1. Recall that for a finite group G, the exponent of the group, $\exp(G)$ is defined as

$$\exp(G) = \min\left\{m \geqslant 1 \,\middle|\, g^m = e, \text{ for all } g \in G\right\} = \operatorname{lcm}\left\{\operatorname{ord}(g) \,\middle|\, g \in G\right\}.$$

In this problem we will prove the following result:

LEMMA — Let G be a finite abelian group. Then $\exp(G) = |G|$ if and only if G is a cyclic group.

(a) Show that if G is a cyclic group then $\exp(G) = |G|$.

The proof of the other direction will take a bit longer.

(b) Suppose that g_i, $g_j \in G$ and that $\operatorname{ord}(g_i)$ and $\operatorname{ord}(g_j)$ are relatively prime. Explain why $\langle g_i \rangle \cap \langle g_j \rangle = \{e\}$.

(c) Conclude that in the situation of (b), if $g_i^m = g_j^n$ for some $m, n \in \mathbb{Z}$, we must have $g_i^m = e$ and $g_j^n = e$.

(d) Again with the hypothesis of (b), if g_i and g_j commute, show that $\operatorname{ord}(g_i g_j) = \operatorname{ord}(g_i)\operatorname{ord}(g_j)$.

(e) Suppose that $g \in G$ and that $p^e \mid \operatorname{ord}(g)$, where p is a prime. Show that G has an element of order exactly p^e. (HINT: An appropriate power of g will work.)

Now we suppose that $\exp(G) = |G|$, and let $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ be the prime factorization of $|G|$.

(f) Explain why for each j, $j = 1, \ldots, r$, there must be an element $g_j' \in G$ such that $p_j^{e_j} \mid \operatorname{ord}(g_j')$. (This will use the hypothesis that $\exp(G) = p_1^{e_1} \cdots p_r^{e_r}$.)

(g) Explain why for each j, $j = 1, \ldots, r$, there must be an element $g_j \in G$ such that $\operatorname{ord}(g_j) = p^{e_j}$.

(h) Assuming that G is abelian and that $\exp(G) = |G|$, show that G is cyclic. I.e., prove the other direction of the lemma.

(i) Compute $\exp(S_3)$, where S_3 is the symmetric group on three elements.

(j) Does the lemma hold for non-abelian groups?

REMARKS. (1) The lemma actually has a stronger form, which can be proved with only a minor change in the argument above : If G is an abelian group, then G has a cyclic subgroup of order $\exp(G)$. (2) If we are allowed to assume the structure theorem for finitely generated abelian groups (i.e., if you already know that theorem), then the lemma follows almost immediately from the structure theorem.

2. Find all monic irreducible polynomials of degree 3 in $\mathbb{F}_3[x]$. Check that the number of such polynomials agrees with the formula for N_3. (NOTE: There are 27 monic polynomials of degree 3 in $\mathbb{F}_3[x]$. However, 9 have constant term 0, and so obviously have $x = 0$ as a root, so there really are only 18 polynomials to check. Furthermore, for those 18 you only have to check whether or not $x = 1$ and $x = 2$ are roots, since you've already eliminated the possibility $x = 0$.)

3. The polynomial $q(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ is irreducible, and so $F = \mathbb{F}_2[x]/(q(x))$ is a field with $2^3 = 8$ elements (i.e, $F \cong \mathbb{F}_8$). Let α be the class of x in the quotient. Then the elements of F can be written as $a\alpha^2 + b\alpha + c$ with $a, b, c \in \mathbb{F}_2$.

(a) Write out the multiplication table for the nonzero elements of F. (To keep the answers uniform, use the order 1, α, $\alpha + 1$, α^2, $\alpha^2 + 1$, $\alpha^2 + \alpha$, and $\alpha^2 + \alpha + 1$ in the table.) You do not have to include all the details of your computations, but do include some sample multiplications to demonstrate how you carried out the calculations.

(b) By looking at your table find an element $\beta \in F^*$ of order 7, i.e., find a generator of the cyclic group F^*.

(c) The elements 1, α, and α^2 form a basis for F over $\mathbb{F}_2$. In this basis, write out the 3×3 matrix giving the action of $\sigma_2 \in \mathrm{Gal}(F/\mathbb{F}_2)$ on F.

(d) Check that the matrix you found in (c) has order 3, confirming in this case that $\mathrm{Gal}(F/\mathbb{F}_2)$ is a cyclic group.