = f(1)$ and therefore f is not injective. This shows that f cannot be an isomorphism.

For the second part, we will think of $\mathbb{Z}_2$ as $\{-1, 1\}$ with multiplication as the group operation. Then the map $\text{sign} : \mathbb{R}^\times \rightarrow \mathbb{Z}_2$ defined by $\text{sign}(a) = a/|a|$ is a homomorphism and the absolute value $|\cdot| : \mathbb{R}^\times \rightarrow \mathbb{R}_+^\times$ is also a homomorphism. Using problem 3 c) we get a homomorphism $f : \mathbb{R}^\times \rightarrow \mathbb{Z}_2 \times \mathbb{R}_+^\times$ defined by $f(a) = (\text{sign}(a), |a|)$. The kernel of

f is trivial: if $f(a) = (1, 1)$ then $a/|a| = 1 = |a|$, so $a = 1$. Thus f is injective. We have $(1, a) = f(a)$ and $(-1, a) = f(-a)$, so f is surjective. Thus f is an isomorphism.

d) Let S be a subgroup of $\mathbb{Q}$ generated by the rational numbers $a_1/b_1, \dots, a_n/b_n$. Let $N = b_1 b_2 \dots b_n$, $N_i = N/b_i$ and $a = 1/N$. Then $a_i/b_i = (a_i N_i)a$. Since $a_i N_i$ are integers, each a_i/b_i belongs to the cyclic subgroup $\langle a \rangle$ generated by a . Thus S is a subgroup of $\langle a \rangle$. We proved in class that a subgroup of a cyclic group is cyclic, so S is cyclic.

The group $\mathbb{Q}$ is not cyclic. Indeed, if $a \neq 0$ is a rational number then $a/2$ is also a rational number and $a/2 \notin \langle a \rangle$, so no cyclic subgroup of $\mathbb{Q}$ can contain all rational numbers.

Problem 6. Problem H to chapter 9.

Solution. 1) Consider the function $f : G \times H \longrightarrow H \times G$ defined by $f(g, h) = (h, g)$. Clearly f is a bijection. Checking that f is a homomorphism is straightforward.

2) If $\phi : G_1 \longrightarrow G_2$ and $\psi : H_1 \longrightarrow H_2$ are isomorphisms then the function $\eta : G_1 \times H_1 \longrightarrow G_2 \times H_2$ given by $\eta(g, h) = (\phi(g), \psi(h))$ is also an isomorphism. The verification of this claim is straightforward and left to the reader.

3) Suppose that G is abelian. Then

$$f(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a)f(b)$$

so f is a homomorphism. Since f is a bijection (an involution in fact), f is an automorphism.

Conversely, suppose that f is a homomorphism. Then for any $a, b \in G$ we have

$$ba = (a^{-1}b^{-1})^{-1} = f(a^{-1}b^{-1}) = f(a^{-1})f(b^{-1}) = ab.$$

Thus G is commutative.

For parts 4. and 5. we can use Problem 2a) from homework 2. Note that in the notation of that problem the function f is an isomorphism from the group A with operation $*$ onto the group G .

4) Taking $f : H \longrightarrow G$, $f(x) = x^{-1}$ we see that $x * y = f^{-1}(f(x)f(y)) = (x^{-1}y^{-1})^{-1} = yx$. Thus f is an isomorphism from H to G .

5) Taking $F : H \longrightarrow G$, $F(x) = cx$ we see that $F^{-1}(g) = c^{-1}g = f(g)$. Thus

$$x * y = F^{-1}(F(x)F(y)) = c^{-1}((cx)(cy)) = xcy.$$

Thus F is an isomorphism from the group H to G and f is the inverse isomorphism.

Problem 7. Problem E to chapter 11.

Solution. 1) The element g generates a group G if and only if every element of G is a power of g . Since (a, b) generates $G \times H$, for every $g \in G$ and every $h \in H$ there is an integer m such that $(a, b)^m = (g, h)$. This means that $a^m = g$ and $b^m = h$. Thus every element in G is a power of a and every element in H is a power of b .

2) This is an immediate consequence of 1): $G \times H$ cyclic means that there is $(a, b) \in G \times H$ which generates $G \times H$, so a generates G and b generates H , i.e. G and H are both cyclic.

3) Take $G = H = \mathbb{Z}_2$ (cyclic group of order 2). Then every element of $G \times H$ has order 1 or 2 and $G \times H$ has order 4. Thus $G \times H$ is not cyclic (a cyclic group of order n has an element of order n).

4) Note that $(a, b)^N = (a^N, b^N) = (e, e)$ if and only if $a^N = e = b^N$ which is equivalent to the condition that $m|N$ and $n|N$, which is equivalent to $\text{lcm}(m, n)|N$. This means that $\text{lcm}(m, n)$ is the order of (a, b) .

5) This is straightforward: if m and n are relatively prime then $\text{lcm}(m, n) = mn$.

6) Again, this is a straightforward consequence of 4: if m and n are not relatively prime then $\text{lcm}(m, n) < mn$.

7) Let m be the order of a and n the order of b . Then the group $\langle a \rangle \times \langle b \rangle$ has mn elements. If m and n are relatively prime, then (a, b) has order mn so the cyclic subgroup $\langle (a, b) \rangle$ of $\langle a \rangle \times \langle b \rangle$ has mn elements. Thus $\langle (a, b) \rangle = \langle a \rangle \times \langle b \rangle$, hence $\langle a \rangle \times \langle b \rangle$ is cyclic.

Problem 8. Problem G to chapter 14.

Solution. $f : G \longrightarrow H$ is a surjective homomorphism.

1) Suppose that G is abelian. If $u, w \in H$ then $u = f(a)$, $w = f(b)$ for some $a, b \in G$ (since f is surjective). Thus

$$uw = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = wu.$$

This proves that H is abelian.

2) Suppose that G is cyclic generated by g . Then every element in G is a power of g . Let $h = f(g)$. Take any $u \in H$. Then $u = f(a)$ for some $a \in G$. We have $a = g^m$ for some integer m , so

$$u = f(a) = f(g^m) = f(g)^m = h^m.$$

We showed that every element of H is a power of h , thus H is a cyclic group generated by h .

3) Suppose that every element in G has finite order. Take any element $u \in H$. Then $u = f(a)$ for some $a \in G$. Since a has finite order, we have $a^n = e$ for some integer $n > 0$. Then

$$u^n = (f(a))^n = f(a^n) = f(e) = e$$

so u has finite order.

4) Suppose that every element in G is its own inverse. Take any element $u \in H$. Then $u = f(a)$ for some $a \in G$. Since $a = a^{-1}$ we have

$$u = f(a) = f(a^{-1}) = f(a)^{-1} = u^{-1}.$$

5) Suppose that every element in G has a square root. Take any element $u \in H$. Then $u = f(a)$ for some $a \in G$. There is $b \in G$ such that $b^2 = a$. Let $w = f(b)$. Then

$$w^2 = f(b)^2 = f(b^2) = f(a) = u.$$

Thus every element in H has a square root.

6) Suppose that G is finitely generated and let $S = \{a_1, \dots, a_n\}$ be a finite set which generates G . Let $T = \{f(a_1), \dots, f(a_n)\}$. We will show that T generates H . Let $u \in H$. Then $u = f(a)$ for some $a \in G$. Since S generates G , we can find an expression

$$a = s_1 s_2 \dots s_k$$

for some $k \geq 1$, where for every i either s_i is in S or s_i^{-1} is in S . Then

$$u = f(a) = f(s_1)f(s_2) \dots f(s_k)$$

and for every i either $f(s_i)$ is in T or $f(s_i^{-1}) = f(s_i)^{-1}$ is in T . Thus T indeed generates H .