189-235A: Basic Algebra I
Assignment 5
Due: Thursday, October 20

1. Perform the division algorithm for dividing $f(x) = 3x^4 - 2x^3 + 6x^2 - x + 2$ by $g(x) = x^2 + x + 1$ in $\mathbf{Q}[x]$. (I.e., find polynomials $q(x)$ and $r(x)$ with $\deg(r) < \deg(g)$ satisfying $f = gq + r$.

2. Same question as 1, with $f(x) = x^5 - x + 1$ and $g(x) = x^2 + x + 1$ in $\mathbf{Z}_2[x]$.

3. Let $f : \mathbf{Z}[x] \to \mathbf{Z}$ be the function which to any polynomial $p(x) = a_0 + a_1 x + \cdots + a_d x^d$ associates its constant term a_0: $f(p) = a_0$. Show that f is a homomorphism of rings.

4. Find the gcd of $x^4 - x^3 - x^2 + 1$ and $x^3 - 1$ in $\mathbf{Q}[x]$ using the Euclidean algorithm.

5. Find the gcd of $x^4 + 3x^3 - 2x + 4$ and $x^2 + 1$ in $\mathbf{Z}_5[x]$ using the Euclidean algorithm.

6. Let $\mathbf{C}$ denote the field of complex numbers, and let $\overline{z} = a - bi$ denote as usual the complex conjugate of the complex number $z = a + bi$. Let H be the subset of $M_2(\mathbf{C})$ consisting of matrices of the form

$$\begin{pmatrix} z_1 & z_2 \\ -\overline{z_1} & \overline{z_2} \end{pmatrix},$$

where z_1 and z_2 are complex numbers. Show that H is a subring of $M_2(\mathbf{C})$.

7. Show that the ring H of exercise 6 is a non-commutative ring in which every non-zero element has a multiplicative inverse. (In other words, H is a non-commutative field.) The ring H is called the field of *quaternions*.

The next few questions are optional.

8. Let H' be the set of all expressions of the form $a+bi+cj+dk$, where a, b, c and d are real numbers, and i, j, k are formal variables. Define a multiplication on H' by combining the usual rules for addition and multiplication of real numbers with the rules

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad ki = -ik = j, \quad jk = -kj = i.$$

Show that H' is isomorphic to the ring H of exercise 7. (So from now on, we will write H instead of H'.)

9. Let H be the ring of real quaternions introduced in the previous exercise. A quaternion is said to be *integral* if it is of the form $a1 + bi + cj + dk$, where a, b, c, d are *integers*. Let R be the set of integral quaternions. Show that R is a subring of H.

10. Define a "complex conjugation" on H by the rule

$$\overline{a1 + bi + cj + dk} := a1 - bi - cj - dk.$$

Show that if α and β are two quaternions, then

$$\overline{\alpha\beta} = \overline{\beta} \cdot \overline{\alpha}.$$

(Note the change in the order of multiplication!)

11. If α belongs to H, define $||\alpha|| := \alpha\overline{\alpha}$. Show that if $\alpha = a1 + bi + cj + dk$, then

$$||\alpha|| = a^2 + b^2 + c^2 + d^2.$$

Note in particular that if α belongs to the ring R of integral quaternions, then $||\alpha|| \in \mathbf{Z}$.

12. Show that $||\alpha\beta|| = ||\alpha|| \cdot ||\beta||$. (Remember in your proof that multiplication in H is not commutative!)

13. Using 12, show that, if m and n are integers which can be expressed as a sum of 4 integer squares, then their product mn can also be expressed as a sum of four integer squares. Use your proof to express $161 = 7 \cdot 23$ as a sum of four squares.

This last exercise illustrates the usefulness of the ring R for number theory, and in particular for the study of representations of integers as sums of four squares. A deeper study of the ring theoretic structure of R leads to the following beautiful theorem of Lagrange: *Every positive integer can be expressed as a sum of four squares.* You should try to test this theorem empirically to get a feeling for what it says. Try also to find a proof!