Final Solutions

1) [10 points] Use the *Extended Euclidean Algorithm* to write the GCD of

$$\begin{aligned} f(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + 1, \text{ [notice, no } x^1\text{!]} \\ g(x) &= x^4 + x^3 \end{aligned}$$

in $\mathbb{F}_2[x]$ [*not in* $\mathbb{Q}[x]$*!*] as a linear combination of themselves. *Show the computations explicitly!* [**Hint:** You should get $x+1$ for the GCD!]

Solution. We have:

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

So, the GCD is $x+1$, and

$$\begin{aligned} x+1 &= g + (x^2+1)(x^2+x+1) \\ &= g + (f + g(x^2+1))(x^2+x+1) \\ &= (x^2+x+1)f + (x^4+x^3+x)g. \end{aligned}$$

□

2) [16 points] Determine if the following polynomials are irreducible or not in $\mathbb{Q}[x]$. [Justify!]

(a) $f(x) = x^{30} - 13x^{17} + 10x^6 + 8x^3 - 5x - 1$

Solution. We have, by trying the rational root test, that $f(1) = 0$, so $(x-1)$ is a proper factor and hence $f(x)$ is *reducible.* □

(b) $f(x) = 3x^5 + 8x^4 - 14x^3 - 6x^2 - 2x + 14$

Solution. By Eisenstein's Criterion for $p = 2$, we have that $f(x)$ is *irreducible.* □

(c) $f(x) = 7x^3 - 4x + 16$

Solution. Reducing modulo $p = 3$, we get $x^3 - x + 1$, which has no root in $\mathbb{F}_3$. Since it has degree 3 and no root, it is irreducible in $\mathbb{F}_3[x]$, so *irreducible* in $\mathbb{Q}[x]$. □

(d) $f(x) = x^{200} + 2x^{100} + 1$

Solution. We have that $f(x) = (x^{100} + 1)^2$. So, it is *reducible*. ☐

3) [15 points] Let $\sigma, \tau \in S_9$ be given by

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

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

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

(b) Compute $\tau\sigma$. [Your answer can be in matrix or disjoint cycles form.]

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

(c) Compute $\sigma\tau\sigma^{-1}$. [Your answer can be in matrix or disjoint cycles form.]

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

(d) Write τ as a product of transpositions.

Solution. $\tau = (1\;2)(1\;3)(1\;5)(4\;9)(4\;8)$. ☐

(e) Compute $\text{sign}(\tau)$.

Solution. $\text{sign}(\tau) = (-1)^5 = -1$. ☐

4) [15 points] Compute the order of the following group elements [remember $|g|$ denotes the order of g]:

(a) $|[6]|$ in $\mathbb{I}_{15}$;

Solution. We have:

$$\begin{aligned} 1 \cdot [6] &= [6] \neq 0, \\ 2 \cdot [6] &= [12] \neq 0, \\ 3 \cdot [6] &= [18] = [3] \neq 0, \\ 4 \cdot [6] &= [24] = [9] \neq 0, \\ 5 \cdot [6] &= [30] = 0. \end{aligned}$$

So, $|[6]| = 5$. ☐

(b) $|[3]|$ in $U(\mathbb{I}_{11})$ [i.e., in the group of units of $\mathbb{I}_{11}$];

Solution. We have:

$$\begin{aligned}
[3]^1 &= [3] \neq 1, \\
[3]^2 &= [9] \neq 1, \\
[3]^3 &= [27] = [5] \neq 1, \\
[3]^4 &= [3] \cdot [5] = [15] = [4] \neq 1, \\
[3]^5 &= [3] \cdot [4] = [12] = 1.
\end{aligned}$$

□

(c) $|-7|$ in $\mathbb{Z}$;

Solution. Since for all positive integer n we have $n \cdot 7 \neq 0$, we have that n has infinite order. □

(d) $|(2\ 3\ 7)(1\ 5)(6\ 4)|$ in S_9

Solution. We have $|(2\ 3\ 7)(1\ 5)(6\ 4)| = \operatorname{lcm}(3, 2, 2) = 6$. □

5) [14 points] Examples:

(a) Give an example of an *infinite* integral domain R for which $14 \cdot a = 0$ for all $a \in R$.

Solution. Either $\mathbb{F}_2[x]$ or $\mathbb{F}_7[x]$. [$\mathbb{I}_{14}[x]$ is not a domain.] □

(b) Give an example of a field F that contains $\mathbb{C}$ properly [i.e., $\mathbb{C} \subseteq F$, but $F \neq \mathbb{C}$].

Solution. $F = \mathbb{C}(x)$. □

6) [10 points] Let G be an *Abelian* group [using multiplicative notation]. Let n be a [fixed!] integer and consider

$$H \overset{\text{def}}{=} \{x \in G \ : \ x^n = 1\}.$$

Prove that H is a subgroup of G. *Point out where, if ever, you've used the fact that G is Abelian!* [If never, do say so!]

Proof. We have that $1^n = 1$, so $1 \in H$.
If $x, y \in H$, then $x^n = y^n = 1$. Then, *since G is Abelian*, we have that $(xy)^n = x^n y^n = 1 \cdot 1 = 1$.
Finally, if $x \in H$, then $x^n = 1$. Thus, $(x^{-1})^n = (x^n)^{-1} = 1^{-1} = 1$.
So, H is a subgroup of G. □

7) [10 points] Let G be a group [with multiplicative notation] of order 12, *not cyclic*, and suppose that $g^6 \neq 1$ for some $g \in G$. Find $|g|$.

Proof. We know that $|g| \mid |G| = 12$. So, $|g| \in \{1, 2, 3, 4, 6, 12\}$. Since $|g|^6 \neq 1$, we can discard order 1, 2, 3 and 6. So, it is either of order 4 or order 12. If $|g| = 12$, then $\langle g \rangle = G$ [as it has 12 elements], and G would be cyclic. Since it is not, we must have that $|g| = 4$. $\square$

8) [10 points] Let R be a ring for which $(a+b)^2 = a^2 + b^2$ for all $a, b \in R$. Prove that for all $c \in R$, we have that $2 \cdot c = 0$ [i.e., $c + c = 0$].
[**Hint:** What *should* $(a+b)^2$ be equal to?]

Proof. Since R is a commutative ring, we have that

$$(c+1)^2 = c^2 + 2c + 1.$$

But, by assumption, $(c+1)^2 = c^2 + 1$. Hence, $2c = 0$. $\square$