MAT 3530: Algebra **Name:** _____

Final Exam: take-home portion.
Due at the beginning of the in-class final exam on May 1, 2012.
Solutions must be typeset in Latex.

You are expected to work on this exam alone and to refrain from talking about the exam to anyone except the professor until the time and date when it is due. You may use your own notes and any published materials that you like. Published sources (whether hard-copy or on the Web) must be appropriately cited!

Your signature below attests to a pledge that you have done the exam according to the above instructions. (Please attach this cover page to your solutions.)

Signature:_____

1. Find all subgroups of D_6, the group of isometries of a regular hexagon. State which subgroups are normal and which ones are conjugate to each other. Justify your answers. Give a minimal set of generators for each subgroup. Present your final answer with groups listed in order from smallest (that would be the trivial group, consisting only of the identity - don't forget that one!) to the largest (that would be the entire group D_6 - don't forget that one, either!) and each set of conjugate subgroups listed together on a separate line. Finally, state which of these subgroups is the center, $C(D_6)$.

2. Let R be a Euclidean domain, and let $r_1, r_2, r_3, \ldots r_n$ be (distinct) elements of R. Prove that there are elements $a_1, a_2, a_3, \ldots a_n$ such that $d = a_1r_1 + a_2r_2 + a_3r_3 + \cdots + a_nr_n$ is the greatest common divisor (defined up to multiplication by units) of $r_1, r_2, r_3, \ldots r_n$ (in the sense that $d \mid r_i$ for $i = 1, 2, 3, \ldots, n$ – that is, d is a common divisor – and, in addition, if d' is any other common divisor, then $d' \mid d$). Prove this from scratch, assuming nothing except the definitions. (Hint: This does *not* require proof by induction!)

3. Let R be a Euclidean domain.

   (a) Prove that every ideal of R is principle. (Hint: Generalize the proof of Theorem 6.3.)

   (b) By the result of part (a), since the ring of polynomials with rational coefficients, $\mathbb{Q}[x]$, is Euclidean, all of its ideals are principle. What single monic polynomial generates the ideal $(x^2 - 1, x^3 - 1)$ generated by the two polynomials $x^2 - 1$ and $x^3 - 1$?

   (c) By the result of part (a), since the ring of Gaussian integers, $\mathbb{Z}[i]$, is Euclidean, all of its ideals are principle. What single Gaussian integer $a + bi$ with $a > 0$ and $b \geq 0$ generates the ideal $(2, 1 + i)$?

4. Prove or give a counterexample: For all integers m and n, if there exist integers q and r such that $n = qm + r$ and $r \mid m$, then r is the greatest common divisor of m and n. (Disregard whether r is positive or negative; we consider the GCD to be defined only up to units.)

5. Let $\omega = e^{\frac{2\pi i}{3}}$. Let $\mathbb{R}[\omega]$ denote the ring generated by adjoining ω to $\mathbb{R}$. (That is, $\mathbb{R}[\omega]$ is the smallest subring of the complex numbers containing both the field of real numbers and ω.) Prove that $\mathbb{R}[\omega] = \mathbb{R}[x]/(x^2 + x + 1)$. (Hint: The map $\phi : \mathbb{R}[x] \to \mathbb{R}[\omega]$ defined by $\phi(P(x)) = P(\omega)$ is clearly an epimorphism. Explain briefly why this is so, and compute $Ker(\phi)$.)