Answer **four** problems. (If you turn in more, the first four will be graded.) Put your answers in numerical order and circle the numbers of the four problems below your name. Within reason, you may quote theorems as long as you state them clearly.

Name: ______________________________

Problems to be graded: 1 2 3 4 5 6

1. (10 points) Let D be a positive integer such that $D \equiv -1 \pmod 4$. Define $\omega = \frac{1+\sqrt{-D}}{2}$, $R = \{a + b\omega : a, b \in \mathbf{Z}\}$. For $a \in R$ define $N(a) = a\overline{a}$, where $\overline{a}$ is the complex conjugate of a.
   (a) (2 points) Prove that R is a subring of the field $\mathbf{C}$ of complex numbers.
   (b) (2 points) Prove that for all $a \in R$ we have $N(a) \in \mathbf{Z}_{\geq 0}$.
   (c) (3 points) Prove that for all $\alpha, \beta \in R$ we have $N(\alpha\beta) = N(\alpha)N(\beta)$.
   (d) (3 points) Let $a \in R$. Prove that a is a unit if and only if $N(a) = 1$.
2. Let F be a field and let V be a vector space over F. Prove that V has a basis. (You may not assume that V is finite dimensional).
3. Which of the following polynomials are irreducible? Explain.
   (a) (3 points) $X^4 + X^2 + 1$ in $\mathbf{F}_2[X]$ (here $\mathbf{F}_2$ is the field with 2 elements);
   (b) (3 points) $X^3 + X + 1$ in $\mathbf{R}[X]$ (here $\mathbf{R}$ is the field of real numbers);
   (c) (4 points) $X^6 + 14X^2 + 21X + 35$ in $\mathbf{Q}[X]$ (here $\mathbf{Q}$ is the field of rational numbers).
4. Let R be a ring with identity, and let M be a (left) R-module. Let N be a submodule of M. Prove that M/N is a (left) R-module.
5. Find representatives of every similarity class of 6×6 matrices with real coefficients whose minimal polynomial is $(x + 2)^2(x - \sqrt{3})^2$.
6. Let F/K be a field extension.
   (a) (3 points) Define what it means to say that $\theta \in F$ is *algebraic* over K.
   (b) (7 points) Prove that if $\theta \in F$ is algebraic over K, then the smallest subring $K[\alpha]$ of F containing K and α is a field, and it is isomorphic to $K[x]/(p(x))$ for some polynomial $p(x) \in K[x]$.