Let p be a prime number. We use the additive notation here: for example px instead of x^p. We first reduce the problem to the case when for every a in A, $pa = 0$: Let $\phi : A \to A$ be the homomorphism $\phi(a) = pa$. Let B be the kernel of ϕ and C its image.

(a) Show that every subgroup of order p in A is contained in B, and every subgroup of index p contains C. Show that the orders of the groups B and A/C are equal.

The groups B and A/C are finite abelian groups with the property that every non-zero element has order p. (so in particular they are p-groups.) Groups of this form are called *elementary abelian groups.* Now It is enough to show the number of subgroups of order p in B and subgroups of index p in A/C are equal. Let

$$|B| = |A/C| = p^n.$$

(b) Show that in an elementary abelian group with p^n elements, every non-zero element generates a subgroup of order p, and therefore the number of subgroups of order p is $(p^n - 1)/(p - 1)$

(c) Show that in an elementary abelian group G with p^n elements, the number of subgroups of index p is $(p^n - 1)/(p - 1)$ in the following way: we have $G \cong \mathbf{Z}_p \oplus \cdots \oplus \mathbf{Z}_p$ (n copies), so the number of non-zero (and therefore onto) homomorphisms

$$G \to \mathbf{Z}_p$$

is $p^n - 1$. the kernel of any such homomorphism is a subgroup of index p, and conversely every subgroup H of index p can be obtained as a kernel of such a homomorphism because $G/H \cong \mathbf{Z}_p$. Fix H and show that the number of homomorphisms α as above whose kernel is H is $p - 1$ by showing α is determined by the image of any element which is not H.