No. 32. Let G be a group, let H be a subgroup, and let a and b be elements of G such that $aH = bH$. Then it follows that $HA^{-1} = Hb^{-1}$. Indeed, if $aH = bH$, then a and b lie in the same left coset, so $b = ah$ for some $h \in H$. Hence $b^{-1} = (ah)^{-1} = h^{-1}a^{-1}$. Since H is a subgroup, $h^{-1} \in H$, so $\mathrm{Hb}^{-1} = Ha^{-1}$.

No. 39. Let H be a subgroup of index 2 in G. Then H is normal. Indeed, the set of left cosets is a partition of G, containing exactly two elements, each a subset of G. One of these subsets is H and hence the other must be $G \setminus H$, the complement of H. The same applies to the set of right cosets. Thus the left and right cosets are the same.

No. 40. Let G be a group of order n and let g be an element of G. Then $g^n = e$. Indeed, by the theorem of Lagrange, the order of the cyclic subgroup $< g >$ generated by g, call it m, divides n. But m is also the smallest positive integer such that $g^m = e$. If $n = md$, it follows that $g^n = g^{md} = e$.

No. 35. Let G be a group and H a subgroup. The problem is to show that the number of left cosets of H is the same as the number of right cosets. Let G/H denote the set of left cosets of G and let $H\backslash G$ denote the set of right cosets of G. We will construct a bijective mapping ϕ from G/H to $H\backslash G$. Namely, if C is a left coset, then we claim that $C^{-1} := \{c^{-1} : c \in C\}$ is a right coset. Indeed, if $g \in C$, then $C = \{gh : h \in H\}$, so $C^{-1} = \{(gh)^{-1} = h^{-1}g^{-1} : h \in H\} = \{hg^{-1} : h \in H\} = Hg^{-1}$. The same argument shows that if C is a right coset, then C^{-1} is a left coset, so we also get a map $\psi \colon H\backslash G \to G/H$. Evidently $\phi \circ \psi = \mathrm{id}$ and $\psi \circ \phi = \mathrm{id}$, so both maps are bijective.

No. 46. Let G be a cylic group of order n. For each element g of G, let $\operatorname{ord} g$ denote the order of g, that is the smallest positive number m such that $g^m = e$, or, equivalently, the number of elements in the cyclic subgroup $\langle g \rangle$ generated by g. Let G_d be the subset of G consisting of those elements of order d. This is empty if d does not divide n, and is not empty otherwise. Thus the set of all G_d such that $d|n$ forms a partition of G into disjoint sets. Consequently, the number of elements in G is the sum of the numbers of elements in each G_d: $|G| = \sum_{d|n} |G_d|$. Now for each divisor d of n, by exercise 45, there is a unique subgroup H_d of order d, and furthermore H_d is cyclic and is the set of all elements such that $g^d = e$. Thus $G_d \subseteq H_d$, and in fact an element of H_d belongs to G_d if and only if it generates H_d. Since H_d is cyclic of order d, it is isomorphic to $\mathbf{Z}_d$, and has exactly $\phi(d)$ generators.

Thus $|G_d| = \phi(d)$. Returning to our formula, we find that

$$n = |G| = \sum_{d|n} |G_d| = \sum_{d|n} \phi(d).$$

No. 47. In fact we can easily prove a stronger form of the result, which is very useful.

Theorem Let G be a finite group of order n. Then the following conditions are equivlaent.

1. For every natural number m dividing n, the number of elements g of G such that $g^m = e$ is less than or equal to m.
2. For every natural number m dividing n, G has at most one (cyclic) subgroup of order m.
3. For every natural number m dividing n, G has at most most $\phi(m)$ elements of exact order m.
4. G is cyclic.

Proof: (1) implies (2). If H is a subgroup of order m, then every element h of H satisfies $h^m = e$, and of course H has m elements. If there were two such groups, there would consequenctly be more than m elements of G such that $g^m = e$.

(2) implies (3). If g has exact order m, it generates a cyclic subgroup H of order m, and this H has exactly $\phi(m)$ generators. Hence if there were more than $\phi(m)$ such elements, not all could generat H, and hence we would find another (cyclic) subgroup of order m.

(3) implies (4). Let $\psi(m)$ denote the number of elements of G which have exact order m. Since every element of G has some order dividing n, we get that $n = \sum_{m|n} \psi(m)$. On the other hand, we know that $n = \sum_{m|n} \phi(m)$. By assumption, $0 \leq \psi(m) \leq \phi(m)$ for all m. These equations together imply that $\psi(m) = \phi(m)$ for all m. In particular, $\psi(n) = \phi(n) \neq 0$. This implies that G contains an element of exact order n, hence is cyclic.

(4) implies (1). We did this a while ago.