# Math 422 2011 Assignment 4

April 4$^{\text{th}}$, 2011

Answer all questions and give complete reasons and checks for your answers. Please do not erase anything, just put a line through your work and continue; you cannot lose marks for anything you write. The parts of the questions are weighted as shown and can be answered in any order. Feel free to use Maple to make your calculations easier.

1. (a) You should each choose $m(x)$ as a different irreducible monic cubic polynomial in $\mathbb{Q}[x]$ (with all non-zero coefficients) which satisfies Eisenstein's criteria and verify that the rational roots theorem also shows that $m(x)$ is irreducible. [2]

   (b) Use the method described in class to find the radical form of two roots, one of which is real. Verify that both roots satisfy the relation for $\alpha^3$ formed from $m(\alpha) = 0$. [5]

   (c) Let $\alpha$ be any root of $m(x) = 0$. Find the inverse of $2\alpha^2 - \alpha + 3$ in $\mathbb{Q}[\alpha]$ in terms of $\alpha$ using the polynomial Euclidean algorithm. Check using Maple or your calculator that the decimal values agree for your real root. [5]

2. What is the minimal polynomial of $c - \sqrt{a + \sqrt{b}}$? (where $a$, $b$ and $c$ are non-zero digits in your registration number). What is the largest number of zero coefficients that could exist in the polynomial answer for this question? [4]

3. (a) Find a primitive element for the quadratic irreducible in $\mathbb{Z}_5[x]$ you selected and list the other elements as powers of it. [4]

   (b) Prove that every non-zero element in a Galois field has a smallest power that equals unity (its order) and that each element's order must be a divisor of $q - 1$ in $GF(q)$. What is the splitting field of $x^q - x$ in $GF(q)$? [5]