Exam 4

1) [40 points] Let $\sigma, \tau \in S_9$ be given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 4 & 1 & 9 & 6 & 3 & 2 & 8 \end{pmatrix} \quad \text{and} \quad \tau = (1\ 5)(3\ 2\ 4\ 7)(6\ 8\ 9).$$

(a) Write the complete factorization of σ into disjoint cycles.

Solution. $\sigma = (1\ 7\ 3\ 4)(2\ 5\ 9\ 8)(6)$. □

(b) Write τ is matrix form.

Solution.

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 2 & 7 & 1 & 8 & 3 & 9 & 6 \end{pmatrix}.$$

□

(c) Compute σ^{-1}. [Your answer *must* be in *disjoint cycles form*!]

Solution. $\sigma^{-1} = (4\ 3\ 7\ 1)(8\ 9\ 5\ 2)(6) = (1\ 4\ 3\ 7)(2\ 8\ 9\ 5)(6)$. □

(d) Compute $\sigma\tau$. [Your answer *must* be in *disjoint cycles form*!]

Solution. $\sigma\tau = (1\ 9\ 6\ 2)(3\ 5\ 7\ 4)(8)$ □

(e) Compute $\sigma\tau\sigma^{-1}$. [Your answer *must* be in *disjoint cycles form*!]

Solution. $\sigma\tau\sigma^{-1} = (7\ 9)(4\ 5\ 1\ 3)(6\ 2\ 8)$. □

(f) Write τ as a product of transpositions.

Solution. $\tau = (1\ 5)(3\ 7)(3\ 4)(3\ 2)(6\ 9)(6\ 8)$. □

(g) Compute $\mathrm{sign}(\tau)$.

Solution. $\mathrm{sign}(\tau) = (-1)^6 = 1$ [or $\mathrm{sign}(\tau) = (-1)^{9-3} = 1$]. □

(h) Compute $|\tau|$.

Solution. $|\tau| = \mathrm{lcm}(2, 4, 3) = 12$. □

2) Decide if True or False [*with justifications!*].

(a) [7 points] The set of real numbers $\mathbb{R}$ is a group with multiplication.

Solution. It's *False*. Clearly $e = 1$ [the identity] and there is no $x \in \mathbb{R}$ such that $x \cdot 0 = 1$. □

(b) [8 points] Every infinite group has an element of infinite order.

[**Hint:** Every ring is a group with addition. So, we have lots of examples of groups to think of.]

Solution. It's *False*. We have that $\mathbb{F}_2[x]$ is a group with *addition* [as $\mathbb{F}_2[x]$ is a ring] and in it every $f \in \mathbb{F}_2[x]$ is such that $f + f = 0$ [as $2 = 0$ in $\mathbb{F}_2$], so every non-zero element has order 2. Also note it is infinite [as any polynomial ring], as it contains x, x^2, x^3, etc. □

3) [15 points] Let G be a group [with *multiplicative* notation], m and n be positive integers such that $\gcd(m, n) = 1$, and $x \in G$ such that $x^m = x^n = e$ [where e is the identity element, i.e., the "1" of the group]. Prove that $x = e$.

[**Hint:** Use the *Extended Euclidean Algorithm* [or what I call *Bezout's Theorem*] for m and n. What is then x^1? [Think of two ways to find what it is. Of course, they have to be equal to each other, even if the *look* different.] Also, Corollary 2.50 might come handy.]

Proof. By *Bezout's Theorem*, we have that there are integers r and s such that $1 = rm + sn$. So, using Corollary 2.50 we get:

$$x = x^1 = x^{rm+sn} = x^{rm} \cdot x^{sn} = (x^m)^r \cdot (x^n)^s = e^r \cdot e^s = e \cdot e = e.$$

□

4) [15 points] Let $G = \mathbb{Q}(x, y) \setminus \{0\}$ [i.e., the set of rational functions on x and y and rational coefficients, except for 0] and

$$H = \{ax^m y^n \ : \ a \in \mathbb{Q} \setminus \{0\} \text{ and } m, n \in \mathbb{Z}\}.$$

[Note that m and n can be zero or negative!] Prove that H is a subgroup of G. [Of course, G and H are *multiplicative* groups, as they are not groups with respect to addition.]

Proof. First, observe that $1 \in H$, as $1 = 1 \cdot x^0 \cdot y^0$.

Now, let $ax^m y^n$ and $bx^r y^s$, such that $a, b \in \mathbb{Q} \setminus \{0\}$ and $m, n, r, s \in \mathbb{Z}$. Since $b \in \mathbb{Q} \setminus \{0\}$, we have that $b^{-1} \in \mathbb{Q} \setminus \{0\}$. So,

$$ax^m y^n \cdot (bx^r y^s)^{-1} = ax^m y^n \cdot b^{-1} x^{-r} y^{-s} = (ab^{-1}) x^{m-r} y^{n-s}.$$

Since $ab^{-1} \in \mathbb{Q} \setminus \{0\}$ and $(m - r), (n - s) \in \mathbb{Z}$, we have that $ax^m y^n \cdot (bx^r y^s)^{-1} \in H$.

Hence, H is a subgroup of G. □

5) [15 points] Let p be a prime and G be a group of order p^2. Prove that G has an element of order p.

[**Hint:** What are the possible orders of elements in G? What elements have order 1? You can also use Problem 2.40 [without solving it].]

Proof. Let $x \in G$. Since $p^2 > 1$, we may assume $x \neq e$ [i.e., not the identity element]. Hence, we have that $|x| \neq 1$. Since $|x| \mid |G| = p^2$, and p is prime, we have that $|x|$ is either p or p^2. If $|x| = p$, we are done. If not, then by Problem 2.40, we have that $|x^p| = p$. So, either x or x^p has order p. $\square$