The point values add up to 106. This is an 120-minute exam, so the point values double as time recommendations (e.g, 8 minutes on an 8-point problem).

You must justify/show work for all answers.

1. (8 points)

(a) What is an *ideal*? Carefully state a theorem involving ideals.

(b) What does *kernel* mean? Carefully state a theorem involving kernels.

2. (20 points) *True or False?*

(a) If $f(x), g(x) \in \mathbb{Q}[x]$ and $x \cdot f(x) + (x^2 + x) \cdot g(x) = \frac{1}{3}x$, then the gcd of $f(x)$ and $g(x)$ is 1.

(b) The set $D = \{\frac{a}{2^k} : k \in \mathbb{Z}_{\geq 0}\}$ (called the *dyadic rationals*, in case you're curious) is a subfield of $\mathbb{Q}$.

(c) There are at least two irreducible polynomials in $\mathbb{Z}_2[x]$ of degree three.

(d) There are at least five irreducible polynomials in $\mathbb{R}[x]$ of degree three.

(e) $\mathbb{Q}(i)$ is isomorphic to $\mathbb{C}$ as a field. (Here, i represents a root of the polynomial $x^2 + 1$.)

3. (14 points) Prove that

$$N \trianglelefteq G, \quad G/N \text{ abelian} \quad \not\Rightarrow \quad G \text{ abelian}.$$

You can use the example of $A_n \leq S_n$ if you check all the relevant properties.

4. (12 points) Let $G = \mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$, and consider the subgroup $H = \{(6b, 12b) : b \in \mathbb{Z}\} \leq G$.

(a) Is H a cyclic group?

(b) Describe the elements of G/H and give two examples of distinct elements.

(c) Is G/H a group? (And if so, under what operation?)

(d) For what integers $a \in \mathbb{Z}$ are the cosets $(0, a) + H$ and $(-18, 1) + H$ equal?

(e) If $\alpha = (1, 0) + H$ and $\beta = (-2, -4) + H$, what are their additive orders?

EXAM CONTINUES ON REVERSE.

5. (8 points) Let A, B, and C be multiplicative groups, let $f : A \to B$ and $g : A \to C$ be group homomorphisms such that $\ker f \cap \ker g = \{1\}$. Let $F : A \to B \times C$ be defined by $F(a) = \big(f(a), g(a)\big)$.

(a) Show that $\ker F = \{1\}$.

(b) Find a subgroup of $B \times C$ that is isomorphic to A.

6. (12 points) As usual, let $\langle r \rangle$ denote the ideal generated by an element r in a ring R.

(a) What is $\langle 5 \rangle$ in $\mathbb{Z}$?

(b) What is $\langle 5 \rangle$ in $\mathbb{C}$?

(c) List two quadratic polynomials contained in $\langle x - 1 \rangle$ in $\mathbb{Z}[x]$.

(d) If I give you a complicated polynomial in $\mathbb{Z}[x]$, give a *simple* way to decide whether it is in that ideal. Example: $f(x) = 129x^7 - 12x^4 + 35x - 200$.

7. (16 points) Let $p(x) = x^3 + 5$ and let $E := \mathbb{Q}[x]/\langle p(x) \rangle$.

(a) Carefully explain how you know that E is a field, describing what major results you are quoting.

(b) Writing u for the equivalence class of x in E (i.e., $u = [x] = x + \langle p(x) \rangle$), explain why every element of E can be written in a unique way in the form $au^2 + bu + c$ for $a, b, c \in \mathbb{Q}$.

(c) Reduce the element $(1 + u^2)^2 \in E$ into that form.

(d) Do the same for the element $\frac{1}{1+u} \in E$.

8. (16 points) Let $q(x) = x^4 + 9x^2 + 12 \in \mathbb{Z}_{29}[x]$, and let $R = \mathbb{Z}_{29}[x]/\langle x^2 \rangle$.

(a) Explain steps that would suffice to determine whether $q(x)$ is irreducible in $\mathbb{Z}_{29}[x]$.

(b) Compute $d(x) = \gcd(x^2, q(x))$ and express it in the form $d(x) = u(x)x^2 + v(x)q(x)$ for $u(x), v(x) \in \mathbb{Z}_{29}[x]$.

(c) Does (the equivalence class of) $q(x)$ have a multiplicative inverse in R?

(d) Find zero divisors in R; that is, find nonzero elements whose product is zero. Is R a field?

END OF EXAM

EXTRA CREDIT: For a group G, let $Z(G)$ denote its *center*: the set of all elements that commute with everything in G. Let the dihedral group D_4 be generated by two elements, a rotation a and a flip b, as usual. Prove first that $Z(D_4) = \{e, a^2\}$, and then that $D_4/Z(D_4) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.