1) Let $\sigma, \tau \in S_8$ be given by

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

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

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

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

Solution.

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

and

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

□

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

Solution.

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

□

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

Solution.

$$\begin{aligned} \tau^{-1}\sigma\tau &= (\tau^{-1}(1)\ \tau^{-1}(4)\ \tau^{-1}(5)\ \tau^{-1}(2))(\tau^{-1}(3))(\tau^{-1}(6)\ \tau^{-1}(8)\ \tau^{-1}(7)) \\ &= (5\ 1\ 2\ 4)(7)(3\ 8\ 6) \end{aligned}$$

□

(e) Write τ as a product of transpositions.

Solution.

$$\tau = (1\ 5)(1\ 2)(1\ 4)(3\ 7)(3\ 6)$$

□

2) Give all possible rational roots of

$$f(x) = x^5 + \frac{2}{3}x^4 - 2x^3 + 7x^2 - x + 1.$$

[Be careful! Don't be tricked!]

Solution. We cannot use the theorem for rational roots since f does not have integral coefficients. But, the roots of f and $3 \cdot f$ are the same, and $3 \cdot f$ has integral coefficients. Since the leading and constant coefficients are both 3, the possible rational roots [of f and $3 \cdot f$] are $\{\pm 1, \pm 3, \pm 1/3\}$. □

3) Let $f(x) = x^5 + 1$ and $g(x) = x^3 + 1$ in $\mathbb{F}_2[x]$. Write the GCD of f and g as a linear combination of them.

Solution. We have:

$$\begin{aligned} f(x) &= g(x) \cdot x^2 + (x^2 + 1), \\ g(x) &= (x^2 + 1) \cdot x + (x + 1), \\ (x^2 + 1) &= (x + 1)(x + 1) + 0. \end{aligned}$$

So, the GCD is $x + 1$. Then, we have [remembering that in $\mathbb{F}_2$ we have that $1 = -1$]:

$$\begin{aligned} (x + 1) &= g(x) + (x^2 + 1) \cdot x \\ &= g(x) + (f(x) + g(x) \cdot x^2) \cdot x \\ &= x \cdot f(x) + (x^3 + 1) \cdot g(x). \end{aligned}$$

□

4) Determine which of the following polynomials are irreducible in $\mathbb{Q}[x]$. [Justify!]

(a) $f(x) = x^3 - 3x^2 + 2x - 7$.

Solution. Reduce modulo 2. Then, $\bar{f}(x) = x^3 + x^2 + 1$. Since $\bar{f}(0) = \bar{f}(1) = 1$, $\bar{f}(x)$ has no roots, and since its degree is 3 it is irreducible. Hence, so is $f(x)$. □

(b) $f(x) = x^4 + 1$. [**Hint:** What happens with $f(x + 1)$?]

Solution. We have that $f(x + 1) = x^4 + 4x^3 + 6x^2 + 4x + 2$, and then Eisenstein's criterion [with $p = 2$] gives us that $f(x + 1)$ is irreducible, and hence so is $f(x)$. □

(c) $f(x) = 3x^7 + 6x^4 + 81x^3 - 9x + 1$ [**Hint:** Using a [tricky] HW problem makes this much easier!]

Solution. We have that $g(x) = x^7 + 9x^6 + 81x^4 + 6x^3 + 3$ is irreducible by Eisenstein's criterion [with $p = 3$], and hence, by the HW problem, we have that $f(x)$ is also irreducible. □

5) Let F be a field and $f, g \in F[x]$. Let also

$$I = \{f \cdot r + g \cdot s \ : \ r, s \in F[x]\}.$$

[Hence, I is a the set of all linear combinations of f and g.] Prove that there exist $d \in F[x]$ such that

$$I = \{d \cdot t \ : \ t \in F[x]\}.$$

[**Hint:** d is the GCD of f and g. Also, we've done the analogue of this for integers in class! The proof is the same.]

Proof. Let $d = \gcd(f, g)$.

[$\subseteq$] Let $f \cdot r + g \cdot s \in I$. Then, since $d \mid f, g$, we have that $d \mid (f \cdot r + g \cdot s)$, and hence there exists $t \in F[x]$ such that $f \cdot r + g \cdot s = d \cdot t$.

[$\supseteq$] By Bezout's Theorem, we have that $d = f \cdot r_1 + g \cdot s_1$ for some $r_1, s_1 \in F[x]$. Then, for all $t \in F[x]$, we have that $d \cdot t = f \cdot (r_1 \cdot t) + g \cdot (s_1 \cdot t)$, and hence $d \cdot t \in I$.

$\square$

6) Give example polynomials $f, g \in R[x]$, for some suitable ring R, such that f has more [distinct] roots in R than its degree, and g has degree greater than zero and yet is a unit. [**Hint:** Take $R = \mathbb{Z}/n\mathbb{Z}$ for the smallest $n > 1$ for which R is not a domain. The degrees of f and g can be low. Note that I showed you these examples in class!]

Solution. Let $R = \mathbb{Z}/4\mathbb{Z}$. Then, take $f = 2x$. Then, $f(0) = 0$ and $f(2) = 0$, so there are two roots, even though $\deg f = 1$.

Now, take $g = 2x + 1$. Then, $(2x + 1)(2x + 1) = 4x^2 + 4x + 1 = 1$, and hence g is a unit, even though $\deg g > 0$.

$\square$

7) Prove that there is no integer n whose square n^2 has its last two digits as 35. [**Hint:** If the last digit of n^2 is 5, what can we say about the last digit of n, i.e., what is the remainder of n when divided by 10? Then, what happens with n^2 modulo 100?]

Proof. We have that $n^2 \equiv 5 \pmod{10}$ if, and only if, $n \equiv 5 \pmod{10}$. We can find that by trial and error, as there are only 10 possibilities.

Then, $n = 10q + 5$ and hence $(10q + 5)^2 = 100q^2 + 100q + 25 \equiv 25 \pmod{100}$. Hence, if n^2 has last digit 5, the digit before that must be 2 [and hence never 3]. $\square$

8) Let F be a field with exactly 4 elements, say $F = \{0, 1, a, b\}$. [Hence, we are assuming that all these elements are distinct, e.g., $a \neq 1$, $b \neq 0$, etc.]

(a) Prove that $1 = -1$ in F. [**Hint:** Suppose not. Then, $-1 \neq 1$. Then, as $-1 \neq 0$, we can assume without loss of generality, that $-1 = a$. Show then that $b = -b$ by checking that no other element can be $-b$. This would mean that $b + b = b(1 + 1) = 0$. Since $b \neq 0$ and we are in a field, we would have that $1+1 = 0$, contradicting the assumption that $1 \neq -1$.]

Proof. Suppose that $1 \neq -1$. Then, we may assume, as in the hint, that $a = -1$, as if $-1 = 0$, then $1 = 0$, which is not true in a field, and if $b = -1$, we could switch the names of a and b.

Now, if $b + 0 = 0$, then $b = 0$, which is false. If $b + 1 = 0$, then $b = -1 = a$, which is also false. If $b + a = b - 1 = 0$, then $b = 1$, which is also false. Thus, the only possibility left is $b = -b$.

Then, $0 = b + b = b(1 + 1)$, which is a contradiction as $b, (1 + 1) \neq 0$. Therefore, we must have that $1 = -1$. □

(b) Prove that $b = a + 1$. [**Hint:** Can $a + 1$ be any other element? You need to use (a)!]

Proof. If $a + 1 = 0$, then $a = -1 = 1$, which is false. If $a + 1 = 1$, then $a = 0$, which is false. If $a + 1 = a$, then $1 = 0$, which is also false. Therefore, the only possibility left is $a + 1 = b$. □

(c) Prove that if $b = a^2$. [**Hint:** Can a^2 be any other element? You need to use (a) and the fact that $xy = 0$ implies that either $x = 0$ or $y = 0$.]

Proof. If $a^2 = a \cdot a = 0$, then $a = 0$, which is false.

If $a^2 = 1$, then $a^2 - 1 = (a - 1)(a + 1) = 0$, i.e., $a = 1$ or $a = -1$. Since, $1 = -1$, this would mean that $a = 1$, which is false.

If $a^2 = a$, then $a^2 - a = a(a - 1) = 0$. Thus, either $a = 0$ or $a = 1$, and both are false.

Thus, $a^2 = b$ is the only possibility. □

(d) Prove that a is a root of $x^2 + x + 1 \in F[x]$. [Use the previous items.]

Proof. We have that $a^2 + a + 1 = a^2 + (a + 1) = b + b = b(1 + 1) = b \cdot 0 = 0$. □