Homework 4
Solutions

(1) The center $Z(G)$ of G is a subgroup of G. Hence by Lagrange's theorem $|Z(G)| = 1$, $|Z(G)| = p$ or $|Z(G)| = p^2$. Let us first show that $|Z(G)| = 1$ cannot occur. Let $x \in G$ be a nonidentity element. Then $|x| \geq 2$. Since $|x|$ divides $|G|$ either $|x| = p$ or $|x| = p^2$. If $|x| = p^2$ then $G = \langle x \rangle$ and G is abelian. Hence we may assume that every nonidentity element in G has order p. If $|Z(G)| = 1$ this implies

$$|G| = p^2 = 1 + kp$$

for some positive integer k. The left-hand side is divisible by p whereas the right-hand side is not since p is a prime. This shows that $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2$ then $Z(G) = G$ and hence G is abelian.

It remains to consider the case $|Z(G)| = p$. Then $|G/Z(G)| = p$ and hence $G/Z(G)$ is cyclic by Corollary 10 on page 91. By Exercise 3 on Homework 3 this implies that G is abelian.

(2) (a) This is clear since $|\{(x_1, \ldots, x_p)\}| = |G|^p$, but the condition $x_1 \cdots x_p = 1$ fixes $x_p = (x_1 \cdots x_{p-1})^{-1}$. Hence $|\mathcal{S}| = |G|^{p-1}$.

(b) It suffices to show that if $x = (x_1, \ldots, x_p) \in \mathcal{S}$ then $\tilde{x} = (x_2, \ldots, x_p, x_1) \in \mathcal{S}$. But $x_2 \cdots x_p x_1 = x_1^{-1}(x_1 \cdots x_p)x_1 = x_1^{-1}x_1 = 1$ and hence $\tilde{x} \in \mathcal{S}$.

(c) Say that $x \sim y$ if y is a cyclic permutation of x. This is an equivalence relation: (1) $\sim$ is reflexive since $x \sim x$ (x is a cyclic permutation of itself), (2) $\sim$ is symmetric since $x \sim y$ implies $y \sim x$; if x is a cyclic permutation of y then so is y a cyclic permutation of x, (3) $\sim$ is transitive since x a cyclic permutation of y and y a cyclic permutation of z implies that x is a cyclic permutation of z.

(d) If an equivalence class contains exactly one element then all cyclic permutations must be equal. This implies that the element is of the form $(x, \ldots, x)$ with $x^p = 1$. Conversely, if $(x, \ldots, x)$ with $x^p = 1$ then this forms an equivalence class with only one element.

(e) We show that every equivalence class has order 1 or p. Certainly every equivalence class has order $\leq p$. Suppose that $x = (x_1, \ldots, x_p)$ has order m with $1 < m < p$. This means that $(x_1, \ldots, x_p) = (x_{1+km}, \ldots, x_{p+km})$ for all integers k. Here we view the indices modulo p. We know that $\mathbb{Z}/p\mathbb{Z}$ is generated by any $1 \leq a < p$ if p is prime. Hence $(x_1, \ldots, x_p) = (x_{1+km}, \ldots, x_{p+km})$ for all k implies that all x_i are equal. But by (e) this means $| \sim x| = 1$ which contradicts our assumptions. Hence $| \sim x| = p$.
This implies that $|G|^{p-1} = |\mathcal{S}| = k + pd$ which is the number of equivalence classes of order 1 plus the number of equivalence classes of order p.

(f) $(1, \ldots, 1)$ is an equivalence class of order 1. Hence $k \geq 1$. But p divides $|G|^{p-1}$, hence p must divide k. Hence $k > 1$ which shows that there exists and element $x \in G$, $x \neq 1$ such that $x^p = 1$.

(3) We have

$$\begin{aligned} |G| &= |G : H| \cdot |H| \\ |G| &= |G : K| \cdot |K| \\ |K| &= |K : H| \cdot |H|. \end{aligned}$$

Hence $|G| = |G : K| \cdot |K| = |G : K| \cdot |K : H| \cdot |H|$. Comparing with $|G| = |G : H| \cdot |H|$ yields $|G : H| = |G : K| \cdot |K : H|$.

These equations still make sense when $|G| = \infty$. Namely, setting $n = |G : K|$ and $m = |K : H|$ they mean that G and K are partitioned by the following disjoint sets $G = \cup_{i=1}^{n} a_i K$ and $K = \cup_{i=1}^{m} b_i H$ where $a_i^{-1} a_j \notin K$ if $i \neq j$ and $b_i^{-1} b_j \notin H$ if $i \neq j$. Hence G is also partitioned into to following disjoint sets $G = \cup_{i=1}^{n} \cup_{j=1}^{m} a_i b_j H$ (namely $a_i b_j H = a_k b_l H$ implies that $i = k$ and $j = l$ since $b_j H$ and $b_l H$ are both subsets of K and hence $i = k$. This in turn implies $j = l$ since then $b_l^{-1} b_j \in H$).

(4) If p is prime the order of $(\mathbb{Z}/p\mathbb{Z})^\times$ is $p-1$. If $a = 0$ the assertion holds trivially. If $a \neq 0$ then $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Consider $H = \langle a \rangle$. By Lagrange's theorem, $|a|$ divides $p-1$ so that $a^{p-1} \equiv 1 \mod p$ or $a^p \equiv a \mod p$.

(5) The lattice is given by $MN \times 1 \leq G \times G$, $M \times N \trianglelefteq G \times G$, $M \cap N \times 1 \trianglelefteq MN \times 1$ and $M \cap N \times 1 \leq M \times N$. By the second isomorphism theorem $G/(M \cap N) \cong (G/M) \times (G/N)$.

(6) We have a group G with $|G| = p^a m$ where p does not divide m, $P \leq G$ with $|P| = p^a$ and $N \trianglelefteq G$ with $|N| = p^b n$ where p does not divide n. Since $P \leq PN$ the order of P must divide the

order of PN. Since PN is a subgroup of G, this implies that $|PN| = p^a k$ for some positive integer k. Since N is a subgroup of PN, $p^a k$ must be divisible by $p^b n$ so that $|PN| = p^a ni$ for some positive integer i which does not divide p. Now

$$|P \cap N| = \frac{|P||N|}{|PN|} = \frac{p^b}{i}.$$

Since this has to be an integer it follows that $i = 1$. By the second isomorphism theorem we have $PN/N \cong P/P \cap N$ so that $|PN/N| = |P/P \cap N| = p^{a-b}$.

(7) Let G be a group of order 6. By Cauchy's theorem we know that there is an element $x \in G$ of order 3 and an element $y \in G$ of order 2. If $xy = yx$ then $(xy)^6 = x^6 y^6 = 1$. Note that $xy = 1$ would imply $y = x^2$, but x^2 has order 3 and not 2. Also $(xy)^2 = x^2$, $(xy)^3 = y$, $(xy)^4 = x$, $(xy)^5 = x^2 y \neq 1$ since otherwise $x = y$. Hence xy has order 6 which implies that $G \cong Z_6$. This shows that $xy \neq yx$ if G is nonabelian so that $xyx^{-1} \neq y$. Hence the subgroup $\langle y \rangle$ of G is nonnormal. By Corollary 5 on page 123 the subgroup $\langle x \rangle$ is normal so that $yxy^{-1} = x^a$. $a = 0$ would imply $x = 1$ which contradicts that x has order 3. $a = 1$ contradicts $xy \neq yx$. Hence $a = 2$. This shows that G is generated by x and y with the relations $x^3 = y^2 = 1$ and $xy = yx^2$ which shows that $G \cong S_3$. Hence the only groups of order 6 are S_3 and Z_6.