Solutions to Homework 6

Problem 1. Let G be a finite group and let H, K be subgroups of G.

a) Suppose that $h, h_1 \in H$ and $k, k_1 \in K$. Prove that $hk = h_1k_1$ if and only if $h_1 = hu$ and $k_1 = u^{-1}k$ for some $u \in H \cap K$.

b) Prove that $|HK| = |H||K|/|H \cap K|$.

Solution. a) If $hk = h_1k_1$ then $h^{-1}h_1 = kk_1^{-1}$. The element on the left hand side is in H and the element on the right hand side is in K. Since they are equal, we can write $h^{-1}h_1 = kk_1^{-1} = u$ for some $u \in H \cap K$. Thus $h_1 = hu$ and $k_1 = u^{-1}k$. Conversely, is $h_1 = hu$ and $k_1 = u^{-1}k$ then $h_1k_1 = (hu)(u^{-1}k) = hk$.

b) Consider the function $f : H \times K \longrightarrow HK$, $f(h, k) = hk$. This function is surjective. By part a), the preimage $f^{-1}(hk) = \{(hu, u^{-1}k) : u \in H \cap K\}$ has exactly $|H \cap K|$ elements for every element $hk \in HK$. This implies that $|H \times K| = |HK||H \cap K|$. Since $|H \times K| = |H||K|$, the result follows.

A slightly different argument. Note that HK is a union of cosets hK, $h \in H$. Each such coset has $|K|$ elements. Let t be the number of distinct cosets of this form. Then $|HK| = t|K|$. So we need to find t. We have $hK = h_1K$ if and only if $h^{-1}h_1 \in K \cap H$ (note that $h^{-1}h_1$ is always in H) which is equivalent to $h(H \cap K) = h_1(H \cap K)$. This implies that the function $hK \mapsto h(H \cap K)$ is well defined and is a bijection between cosets of K contained in HK and cosets of $H \cap K$ in H. Thus $t = [H : H \cap K] = |H|/|H \cap K|$.

Problem 2. Let G be a group and H a subgroup of G.

a) Prove that aHa^{-1} is a subgroup of G for any $a \in G$. Any subgroup of the form aHa^{-1} is called a **conjugate** of H.

b) Prove that $aHa^{-1} = bHb^{-1}$ if and only if $a^{-1}b \in N_G(H)$. Conclude that the number of different conjugates of H is equal to the index $[G : N_G(H)]$.

c) Prove that the intersection of all subgroups conjugate to H is a normal subgroup in G. Show that this subgroup is the largest subgroup of H which is normal in G (this means that any normal in G subgroup of H is contained in the above intersection).

d) Suppose that H has finite index in G. Prove that there is a normal subgroup of G which is contained in H and has finite index in H (use b), c) and Problem 2c) from homework 5).

Solution. a) Recall that the "conjugation by a" map $c_a : G \longrightarrow G$, $c_a(g) = aga^{-1}$ is an automorphism. Clearly $aHa^{-1} = c_a(H)$, and the image of a subgroup under any homomorphism is also a subgroup.

b) $aHa^{-1} = bHb^{-1}$ if and only if $c_a(H) = c_b(H)$ if and only if $H = c_a^{-1}c_b(H) = c_{a^{-1}b}(H)$. By part a) of problem 3 in homework 5, this is equivalent to $a^{-1}b \in N_G(H)$, which in turn is equivalent to $aN_G(H) = bN_G(H)$. This observation means that the function which assigns to a conjugate aHa^{-1} the coset $aN_G(H)$ is well defined and injective. It is clear that it is also surjective. Thus we have a bijection between conjugates of H and left cosets of $N_G(H)$ in G.

c) Let N be the intersection of all conjugates of H. Let $n \in N$ and $g \in G$. For any $a \in G$ we

have $n \in (g^{-1}a)H(g^{-1}a)^{-1} = g^{-1}aHa^{-1}g$. Thus $gng^{-1} \in g(g^{-1}aHa^{-1}g)g^{-1} = aHa^{-1}$. This shows that gng^{-1} is in every conjugate of H, so $gng^{-1} \in N$. Since g was arbitrary, N is a normal subgroup of G.

Suppose now that K is a subgroup of H which is normal in G. Then for any $g \in G$ we have

$$K = gKg^{-1} \subseteq gHg^{-1}.$$

Thus K is contained in every conjugate of H, so $K \subseteq N$.

d) Suppose $[G : H]$ is finite. Since conjugation is an automorphism, we have $[G : aHa^{-1}] = [G : H]$ for every $a \in G$. Thus all conjugates of H have finite index. Since $H \subseteq N_G(H)$, we have $[G : N_G(H)] \leq [G : H]$. Part b) tells us that H has a finite number of distinct conjugates. By part c) of problem 1 from homework 5, the intersection of finitely many subgroups of finite index is also of finite index. Thus the group N from part c) has finite index and it is normal.

Problem 3. Let G be a group.

a) Prove that if H is a subgroup of G and K is a normal subgroup of G then the groups KH/K and $H/(H \cap K)$ are isomorphic (hint: consider the restriction of the quotient homomorphism $KH \longrightarrow KH/K$ to the subgroup H of KH and show that it is surjective; then describe its kernel and apply FHT). Consult Problem 2 c) from homework 5.

b) Let K and H be normal subgroups of G such that $K \subseteq H$. Show that H/K is a normal subgroup of G/K. Prove that $(G/K)/(H/K)$ is isomorphic to G/H. Hint: consider the quotient homomorphisms $f : G \longrightarrow G/H$ and $\pi : G \longrightarrow G/K$. Use FHT to get a homomorphism $G/K \longrightarrow G/H$. Note that H/K is the kernel of this homomorphism. Apply FHT again.

Solution. a) Since K is normal in G we know from problem 2c) in homework 5 that that $HK = KH$ is a subgroup of G. Clearly HK contains K and H and K is normal in HK. Consider the quotient homomorphism $\pi : HK \longrightarrow HK/K$. We know that $K = \ker \pi$ and π is surjective. If $g \in HK$ then $g = hk$ for some $h \in H$ and $k \in K$. Thus $\pi(g) = \pi(hk) = \pi(h)\pi(k) = \pi(h)$. This shows that $\pi(H) = \pi(HK) = HK/K$. This means that the homomorphism $\pi : H \longrightarrow HK/K$ (i.e. restriction of π to H) is surjective. Its kernel is clearly equal to $H \cap \ker \pi = H \cap K$. Let $\sigma : H \longrightarrow H/(H \cap K)$ be the quotient homomorphism. The FHT tells us that there is unique isomorphism $\phi : H/(H \cap K) \longrightarrow HK/K$ such that $\phi\sigma = \pi$. It is easy to see that it is given by $\phi(h(H \cap K)) = hK$.

Remark. Another way to solve the problem is to show that the function from $H/(H \cap K)$ to HK/K given by $\phi(h(H \cap K)) = hK$ is well defined and then show that it is a bijection and a group homomorphism.

b) Let $f : G \longrightarrow G/H$ and $\pi : G \longrightarrow G/K$ be the quotient homomorphisms. Note that $\ker \pi = K \subseteq H = \ker f$. By FHT there is unique homomorphism $\overline{f} : G/K \longrightarrow G/H$ such that $\overline{f}\pi = f$. Since f is surjective, so is $\overline{f}$. Now $\ker \overline{f} = \pi(\ker f) = \pi(H) = H/K$. Let $\tau : G/K \longrightarrow (G/K)/(H/K)$ be the quotient homomorphism. Since $\overline{f}$ is surjective and $\ker \overline{f} = \ker \tau$, FHT tells us that there is a unique isomorphism $h : (G/K)/(H/K) \longrightarrow G/H$ such that $h\tau = \overline{f}$. It is easy tho see that $h((gK)(H/K)) = gH$.

Problem 4. Let G be a finite group and let H be a subgroup of G. Let m be the smallest positive integer such that $a^m \in H$. Prove that $< a^m >= H \cap < a >$ and that m divides

the order of a. **Hint:** Prove first that $\{k \in \mathbb{Z} : a^k \in H\}$ is a subgroup of $\mathbb{Z}$.

Solution: Consider the set $J = \{k \in \mathbb{Z} : a^k \in H\}$. If $s, t \in J$ then $a^s \in H$ and $a^t \in H$. Since H is a group, we have $a^{s+t} = a^s a^t \in H$ and $a^{-s} = (a^s)^{-1} \in H$. Thus $s + t$ and $-s$ are both in J. This shows that J is a subgrpup of $\mathbb{Z}$ (clearly, $0 \in \mathbb{Z}$). Since G is finite, the order of a is finite. Call it n. Thus $a^n = e \in H$, so $n \in J$. Recall now that every non-trivial subgroup of $\mathbb{Z}$ is of the form $d\mathbb{Z}$, where d is the smallest positive element of the subgroup. Since, by its definition, m is the smallest positive element of J, we have $J = m\mathbb{Z}$. Since $n \in J$, we have $m|n$. Finally $a^t \in H$ iff $t \in J$ iff $m|t$. It follows that $H \cap < a >= \{a^t : m|t\} =< a^m >$.

Problem 5. Let G be a group and let f_n be the function $f_n : G \longrightarrow G$, $f_n(g) = g^n$. Prove that if f_3 and f_5 are homomorphisms then G is abelian.

Solution. Let $a, b \in G$. Then $(ab)^3 = f_3(ab) = f_3(a)f_3(b) = a^3b^3$. This implies that $baba = a^2b^2$.
Similarly, $(ab)^5 = a^5b^5$, which implies that $babababa = a^4b^4$. Thus we have $(ba)^2 = a^2b^2$ and $(ba)^4 = a^4b^4$. Thus $a^2b^2a^2b^2 = a^4b^4$, so $b^2a^2 = a^2b^2$. So $baba = a^2b^2 = b^2a^2$, which implies $ab = ba$. This proves that any 2 elements in G commute, i.e. G is abelian.

Problem 6. Let $G = \mathbb{Q} \times \mathbb{Z}$ as a set. Here $\mathbb{Q}$ stands for the group of rational numbers and $\mathbb{Z}$ for the integers (both with addition as the group operation). We define a binary operation on the set G as follows:

$$(q, m)(r, n) = (q + 2^m r, m + n)$$

(this construction is a special case of a general construction called a **semidirect product**).

a) Verify that G with this binary operation is a group. What is the inverse of (q, m)?

b) Let $T = \{(q, 0) : q \text{ is an integer}\}$. Prove that T is a subgroup of G.

c) Show that $(0, 1)(q, 0)(0, 1)^{-1} = (2q, 0)$. Conclude that if $t = (0, 1)$ then tTt^{-1} is a proper subgroup of T. What is $t^{-1}Tt$?

d) What is the normalizer of T in G?

Solution. a) First we check associativity:

$$[(q, m)(r, n)](p, k) = (q + 2^m r, m + n)(p, k) = (q + 2^m r + 2^{m+n} p, m + n + k)$$

and

$$(q, m)[(r, n)(p, k)] = (q, m)(r+2^n p, n+k) = (q+2^m(r+2^n p), m+n+k) = (q+2^m r+2^{m+n} p, m+n+k)$$

so the operation is associative. Note that $e = (0, 0)$ is the identity. Finally

$$(q, m)(-2^{-m} q, -m) = (0, 0) = (-2^{-m} q, -m)(q, m)$$

so $(q, m)^{-1} = (-2^{-m} q, -m)$. Thus G is a group.

b) Clearly $(m, 0)(n, 0) = (m + n, 0)$ and $(m, 0)^{-1} = (-m, 0)$, so T is closed under multiplication and inversion. Also $(0, 0) \in T$, so T is a subgroup.

c) Since $(0, 1)^{-1} = (0, -1)$, we have

$$(0, 1)(q, 0)(0, 1)^{-1} = (2q, 1)(0, -1) = (2q, 0).$$

If m is an integer then $t(m,0)t^{-1} = (2m,0)$. Thus $tTt^{-1} = \{(q,0) : q \text{ is an even integer}\}$, which is a proper subgroup of T. In the same way we see that $t^{-1}Tt = \{(q,0) : 2q \text{ is an integer}\}$, so T is a proper subgroup of $t^{-1}Tt$.

d) We have

$$(q,m)(a,0)(q,m)^{-1} = (q + 2^m a, m)(-2^{-m}q, -m) = (2^m a, 0).$$

It follows that if $m > 0$ then $(1,0) \notin (q,m)T(q,m)^{-1}$ and if $m < 0$ then $(2^m,0) \notin T$ and $(2^m,0) \in (q,m)T(q,m)^{-1}$. In both cases, $T \neq (q,m)T(q,m)^{-1}$. Thus if (q,m) normalizes T then $m = 0$. Conversely, $(q,0)$ commutes with all elements in T, so it normalizes T. Thus the normalizer of T is $\{(q,0) : q \in \mathbb{Q}\}$.

Problem 7. Problem G to chapter 15.

Solution. 1. Note that the conjugacy class of a always contains a. Thus the conjugacy class of a has one element if and only if $a = gag^{-1}$ for all $g \in G$, which is the same as a belongs to the center $Z(G)$ of G (the book denotes it by C).

2. Recall that being conjugate is an equivalence relation (problem I1 to chapter 13, see homework 5). Thus conjugacy classes partition the group, so the size of the group is equal to the sum of the sizes of all conjugacy classes. If we have t conjugacy classes and we list their sizes in non-decreasing order $k_1 \leq k_2 \leq \cdots \leq k_t$ then $k_1 = \ldots = k_{s-1} = 1$ and $k_s > 1$, where $s - 1 = |Z(G)| = c$ (since by part 1. we have exactly $|Z(G)| = c$ conjugacy classes of size 1). Thus $|G| = c + k_s + \ldots k_t$ (the book's notation is not the best; writing $c+1$ instead of s would make more sense).

3. Recall that the size of the conjugacy class of a is equal to the index $[G : C(a)]$ of the centralizer of a in G (problem I6. to chapter 13; see homework 5). In particular, each k_i divides the order of the group. If G is a p-group, then each k_i is a power of p. In particular, if $k_i > 1$ then $p|k_i$.

4. By 3., all the numbers $k_s, k_{s+1}, \ldots, k_t$ are divisible by p and so is $|G|$. Thus $c = |G| - (k_s + \ldots k_t)$ is divisible by p. It follows that $Z(G)$ has at least p elements.

We proved the following fundamental result.

Theorem. If G is a finite p-group then the center of G is a non-trivial subgroup.

5. Suppose that $|G| = p^2$. If $Z(G) = G$ then G is abelian. If $Z(G) \neq G$ then $|Z(G)| = p$. This however implies that $|G/Z(G)| = p$, so $G/Z(G)$ is a cyclic group. By Problem 5 from homework 5 we conclude that G is abelian.

6. If G has an element of order p^2 then $G \cong \mathbb{Z}_{p^2}$ is cyclic. Otherwise, every non-trivial element in G has order p. Take $a \in G$, $a \neq e$. Then $A =< a > \cong \mathbb{Z}_p$. Take any $b \in G$, $b \notin A$. Then $B =< b > \cong \mathbb{Z}_p$. Since $A \neq B$, we have $A \cap B = \{e\}$ and $AB = G$. Since G is abelian, A, B are normal subgroups and $G \cong A \times B \cong \mathbb{Z}_p \times \mathbb{Z}_p$ (this also follows from the Fundamental Theorem of Finite Abelian Groups).