HW5

1. (1). Let $H < G$. Describe the subgroup of G generated by the complement set of H. (2). Let G be a finite group with order $n, S \subseteq G$ and $|S| > n/2$. Prove that for all $g \in G$, there exist $a, b \in S$ s.t. $g = ab$.

Proof. Consider $S \cap gS^{-1}$. Since $|S| > n/2$, there is $a = gb^{-1} \in S \cap gS^{-1}$ and so $g = ab$. □

2. If G is a finite non-trivial group with only one maximal subgroup, show that G is cyclic and $|G| = p^k$ where p is a prime number and k is a positive integer. Then we can deduce that if G is a finite group, and suppose that for any two subgroups H and K either $H \subseteq K$ or $K \subseteq H$. Then G is cyclic of order p^k.

Proof. Since G has the unique maximal subgroup, $G/\Phi(G) \simeq G/M$. Since $G' \leqslant \Phi(G)$, by Widlandt, G is nilpotent and $G/M \simeq \mathbb{Z}_p$. Since G is a direct product of Sylow p-subgroups and G has only one maximal subgroup, G is a p-group. It follows that G has only one generator and so G is cyclic of order p^k.

Alternating proof. Let H be the maximal subgroup of G. Consider $g \in G \backslash H$, then $G = \langle g \rangle$. Otherwise, then $\langle g \rangle \leqslant H$ and it contradicts with $g \notin H$. Hence G is cyclic. Now suppose $|G| = n$ where $p \neq q$ are distinct primes with $p \mid n$ and $q \mid n$. Then $\langle g^p \rangle, \langle g^q \rangle < H$. Since $(p, q) = 1$, there are $l, k \in \mathbb{N}$ such that $lp + kq = 1$ and so $g \in H$, which is impossible. □

3. Let A be a finite abelian group and let p be a prime number. Let

$$A^p = \{a^p \mid a \in A\} \quad \text{and} \quad A_p = \{x \mid x^p = 1\}$$

(so A^p and A_p are the image and kernel of the p^{th} -power map, respectively).

- (a) Prove that $A/A^p \simeq A_p$ (Show that they are both elementary abelian and they have the same order, an elementary abelian group is an abelian group in which all elements other than the identity have the same order. i.e. If G is elementary abelian then $G \simeq (\mathbb{Z}_p)^k$ where p is a prime number and k is a positive integer.)
- (b) Prove that the number of subgroups of A of order p equals the number of subgroups of A of index p (Reduce to the case where A is an elementary abelian p-group.)
- (c) Let $A = Z_{60} \times Z_{45} \times Z_{12} \times Z_{36}$. Find the number of elements of order 2 and the number of subgroups of index 2 in A.

Proof. a) Since $\varphi : A \to A, a \mapsto a^p$ is a group homomorphism with $\ker \varphi = A_p$, there is $A/A_p \simeq A^p$. Thus $|A| = |A_p||A^p|$. Furthermore, note that $A^p \lhd A$ and $A^p \cap A_p = \{1\}$, we have that $A_p \times A^p = A$ and so $A/A^p \simeq A_p$.

b) Note that any subgroup of A of order p is a subgroup of A_p, so the number of subgroups of A of order p equals to the number of subgroups of A_p of order p. For any subgroup H of A of index p, $G/H \simeq \mathbb{Z}_p$ and so $g^p \in H$ for all $g \in H$. Thus $H \geqslant A^p$. Since $G/A^p/H/A^p \simeq G/H \simeq \mathbb{Z}_p$, we have that H/A^p is a subgroup of $G/A^p \simeq A_p$ of index p. Therefore, the number of subgroups of G of index p equals the number of subgroups of A_p of index p.

It suffices to show the number of subgroups of A_p of order p equals the number of subgroups of A_p of index p. By the definition of A_p, we assume that $A_p \cong \mathbb{Z}_p^k$ for some positive integer k. Note that the number of subgroups of $\mathbb{Z}_p^k$ of order p equals $\frac{p^k-1}{p-1}$. Now we compute the number of subgroups of $\mathbb{Z}_p^k$ of index p. Firstly, there are

$$(p^k - 1)(p^k - p) \cdots (p^k - p^{k-2})$$

ways to get $k-1$ elements to generated a group of order $\mathbb{Z}_p^{k-1}$. For a fixed $M \leqslant A_p$ with $M \simeq \mathbb{Z}_p^{k-1}$, there are

$$(p^{k-1} - 1)(p^{k-1} - p) \cdots (p^{k-1} - p^{k-2})$$

ways to choosing $k-1$ elements to generated M. Therefore, the number of subgroups of index p equals to $\frac{(p^k-1)(p^k-p)\cdots(p^k-p^{k-2})}{(p^{k-1}-1)(p^{k-1}-p)\cdots(p^{k-1}-p^{k-2})} = \frac{p^k-1}{p-1}$.

c) When $p=2$ and $A = Z_{60} \times Z_{45} \times Z_{12} \times Z_{36}$, $A_2 = Z_2 \times Z_1 \times Z_2 \times Z_2 \simeq \mathbb{Z}_2^3$, the number of subgroups of A of order p equals the number of subgroups of A of index p equals $2^3 - 1 = 7$. □

4. Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either (i) $K \leq H$ or (ii) $G = HK$ and $|K : K \cap H| = p$.

Proof. Note that H is a maximal subgroup of G. If $K \nleq H$, then $G = \langle H, K\rangle = HK$ and so $K/K \cap H \simeq HK/H \simeq \mathbb{Z}_p$. □

5. If G is a group of odd order, prove for any nonidentity element $x \in G$ that x and x^{-1} are not conjugate in G.

Proof. If $x, x^{-1} \in x^G$, then for any $y \in x^G$, $y^{-1} \in x^G$ and $y \neq y^{-1}$. It follows that $|x^G|$ is even, which contradicts with $|x^G| = |G|/|C_G(x)|$. □

6. Let G be a finite group with order $n, a_1, a_2, \ldots a_n$ are arbitrary n elements of G (not necessary different). Prove that there exist integers p, q where $1 \leqslant p \leqslant q \leqslant n$, s.t. $a_p a_{p+1} \ldots a_q = 1$.

Proof. Assume that for any $1 \leqslant p \leqslant q \leqslant n$, $ap \cdots a_q \neq 1$. It follows that $a_1, a_1a_2, \cdots, a_1 \cdots a_n$ are pairwise different. Since $|G| = n$, there exists k such that $\prod_{i=1}^k a_i = 1$, contradiction. □

7. For $\sigma \in \mathrm{Aut}(G)$, if $\forall g \neq 1, \sigma(g) \neq g$, then σ is called an automorphism with no fixed point. If for a finite group G there exists an automorphism σ with no fixed point and $\sigma^2 = 1$. Prove that G must be an abelian group with odd order.

Proof. (It is motivated by exercise 10.)

Since $\sigma^2 = 1$ and $\sigma(g) \neq g$ for all $g \neq 1$, there is $G = \{1\} \cup \{g_1, \sigma(g_1)\} \cup \cdots \cup \{g_n, \sigma(g_n)\}$ and so $|G|$ is odd.

For a fixed $g \in g$, let $k \in G$ with $k^2 = \sigma(g^{-1})g$. Since $|G|$ is odd, k exists. Then $\sigma(gk^{-1}) = \sigma(g)k^{-1} = gk^{-1}$ and so $g = k$. Therefore, for all $g \in G$, $\sigma(g) = g^{-1}$ and so G is abelian. □

Alternating proof. Define $\varphi : g \mapsto g^{-1}\sigma(g)$. Then φ is injective. Since $|G| < \infty$, φ is injective. Hence each element can be written in the form of $g^{-1}\sigma(g) := h$ and $\sigma(h) = h^{-1}$ for all $h \in G$. Therefore, $\sigma : g \mapsto g^{-1}$ is an automorphism and so G is abelian.

8. Let a, b be two elements of group G. If $aba = ba^2b, a^3 = 1$ and $b^{2n-1} = 1$ for some integer n, prove $b = 1$.

Proof. Note that $(aba^2)^{2n-1} = 1$, we have that $(ba^2)^{3n-3}aba^2 = 1$. Similarly, $(a^2ba)^{2n-1} = 1$ and so $(a^2b)^{3n-3}a^2ba = a^2(ba^2)^{3n-3}ba = 1$. It follows that $a^2(aba^2)^{-1}ba = b^{-1}a^2ba = 1$. Therefore, $b = a^2ba = aba^2b$ and $aba^2 = 1$. Then $ab = aba^2a = a$ and so $b = 1$. □

9. Let $A \leqslant G$, prove $C_GC_GC_G(A) = C_G(A)$.

Proof. Note that $A \subseteq C_G(C_G(A))$ and so $C_G(A) \supseteq C_G(C_G(C_G(A)))$. On the other hand, for any $b \in C_G(A)$, it is easy to show $bg = gb$ for all $g \in C_G(C_G(A))$ and so $b \in C_G(C_G(C_G(A)))$. □

10. Let G be a finite group with odd order, $\alpha \in \mathrm{Aut}(G)$ and $\alpha^2 = 1$. Let

$$G_1 = \{g \in G \mid \alpha(g) = g\}, G_{-1} = \left\{g \in G \mid \alpha(g) = g^{-1}\right\}$$

Prove: $G = G_1 G_{-1}$ **and** $G_1 \cap G_{-1} = 1$.

> Since $|G|$ is odd, for any $g \in G$ there exists h such that $h^2 = g$.

Proof. Since $|G|$ is odd, there exists k such that $k^2 = \sigma(g^{-1})g$. It is easy to verify that $\sigma(k^2) = k^{-2}$. Since $|\sigma(k^2)| = |k^{-2}| := m$, we have that $\sigma(k) = k^{-1} = (k^{-2})^{\frac{m+1}{2}}$. Therefore, $k \in G_{-1}$. It follows that $gk^{-1} \in G_1$ and now we finish the proof. □