THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2019-20
Homework 2 Solution
Due Date: 19th September 2019

Compulsory part

1. Let G be of order ≥ 2 but with no proper nontrivial subgroups. Let $e \neq a \in G$. Note that the nontrivial cyclic subgroup $\langle a \rangle, G$ must be finite, for otherwise it is isomorphic to $\mathbb{Z}$ which has proper subgroups. Then the nontrivial cyclic subgroup $\langle a \rangle$ must be G itself because every cyclic group not of prime order has proper subgroups. Therefore G must be finite and of prime order.

2. From $[G : H] = 2$, we know that $G = H \sqcup gH$ for some $g \in G$, where the union is disjoint (i.e. $H \cap gH = \emptyset$). Observe that $G = H \sqcup Hg^{-1}$. (To see it, we recall the map $\tau : G \to G$, $\tau(x) = x^{-1}$, is a bijective function. Thus $\tau(G) = \tau(H) \sqcup \tau(gH)$. As H is a subgroup, $\tau(H) = H$ and $\tau(gH) = Hg^{-1}$.)

   Clearly from $G = H \sqcup gH = H \sqcup Hg^{-1}$, we deduce (with the disjointness) that

   Case 1. $H = Hg^{-1}$ and $gH = H$: This implies $g \in H$ (as $g = ge \in gH$), then $gH \subset H$, contradicting to $H \cap gH = \emptyset$.

   Case 2. $gH = Hg^{-1}$: This implies $g \in Hg^{-1}$, and $g \in Hg^{-1} \Rightarrow g = hg^{-1}$ for some $h \in H \Rightarrow g^{-1} = h^{-1}g \Rightarrow Hg^{-1} = Hh^{-1} \cdot g = Hg$. i.e. $gH = Hg$.

   Let $x \in G$ $(= H \sqcup gH)$. If $x \in H$, then clearly $xH = Hx$. Otherwise (i.e. $x \in gH = Hg$), let $x = gh = h'g$ for some $h, h' \in H$, then
   $$xH = gh \cdot H = gH \quad \text{and} \quad Hx = H \cdot h'g = Hg.$$

   So $xH = Hx$ for all $x \in G$.
   Remark: Note that $H \lhd G$.

3. (a)
   - Reflexive: $\forall a, a \sim a$ as $a = eae$ with $e \in H$ and $e \in K$.
   - Symmetric: Let $a \sim b$ so $a = hbk$ for some $h \in H, k \in K$. Then $b = h^{-1}ak^{-1}$ so we have $b \sim a$.
   - Transitive: Let $a \sim b$ and $b \sim c$ so $a = h_1bk_1$ and $b = h_2ck_2$ for some $h_1, h_2 \in H, k_1, k_2 \in K$. Then $a = h_1h_2ck_2k_1$ so we have $a \sim c$.

   (b) The equivalence class containing the element a is $HaK = \{hak : h \in H, k \in K\}$. It can be formed by taking the union of all right cosets of H that contain elements in the left coset aK or the union of all left cosets of K that contain elements in the right coset Ha.

4.
   - Closure: Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Because H and K are both subgroups of G, we have $ab \in H$ and $ab \in K$, so $ab \in H \cap K$.
   - Identity: As $e \in H$ and $e \in K$, $e \in H \cap K$.
   - Inverse: Let $a \in H \cap K$. Then $a \in H$ and $a \in K$. Because H and K are both subgroups of G, we have $a^{-1} \in H$ and $a^{-1} \in K$, so $a^{-1} \in H \cap K$.

5. WLOG, we can only work on $\mathbb{Z}_n$. Let $d|n$. Then $\langle n/d \rangle$ is a subgroup of $\mathbb{Z}_n$ with order d. We have the only one such subgroup. (Note that the element $k \in \mathbb{Z}_n$ has order d which says $kd = 1$, but on other hand, $kd = nt$ for $0 \leq t < d$, then $k \in \langle n/d \rangle$.) Every subgroup has the order dividing n, so these are the only subgroups that it has.

6. (a) 36

   (b) $2, 12, 60$

   (c) Find an isomorphic group that is a direct product of cyclic groups of prime-power order. For each prime divisor of the order of the group, write the subscripts in the direct product involving that prime in a row in order of increasing magnitude. Keep the right-hand ends of the rows aligned. Then take the product of the numbers down each column of the array.

7.
   - Closure: Let $a, b \in H$. Then $a^2 = b^2 = e$. Because G is abelian, we see that $(ab)^2 = abab = aabb = ee = e$, so $ab \in H$ also. Thus H is closed under the group operation.
   - Identity: Clearly $e \in H$.
   - Inverses: For all $a \in H$, the equation $a^2 = e$ means that $a^{-1} = a2 \in H$. Thus H is a subgroup.

8. (a) $(h, k) = (h, e)(e, k)$.

   (b) $(h, e)(e, k) = (h, k) = (e, k)(h, e)$.

   (c) The only element of $H \times K$ of the form (h, e) and also of the form (e, k) is $(e, e) = e$.

9.
   - Uniqueness: Suppose that $g = hk = h_1k_1$ for $h, h_1 \in H$ and $k, k_1 \in K$. Then $h_1^{-1}h = k_1k^{-1}$ is in both H and K, and we know that $H \cap K = \{e\}$. Thus $h_1^{-1}h = k_1k^{-1} = e$, from which we see that $h = h_1$ and $k = k_1$.
   - Isomorphic: Suppose $g_1 = h_1k_1$ and $g_2 = h_2k_2$. Then $g_1g_2 = h_1k_1h_2k_2 = h_1h_2k_1k_2$ because elements of H and K commute by hypothesis b. Thus by uniqueness, g_1g_2 is renamed $(h_1h_2, k_1k_2) = (h_1, k_1)(h_2, k_2)$ in $H \times K$.

Optional Part

1. Every element in $\mathbb{Z}_n$ generates a subgroup of some order d dividing n, and the number of generators of that subgroup is $\phi(d)$. By Question 4, there is a unique such subgroup of order d dividing n. Thus $\sum_{d|n} \phi(d)$ counts each element of Zn once and only once as a generator of a subgroup of order d dividing n. Hence

$$\sum_{d|n} \phi(d) = n$$

2. Let d be a divisor of $n = |G|$. Now if G contains a subgroup of order d, then each element of that subgroup satisfies the equation $x^d = e$. Note that if there exists at least one element of order d, then we can generates a cyclic group of order d, whose elements give at most d solutions to the equation $x^d = e$ (by the hypothesis). By the hypothesis that $x^m = e$ has at most m solutions in G, we see that there can be at most one subgroup

of each order d dividing n. Now each $a \in G$ has some order d dividing n, and $\langle a \rangle$ has exactly $\phi(d)$ generators. Because $\langle a \rangle$ must be the only subgroup of order d, we see that the number of elements of order d for each divisor d of n cannot larger than $\phi(d)$. Thus we can establish

$$n = \sum_{d|n} \text{(number of elements of } G \text{ of order } d) \leq \sum_{d|n} \phi(d) = n.$$

This shows that G must have exactly $\phi(d)$ elements of each order d dividing n, in particular, it must have $\phi(n) \geq 1$ elements of order n. Hence G is cyclic.

3. Recall that every subgroup of a cyclic group is cyclic. Thus if a finite abelian group G contains a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$, which is not cyclic, then G cannot be cyclic.

   Conversely, suppose that G is a finite abelian group that is not cyclic. By Fundamental Theorem of finitely generated abelian groups, G contains a subgroup isomorphic to $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$ for the same prime p, because if all components in the direct product correspond to distinct primes, then G would be cyclic ($\mathbb{Z}_n \times \mathbb{Z}_n$ is cyclic if $gcd(n, m) = 1$). The subgroup $\langle p^{r-1} \rangle \times \langle p^{s-1} \rangle$ of $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$ is clearly isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

4. By Fundamental Theorem of finitely generated abelian groups, the groups that appear in the decompositions of $G \times K$ and of $H \times K$ are unique except for the order of the factors. Because $G \times K$ and of $H \times K$ are isomorphic, these factors in their decompositions must be the same. Because the decompositions of $G \times K$ and of $H \times K$ can both be written in the order with the factors from K last, we see that G and H must have the same factors in their expression in the decomposition described in Fundamental Theorem of finitely generated abelian groups. Thus G and H are isomorphic.