Solutions to Homework 2 **Math 5590H**

5pt **1.6.8,10.** *Let A and B be two sets of the same cardinality, that is, such that there exists a bijection $\varphi\colon A \longrightarrow B$. Define a mapping $\Phi\colon S_A \longrightarrow S_B$ by $\Phi(\sigma) = \varphi\circ\sigma\circ\varphi^{-1}$, $\sigma \in S_A$. Prove that Φ is an isomorphism between S_A and S_B.*

Solution. Φ is invertible; – its inverse is defined by the formula $\Phi^{-1}(\rho) = \varphi^{-1}\circ\rho\circ\varphi$, $\rho \in S_B$. And Φ is an isomorphism because for any $\sigma_1, \sigma_2 \in S_A$,

$$\Phi(\sigma_1\sigma_2) = \varphi\circ(\sigma_1\circ\sigma_2)\circ\varphi^{-1} = \varphi\circ\sigma_1\circ\varphi^{-1}\circ\varphi\circ\sigma_2\circ\varphi^{-1} = \Phi(\sigma_1)\Phi(\sigma_2).$$

5pt **2.1.4.** (a) *If G is a finite group and H is a nonempty subset of G such that $HH \subseteq H$, prove that H is a subgroup of G.*

Solution. Let G be finite. Then every element $a \in G$ has finite order, so $a^{-1} = a^{n-1}$ where $n = |a|$. Hence, for every $a \in H$, $a^{-1} = a^{n-1} = aa\cdots aa \in HH\cdots HH \subseteq H$. And also, $1 = aa^{-1} \in H$.

5pt (b) *Show by example that it may not be so if G is infnite.*

Solution. For $G = \mathbb{Z}$, the set $H = \mathbb{N}$ is closed under addition, but is not a subgroup.

5pt **2.1.6.** (a) *Let G be an abelian group. Prove that $H = \{g \in G : |g| < \infty\}$ is a subgroup of G (called the torsion subgroup of G).*

Solution. Let G be abelian. If $a, b \in H$ then $a^n = b^m = 1$ for some $n, m \in \mathbb{N}$, then $(ab^{-1})^{nm} = (a^n)^m(b^m)^{-n} = 1$, so $|ab^{-1}| < \infty$, so $ab^{-1} \in H$. So, H is a subgroup.

5pt (b) *Give an example where G is nonabelian and H is not a subgroup.*

Solution. Consider the nonabelian group $G = \{a, b \,|\, a^2 = b^2 = 1\}$: in this group, a and b have finite orders but $|ab| = \infty$: the elements $1, ab, abab, ababab, \ldots$ are all distinct.

10pt **2.3.16.** *If x and y commute, prove that $|xy|$ divides* $\operatorname{lcm}(|x|, |y|)$. *Show that this may not be so if x and y do not commute. When x and y commute, show that $|xy|$ may not be equal to* $\operatorname{lcm}(|x|, |y|)$.

Solution. If x and y commute, then for every $k \in \mathbb{N}$, $(xy)^k = x^k y^k$. For $l = \operatorname{lcm}(|x|, |y|)$ we have $x^l = y^l = 1$, so $(xy)^l = 1$, so $|xy| \,\big|\, l$.

In S_3, the permutation $(1, 2, 3) = (1, 2)(2, 3)$ has order 3 whereas $|(1, 2)| = |(2, 3)| = 2$.

In the cyclic group $\{1, a, a^2, \ldots, a^{11}\} \simeq \mathbb{Z}_{12}$, a has order 12, a^2 has order 6, but $a^3 = aa^2$ has order 4.

5pt **1.2.3.** *Using the standard presentation $D_{2n} = \left\langle r, s \;\middle|\; r^n = s^2 = 1,\ rs = sr^{-1} \right\rangle$ of the dihedral group, prove that all elements of D_{2n} of the form sr^k have order 2. Deduce that D_{2n} is generated by two elements, s and sr, of order 2.*

Solution. By induction, for any k, $r^k s = sr^{-k}$. So, for any k, $(sr^k)^2 = sr^k sr^k = s^2 r^{-k} r^k = 1$.

D_{2n} is generated by s and $c = sr$ since $r = sc$, so every element of D_{2n} can be rewritten in terms of s and c.

5pt **1.6.24.** *If G is a finite group generated by two distinct elements a and b of order 2, prove that $G \cong D_{2n}$, where $n = |ab|$.*

Solution. In $D_{2n} = \left\langle r, s \;\middle|\; r^n = s^2 = 1,\ rs = sr^{-1} \right\rangle$ take new generators $a = s$ and $b = sr$, so that $s = a$ and $r = ab$; then the relations $r^n = s^2 = 1$ and $rs = sr^{-1}$ take the form $(ab)^n = a^2 = 1$ and $aba = ab^{-1}a$, which is equivalent to $b^2 = 1$. So, $D_{2n} \cong G = \left\langle a, b \;\middle|\; a^2 = b^2 = 1,\ (ab)^n = 1 \right\rangle$. (The isomorphism $\varphi\colon D_{2n} \longrightarrow G$ is defined by $\varphi(s) = a$, $\varphi(r) = ab$, and for any word w in the alphabet $\{r, s\}$, $\varphi(w)$ is obtained by replacing all s by a and all r by ab.)

10pt **1.5.3.** *Using the generators i, j of Q_8, find a set R of relations to get a presentation of Q_8 in the form $Q_8 = \langle i, j \mid R\rangle$.*

Solution. The problem has many solutions; one is to take as the set of relations the complete multiplication table of Q_8.

Q_8 is generated by i and j since all other elements are their products: $-1 = i^2 = j^2$, $k = ij$, $-i = -1 \cdot i$, $-j = -1 \cdot j$, $-k = -1 \cdot k$. Obvious relations are $i^4 = 1$, $i^2 = j^2$, and $ji = i^3 j$. We can now show that the complete multiplication table in Q_8 follows from these three relations; clearly, this will imply that no more relations are needed, so $Q_8 = \langle i, j \,|\, i^4 = 1,\ i^2 = j^2,\ ji = i^3 j \rangle$. (Indeed, $(-1)^2 = i^4 = 1$, $-i = i^3 = i(-1)$, $-j = j^2 j = j^3 = j(-1)$, $-k = i^2 ij = ii^2 j = ij^2 j = ijj^2 = k(-1)$, $k^2 = ijij = ii^3 jj = j^2 = -1$, $ji = ij(-1) = -k$, $ik = i^2 j = -j$, $ki = iji = i^4 j = j$, $jk = jij = i^3 j^2 = ii^2 j^2 = i$, and $kj = ij^2 = -i$.)

A simpler approach is to show that, using the relations $i^4 = 1$, $i^2 = j^2$, and $ij = ji^3$, we can write every element of the group $G = \langle i, j \,|\, i^4 = 1,\ i^2 = j^2,\ ij = ji^3 \rangle$ in the form $i^n j^m$ with $n \in \{0, \ldots, 3\}$ and $m \in \{0, 1\}$, which proves that G has at most 8 elements. Since $|Q_8| = 8$ and Q_8 has all these relations, it must be that $Q_8 = G$. (We will have a rigorous justification of this approach later.)

2.3.12. *Prove that the following groups are not cyclic (cannot be generated by a single element):*

5pt (a) $\mathbb{Z}_2^2 = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Solution. All nontrivial elements of the group have order 2, thus none of four elements of this group generates it.

Another solution. The group has two (actually, three) subgroups of order 2; this is impossible for a cyclic group.

5pt (b) $\mathbb{Z}_2 \times \mathbb{Z}$.

Solution. The group is infinite, but contains an element of finite order; this is impossible for an infinite cyclic group.

5pt (c) $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$.

Solution. No element of this group generates it: for any $u \in \mathbb{Z}^2$, we have $\langle u \rangle = \{nu,\ n \in \mathbb{Z}\}$. If $u = (a, b)$ and $a \neq 0$, then $nu = (na, nb) \neq (0, 1)$ for all $n \in \mathbb{Z}$; if $b \neq 0$, then $nu = (na, nb) \neq (1, 0)$ for all $n \in \mathbb{Z}$.