1) Let $\sigma, \tau \in S_9$ be given by

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

(a) [5 points] Write the complete factorization of σ into disjoint cycles.

Solution. We have:

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

□

(b) [4 points] Compute σ^{-1}. [Your answer can be in any form.]

Solution. We have:

$$\sigma^{-1} = (1\,7\,2\,3\,5)(4\,9\,6\,8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 3 & 5 & 9 & 1 & 8 & 2 & 4 & 6 \end{pmatrix}.$$

□

(c) [4 points] Compute $\tau\sigma$. [Your answer can be in any form.]

Solution. We have:

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

□

(d) [4 points] Compute $\sigma\tau\sigma^{-1}$. [Your answer can be in any form.]

Solution. We have:

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

□

(e) [4 points] Write τ as a product of transpositions.

Solution. We have:

$$\tau = (1\,3)(1\,5)(2\,9)(2\,8)(2\,4)$$

□

(f) [4 points] Compute $\operatorname{sign}(\tau)$ and $|\tau|$.

Solution. We have:

$$\operatorname{sign}(\tau) = (-1)^5 = -1 \qquad \text{and} \qquad |\tau| = \operatorname{lcm}(3,4) = 12.$$

□

2) [10 points] Give the set of all solutions of the system

$$\begin{aligned} 3x &\equiv 2 \pmod{5}, \\ x &\equiv 3 \pmod{11}. \end{aligned}$$

Solution. Since $2 \cdot 3 \equiv 1 \pmod{5}$, we have that the system is equivalent to

$$\begin{aligned} x &\equiv 4 \pmod{5}, \\ x &\equiv 3 \pmod{11}. \end{aligned}$$

Now, $1 = 1 \cdot 11 - 2 \cdot 5$. So, the solutions are all integers of the form $x = 4 \cdot 1 \cdot 11 - 3 \cdot 2 \cdot 5 + 55k = 14 + 55k$, for $k \in \mathbb{Z}$. □

3) [10 points] Let G be an *Abelian* group [with multiplicative notation] and $a, b \in G$. Prove that

$$\langle a, b \rangle \stackrel{\text{def}}{=} \{a^m \cdot b^n \ : \ m, n \in \mathbb{Z}\}$$

is a subgroup of G.

Proof. Since $1 = 1 \cdot 1 = a^0 \cdot b^0$, we have that $1 \in \langle a, b \rangle$.

Now, let $x, y \in \langle a, b \rangle$, Then, there are $m, n, r, s \in \mathbb{Z}$ such that $x = a^m \cdot b^n$ and $y = a^r \cdot b^s$. Since G is Abelian, we have that

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

Since $m - r, n - s \in \mathbb{Z}$, we have that $xy^{-1} \in \langle a, b \rangle$. Hence, $\langle a, b \rangle$ is a subgroup of G. □

4) [10 points] Prove that if R is a domain, then $U(R[x]) = U(R)$. [Remember, $U(R)$ is the set of units of R, which I usually denote by $R^\times$. So, what you need to prove it that the units of the polynomial ring are the constant polynomials which are units of R.]

Solution. See solutions for Midterm 2. □

5) Examples:

(a) [5 points] Give an example of a finite *non-commutative* ring [with $1 \neq 0$]. [What examples of non-commutative rings do you know?]

Solution. Let

$$R \stackrel{\text{def}}{=} M_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \; : \; a, b, c, d \in \mathbb{F}_2 \right\}.$$

Then $|R| = 2^4 = 16$ and it's not commutative as

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \qquad \text{while} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

□

(b) [5 points] Give an example of an *infinite* ring R for which $2015 \cdot a = 0$ for all $a \in R$.

Solution. $R \stackrel{\text{def}}{=} (\mathbb{Z}/2015\mathbb{Z})[x]$ works [or even $\mathbb{F}_5[x]$]. □

6) [10 points] Let R be a [possibly non-commutative] ring [with $1 \neq 0$] and $a \in R$ such that there are $s, t \in R$ for which $sa = at = 1$. Prove that $s = t$.

Proof. We have:

$$s = s \cdot 1 = s(at) = (sa)t = 1 \cdot t = t.$$

□

7) Let $G = \{1, a, b\}$ be a group [with multiplicative notation] with exactly three elements. [So, 1, a and b are distinct and 1 is the identity of G.]

(a) [7 points] Prove that $ab = 1$. [**Hint:** Check that any other possibility would be impossible.]

Proof. Since G is closed under multiplication, we have that ab is either 1, a or b. If $ab = a$, then [since we have cancellation in groups] we have that $b = 1$, which is false. If $ab = b$, then we have that $a = 1$, which is also false. So, we must have that $ab = 1$. □

(b) [8 points] Prove that $a^2 = b$. [**Hint:** Check that any other possibility would be impossible.]

Solution. As above, we have that a^2 must be either 1, a or b. If $a^2 = 1$, by the previous item we have that $a^2 = ab$, and so $1 = b$, which is false. [Alternatively, the previous item says that $b = a^{-1}$, while $a^2 = 1$ says that $a^{-1} = a$, which would say $a = b$, which is a contradiction.] If $a^2 = a$, then $a = 1$ [cancellation again], but that is false. So, the only possibility is that $a^2 = b$. □

8) [10 points] Let R be a ring [with $1 \neq 0$] and suppose there is $a \in R$, with $a \neq 0$, such that $a^n = 0$ for some $n \in \mathbb{Z}_{\geq 1}$. Prove that there is $b \in R \setminus \{0\}$ such that $b^2 = 0$. [**Hint:** Break into n even or odd cases.]

Proof. Suppose $a \neq 0$ and $a^n = 0$ for some $n \in \mathbb{Z}_{\geq 1}$. Let n be the *minimal* positive integer with this property [using the *Well Ordering Principle*].

Suppose n is even, i.e., that $n = 2m$ for some $m \in \mathbb{Z}_{\geq 1}$. By the minimality of n, we have that $a^m \neq 0$ [as $m < n$]. So, taking $b = a^m$, we have that

$$b^2 = (a^m)^2 = a^{2m} = a^n = 0.$$

Now, suppose that n is odd. Note that $n \neq 1$, as $0 \neq a = a^1$. So, $n = 2m + 1$, with $m \in \mathbb{Z}_{\geq 1}$. Let $b = a^{n+1}$. Since $m > 0$, we have that $2m + 1 = m + (m + 1) > m + 1$. So, by the minimality of n, we have that $b = a^{m+1} \neq 0$. But,

$$b^2 = (a^{m+1})^2 = a^{2m+2} = a^{2m+1} \cdot a = a^n \cdot a = 0 \cdot a = 0.$$

□