4. Let H, K be subgroups of a finite group G with $K \subset N_H$. Show that $\#(HK) = \dfrac{\#(H)\#(K)}{\#(H \cap K)}$.

Proof. First, note that HK is a subgroup of G. For $h_1, h_2 \in H, k_1, k_2 \in K$, we have

$$(h_1k_1)(h_2k_2) = ((h_1k_1h_1^{-1})(h_1h_2))k_2 \in HK$$

because $h_1k_1h_1^{-1} \in H$. So HK is closed under multiplication. Also,

$$(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1})(kk^{-1}) = (k^{-1}h^{-1}k)k^{-1} \in HK$$

since $k^{-1}h^{-1}k \in H$. So HK is closed under inverses. Clearly, $1 = 1 \cdot 1 \in HK$, thus HK is a subgroup.

Next, observe that H is normal in HK and $H \cap K$ is normal in K (the intersection of subgroups is always a subgroup): for $h, h' \in H$, $k \in k$, and $g \in H \cap K$, we have

$$(hk)h'(hk)^{-1} = h(kh'k^{-1})h^{-1} \in H$$

since $kh'k^{-1} \in H$; $kgk^{-1} \in K$ because $g \in K$, and $kgk^{-1} \in H$ because $g \in H$ (and K normalizes H).

Now, we can define a map $\varphi : K/H \cap K \to HK/H$ by $kH \cap K \mapsto kH$. φ is a well-defined because if $k' \in kH \cap K$ then $k' = kh$ for some h, thus

$$\varphi(k'H \cap K) = k'H = khH = kH = \varphi(kH \cap K).$$

φ is also a homomorphism, since for $k \in K$ we have

$$\varphi((k_1H \cap K)(k_2H \cap K)) = \varphi(k_1k_2H \cap K) = k_1k_2H = k_1Hk_2H = \varphi(k_1H \cap K)\varphi(k_2H \cap K).$$

If $k \in K$ is such that $kH \cap K \in \ker(\varphi)$, then $\varphi(kH \cap K) = kH = H$; so k is in H, and therefore also in $H \cap K$. So φ is injective.

Finally, given any $hk \in HK$, we have

$$(hk)H = (hH)(kH) = H(kH) = kH = \varphi(kH \cap K)$$

thus φ is surjective.

Therefore, φ is an isomorphism, and so $K/H \cap K \cong HK/H$. Since G is finite, Lagrange's Theorem gives that $\#(HK) = \dfrac{\#(H)\#(K)}{\#(H \cap K)}$. □

7. Let G be a group such that $\mathrm{Aut}(G)$ is cyclic. Prove that G is abelian.

Proof. Denote by $\mathbf{c}_x$ the inner automorphism $y \mapsto xyx^{-1}$. Lang mentions that the association $x \mapsto \mathbf{c}_x$ is a homomorphism of G into its automorphism group (since $\mathbf{c}_x \circ \mathbf{c}_y(g) = (xy)g(xy)^{-1} = \mathbf{c}_{xy}(g)$). Clearly, the kernel of this map is the center Z of G, and its image is the subgroup I of inner automorphisms of G. So $G/Z \cong I$.

Subgroups of cyclic groups are cyclic, so I is cyclic and thus so is G/Z. Let g be such that gZ generates G/Z. Then for any $x, y \in G$ there exist $m, n \in \mathbb{Z}$ and $z, w \in Z$ such that $x = g^m z$ and $y = g^n w$. So

$$xy = (g^m z)(g^n w) = (g^m g^n)(zw) = (g^n g^m)(wz) = (g^n w)(g^m z) = yx$$

thus G is abelian.

□

9. (a) Let G be a group and H a subgroup of finite index. Show that there exists a normal subgroup N of G contained in H and also of finite index.

Proof. For each $g \in G$, let $T_g : G/H \to G/H$ denote the translation $S \mapsto gS$ for any coset S of H in G. First, we will show that T_g is a permutation of G/H. Let $x, y \in G$. If $T_g(xH) = T_g(yH)$, then $gxH = gyH$. So for all $h \in H$, there exists some $h' \in H$ such that $gxh = gyh'$, hence $xh = xh'$. So $xH \subseteq yH$. The symmetric argument shows that $yH \subseteq xH$, thus $xH = yH$ and so T_g is injective. Also, given any $x \in G$, we have $xH = g(g^{-1}x)H = T_g(g^{-1}x)$, thus T_g is surjective as well. So $T_g \in S_{G/H}$ (the group of permutations of G/H).

Define $\varphi : G \to S_{G/H}$ by $g \mapsto T_g$. φ is a homomorphism, since for any $x, y, z \in G$ we have

$$\varphi(xy)(zH) = T_{xy}(zH) = xyzH = x(yzH) = T_x \circ T_y(zH) = (\varphi(x) \circ \varphi(y))(zH).$$

If $g \in \ker \varphi$, then $T_g(H) = gH = H$, thus $g \in H$. So $\ker \varphi \subseteq H$. Therefore, $N = \ker \varphi$ is a normal subgroup of G contained in H. Also, $G/N \cong \operatorname{Im} \varphi \subseteq S_{G/H}$, and $\#(S_{G/H}) = \#(G : H)!$. Thus $\#(G : N) \leq \#(G : H)!$, hence N has finite index in G.

$\square$

(b) Let G be a group and let H_1, H_2 be subgroups of finite index. Prove that $H_1 \cap H_2$ has finite index.

Proof. Consider the map (of sets) $G/H_1 \cap H_2 \hookrightarrow G/H_1 \times G/H_2$ given by $gH_1 \cap H_2 \mapsto (gH_1, gH_2)$. If $gH_1 \cap H_2 = hH_1 \cap H_2$, then $g^{-1}h \in H_1 \cap H_2$, so $gH_1 = hH_1$ and $gH_2 = hH_2$, thus the map is well-defined. Similarly, if $(gH_1, gH_2) = (hH_1, hH_2)$ for some $g, h \in G$, then $g^{-1}h \in H_1$ and $g^{-1}h \in H_2$, hence $gH_1 \cap H_2 = hH_1 \cap H_2$. So the map is injective. Therefore, $(G : H_1 \cap H_2)$ must be finite, since the cardinality of the codomain is finite by assumption.

$\square$

15. Let G be a finite group operating on a finite set S with $\#(S) \geq 2$. Assume that there is only one orbit. Prove that there exists an element $x \in G$ which has no fixed point, i.e. $xs \neq s$ for all $s \in S$.

Proof. For any $s \in S$, we have $\dfrac{\#G}{\#G_s} = (G : G_s) = \#(Gs) = \#S$, so $\#G_s = \dfrac{\#G}{\#S}$. Suppose, for a contradiction, that each element $x \in G$ has a fixed point. Each stabilizer contains the identity, so by "inclusion exclusion" we have

$$\#G = \#S\frac{\#G}{\#S} = \sum_{s \in S} \frac{\#G}{\#S} = \sum_{s \in S} \#G_s \geq \#S + (\#G - 1).$$

The inequality is justified by the fact that, in summing the sizes of all the stabilizers, we count the identity element $\#S$ times and count every other element of G at least once, since each element stabilizes some element. This implies that $\#S \leq 1$, a contradiction. $\square$

16. Let H be a proper subgroup of a finite group G. Show that G is not the union of all the conjugates of H.

Proof. Let $g \in G$. For any $gh \in gH$, we have $(gh)H(gh)^{-1} = g(hHh^{-1})g^{-1} = gHg^{-1}$. Therefore, we have a surjection from the cosets of H in G onto the set of distinct conjugates of H in G, hence there are at most $(G : H) = \dfrac{\#G}{\#H}$ distinct conjugates of H. Each of these conjugates has size $\#H$ (since conjugation is a bijection) and contains the identity, so by "inclusion-exclusion" we have

$$\#\left(\bigcup_{g \in G} gHg^{-1}\right) \leq \frac{\#G}{\#H}(\#H - 1) + 1 = \#G - (G : H) + 1 \leq \#G - 2 + 1 = \#G - 1.$$

The second inequality follows from the fact that H is a proper subgroup, so it has index ≥ 2. Therefore, the union is strictly smaller than G. $\square$

17. Let X, Y be finite sets and let C be a subset of $X \times Y$. For $x \in X$, let $\varphi(x)$ be the number of elements $y \in Y$ such that $(x, y) \in C$. Verify that $\#(C) = \sum_{x \in X} \varphi(x)$.

Proof. Let $\mathbb{1} : X \times Y \to \{0,1\}$ be given by $\mathbb{1}(x,y) = \begin{cases} 1 & (x,y) \in C \\ 0 & \text{else} \end{cases}$. Then

$$\#(C) = \sum_{(x,y)\in X\times Y} \mathbb{1}(x,y) = \sum_{x\in X}\left(\sum_{y\in Y} \mathbb{1}(x,y)\right) = \sum_{x\in X} \varphi(x).$$

□

18. Let S, T be finite sets. Show that $\#(T^S) = (\#T)^{\#(S)}$.

Proof. A function $S \to T$ is defined uniquely by the image of each point in S. For each of the $\#(S)$ points in S, there are $\#(T)$ possible images. So the number of functions is $\prod_{s\in S} \#(T) = \#(T)^{\#(S)}$. □

19. Let G be a finite group operating on a finite set S.

(a) For each $s \in S$ show that $\sum_{t\in Gs} \dfrac{1}{\#(Gt)} = 1$.

Proof. For all $t \in Gs$, $Gt = Gs$, since the orbits partition S. So $\sum_{t\in Gs} \dfrac{1}{\#(Gt)} = \sum_{t\in Gs} \dfrac{1}{\#(Gs)} = \#(Gs)\dfrac{1}{\#(Gs)} = 1$. □

(b) For each $x \in G$ define $f(x)$ to be the number of elements $s \in S$ such that $xs = s$. Prove that the number of orbits of G in S is equal to $\dfrac{1}{\#(G)} \sum_{x\in G} f(x)$.

Proof. Let $\mathbb{1} : G \times S \to \{0,1\}$ be given by $\mathbb{1}(x,s) = \begin{cases} 1 & xs = s \\ 0 & \text{else} \end{cases}$. Since both S and G are finite,

$$\sum_{x\in G} f(x) = \sum_{x\in G}\sum_{s\in S} \mathbb{1}(x,s) = \sum_{s\in S}\sum_{x\in G} \mathbb{1}(x,s) = \sum_{s\in S} \#(G_s).$$

Since G is finite, $\#(Gs) = (G : G_s) = \frac{\#(G)}{\#(G_s)}$, so $\#(G_s) = \frac{\#(G)}{\#(Gs)}$. This gives

$$\frac{1}{\#(G)}\sum_{x\in G} f(x) = \frac{1}{\#(G)}\sum_{s\in S} \#(G_s) = \frac{1}{\#(G)}\sum_{s\in S} \frac{\#(G)}{\#(Gs)} = \sum_{s\in S} \frac{1}{\#(Gs)}$$

$$= \sum_{\mathcal{O}\in S/G}\sum_{s\in\mathcal{O}} \frac{1}{\#(Gs)} = \sum_{\mathcal{O}\in S/G} 1 = \#(S/G)$$

where S/G is the set of orbits of S under the action of G. □