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?

Solution.

(a) Suppose that G is cyclic of order m. As with every finite group, for every $g \in G$ we have $\operatorname{ord}(g) \mid |G| = m$. Since G is cyclic, it has a generator σ of order m. Therefore

$$\exp(G) = \operatorname{lcm}\Big\{\operatorname{ord}(g) \,\Big|\, g \in G\Big\} = m = |G|.$$

(b) Set $H_i = \langle g_i \rangle$ and $H_j = \langle g_j \rangle$. Then H_i and H_j are cyclic, with $|H_i| = \operatorname{ord}(g_i)$ and $|H_j| = \operatorname{ord}(g_j)$. By the hypothesis $\operatorname{ord}(g_i)$ and $\operatorname{ord}(g_j)$ are relatively prime, and so $\gcd(|H_i|, |H_j|) = 1$. Let $H = H_i \cap H_j$. Since H is a subgroup of H_i and H_j, we have $|H| \mid |H_i|$ and $|H| \mid |H_j|$, and therefore $|H| \mid \gcd(|H_i|, |H_j|) = 1$. Therefore $|H| = 1$ and $H = \{e\}$.

(c) If $g_i^m = g_j^n$, then this element is a member of both H_i and H_j, and so (by part (b)) equal to e.

(d) Since g_i and g_j commute, for any k we have $(g_i g_j)^k = g_i^k g_j^k$. Therefore if $k = \operatorname{ord}(g_i g_j)$ we have $e = (g_i g_j)^k = g_i^k g_j^k$, which we can rewrite as $g_i^k = g_j^{-k}$. By part (c) this means that $g_i^k = e$ and $g_j^k = e$. For any element g of a group, $g^m = e$ if and only if $\operatorname{ord}(g) \mid m$, so we conclude that $\operatorname{ord}(g_i) \mid k$ and $\operatorname{ord}(g_j) \mid k$. Since $\operatorname{ord}(g_i)$ and $\operatorname{ord}(g_j)$ are relatively prime this means that $\operatorname{ord}(g_i)\operatorname{ord}(g_j) \mid k$. On the other hand, if we set $m = \operatorname{ord}(g_i)\operatorname{ord}(g_j)$ then $g_i^m = e$ and $g_j^m = e$ so that $(g_i g_j)^m = g_i^m g_j^m = e$. This means that $k \mid \operatorname{ord}(g_i)\operatorname{ord}(g_j)$. Thus $\operatorname{ord}(g_i g_j) = k = m = \operatorname{ord}(g_i)\operatorname{ord}(g_j)$.

(e) Let $m = \operatorname{ord}(g)$ and write $m = p^e \cdot n$. Then $\operatorname{ord}(g^n) = p^e$, since $(g^n)^{p^e} = g^{p^e n} = g^m = e$, so that $\operatorname{ord}(g^m) \mid p^e$. On the other hand, if $1 \leqslant q < p^e$ then $(g^n)^q = g^{nq} \neq e$ since $nq < m$.

(f) Let $m = |G| = p_1^{e_1} \cdots p_r^{e_r}$. For any $g \in G$ we have $\operatorname{ord}(g) \mid m$, which implies that $\operatorname{ord}(g) = p_1^{f_1} \cdots p_r^{f_r}$ for the same primes $p_1, \ldots, p_r$, and with $0 \leqslant f_j \leqslant e_j$ for $j = 1, \ldots, r$. When computing the lcm of a set of numbers, the power of p_j (for a fixed j in the lcm is the maximum of the power that p_j appears in the factors. If $\exp(G) = m$, this means that for each j there must be some $g_j' \in G$ so that the power of p_j dividing $\operatorname{ord}(g_j')$ is exactly e_j.

(g) Applying (e) to g_j' we conclude that there is an element $g_j \in G$ with $\operatorname{ord}(g_j) = p_j^{e_j}$.

(h) We used the hypothesis that $\exp(G) = |G|$ to prove the existance of the elements $g_1, \ldots, g_r$ in (g). If G is commutative, then all the g_j commute, and so applying (d) repeatedly to $g_1, \ldots, g_r$ we see that $g = g_1 g_2 \cdots g_r$ has order $\operatorname{ord}(g_1)\operatorname{ord}(g_2) \cdots \operatorname{ord}(g_r) = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = |G|$. Since G has an element of order $|G|$, G is a cyclic group.

(i) S_3 has elements of order 1, 2, and 3. Therefore $\exp(G) = \operatorname{lcm}\{1, 2, 3\} = 6 = |S_3|$.

(j) The lemma does not hold for non-commutative groups. The non-commutative group S_3 is not cyclic (it is non-commutative!), but has exponent equal to its order.

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 $x = 0$.)

Solution. Here is a table of the 18 polynomials with no constant term, along with the status of each.

x^3+1 $x=2$ root	x^3+2 $x=1$ root	x^3+x+1 $x=1$ root	x^3+x+2 $x=2$ root	x^3+2x+1 irreducible	x^3+2x+2 irreducible
x^3+x^2+1 $x=1$ root	x^3+x^2+2 irreducible	x^3+x^2+x+1 $x=2$ root	x^3+x^2+x+2 irreducible	x^3+x^2+2x+1 irreducible	x^3+x^2+2x+2 $x=1,2$ roots
x^3+2x^2+1 irreducible	x^3+2x^2+2 $x=2$ root	x^3+2x^2+x+1 irreducible	x^3+2x^2+x+2 $x=1$ root	x^3+2x^2+2x+1 $x=1,2$ roots	x^3+2x^2+2x+2 irreducible

There are 8 irreducible monic cubic polynomials over $\mathbb{F}_3$. This agrees with the formula

$$N_3 = \frac{1}{3}\left(p^3 - p\right) = \frac{1}{3}\left(3^3 - 3\right) = \frac{1}{3} \cdot (27 - 3) = \frac{1}{3} \cdot 24 = 8.$$

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.

Solution.

(a) The multiplication table is

$\cdot$	$\mathbf{1}$	$\boldsymbol{\alpha}$	$\boldsymbol{\alpha+1}$	$\boldsymbol{\alpha^2}$	$\boldsymbol{\alpha^2+1}$	$\boldsymbol{\alpha^2+\alpha}$	$\boldsymbol{\alpha^2+\alpha+1}$
$\mathbf{1}$	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
$\boldsymbol{\alpha}$	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\boldsymbol{\alpha+1}$	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
$\boldsymbol{\alpha^2}$	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
$\boldsymbol{\alpha^2+1}$	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\boldsymbol{\alpha^2+\alpha}$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\boldsymbol{\alpha^2+\alpha+1}$	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

In working out the table, the key relation is that α satisfies the polynomial $q(x)$, that is, $\alpha^3+\alpha+1=0$, or $\alpha^3=-(\alpha+1)=\alpha+1$ (The last equality is because $-1=1$ in $\mathbb{F}_2$.) From this we also get $\alpha^4=\alpha\cdot\alpha^3=\alpha(\alpha+1)=\alpha^2+\alpha$. As usual we also have $2x=0$ for all $x\in\mathbb{F}_8$, since $\mathbb{F}_8$ has characteristic 2. Here are a few sample computations using these identities :

$$\begin{aligned}\alpha^2\cdot(\alpha+1) &= \alpha^3+\alpha^2=(\alpha+1)+\alpha^2=\alpha^2+\alpha+1;\\ (\alpha^2+\alpha)\cdot(\alpha+1) &= \alpha^3+2\alpha^2+\alpha=(\alpha+1)+0+\alpha=1;\\ (\alpha^2+\alpha+1)\cdot(\alpha^2+\alpha+1) &= \alpha^4+\alpha^2+1=(\alpha^2+\alpha)+\alpha^2+1=\alpha+1.\end{aligned}$$

(b) By our theorem from class $\mathbb{F}_8^*$ is a cyclic group of order 7. Since 7 is a prime number, any element of the group different from the identity is a generator. (In general, for a cyclic group of order m, any power of a generator relatively prime to m is also a generator.)

To demonstrate this, here are the powers of all the nontrivial elements in $\gamma\in\mathbb{F}_8^*$:

γ	γ^0	γ^1	γ^2	γ^3	γ^4	γ^5	γ^6
$\boldsymbol{\alpha}$	1	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1
$\boldsymbol{\alpha+1}$	1	$\alpha+1$	α^2+1	α^2	$\alpha^2+\alpha+1$	α	$\alpha^2+\alpha$
$\boldsymbol{\alpha^2}$	1	α^2	$\alpha^2+\alpha$	α^2+1	α	$\alpha+1$	$\alpha^2+\alpha+1$
$\boldsymbol{\alpha^2+1}$	1	α^2+1	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	$\alpha+1$	α^2	α
$\boldsymbol{\alpha^2+\alpha}$	1	$\alpha^2+\alpha$	α	$\alpha^2+\alpha+1$	α^2	α^2+1	$\alpha+1$
$\boldsymbol{\alpha^2+\alpha+1}$	1	$\alpha^2+\alpha+1$	$\alpha+1$	α	α^2+1	$\alpha^2+\alpha$	α^2

The fact that $\mathbb{F}_8^*$ is cyclic gives another way to work out the multiplication table in part (a). Pick a generator of $\mathbb{F}_8^*$ (say α) and write down its powers :

	0	1	2	3	4	5	6
$\boldsymbol{\alpha}$	1	α	α^2	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2+1

Then, we write out the multiplication table with the elements in the order we chose, and beside each one write which power of α it is. We then multiply, by adding exponents mod 7, to get the following table of exponents :

		0	1	3	2	6	4	5
	$\cdot$	$\mathbf{1}$	$\boldsymbol{\alpha}$	$\boldsymbol{\alpha+1}$	$\boldsymbol{\alpha^2}$	$\boldsymbol{\alpha^2+1}$	$\boldsymbol{\alpha^2+\alpha}$	$\boldsymbol{\alpha^2+\alpha+1}$
0	$\mathbf{1}$	0	1	3	2	6	4	5
1	$\boldsymbol{\alpha}$	1	2	4	3	0	5	6
3	$\boldsymbol{\alpha+1}$	3	4	6	5	2	0	1
2	$\boldsymbol{\alpha^2}$	2	3	5	4	1	6	0
6	$\boldsymbol{\alpha^2+1}$	6	0	2	1	5	3	4
4	$\boldsymbol{\alpha^2+\alpha}$	4	5	0	6	3	1	2
5	$\boldsymbol{\alpha^2+\alpha+1}$	5	6	1	0	4	2	3

Finally, we look at the exponent table and read off the corresponding element of the field, and fill it in to get the multiplication table.

(c) We have $\sigma_2(1) = 1^2 = 1 + 0 \cdot \alpha + 0 \cdot \alpha^2$, $\sigma_2(\alpha) = \alpha^2 = 0 + 0 \cdot \alpha + 1\alpha^2$, and $\sigma_2(\alpha^2) = \alpha^4 = \alpha^2 + \alpha = 0 + 1 \cdot \alpha + 1 \cdot \alpha^2$. Therefore in the basis $\{1, \alpha, \alpha^2\}$ the Frobenius automorphism σ_2 has matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

(d) Let M be the matrix from part (c). Computing over $\mathbb{F}_2$ we have

$$\begin{aligned} M^2 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \\ M^3 = M \cdot M^2 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \end{aligned}$$

Therefore σ_2 does have order 3 in $\mathrm{Gal}(\mathbb{F}_8/\mathbb{F}_2)$.