Final (Take Home)

You must upload the solutions to this exam by 11:59pm on Thursday 07/02. Since this is a take home, I want all your solutions to be neat and well written.
You can look at your notes, class discussions on SMC, *our* book, our videos and solutions posted by me, but you cannot look at any other references (including the Internet) and you cannot discuss this with *anyone*!
You can use a computer only to check your answers, as **you need to show work in all questions**.

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

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

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!]

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

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

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

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

(d) $f(x) = x^{200} + 2x^{100} + 1$ [**Hint:** $200 = 2 \cdot 100$.]

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.

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

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

(d) Write τ as a product of transpositions.

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

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

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

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

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

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

5) [14 points] Examples:

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

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

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

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

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!]

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 $|g|$.

8) [10 points] Let R be ring [you may assume commutative, but it is not necessary] 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* $(c+1)^2$ be equal to?]