Problem Set 5 (Due Friday, October 11)

(39) These are the problems carried over from the previous problem set.
   (a) In the ring \( \mathbb{Z}[i] \), use the Euclidean algorithm to find the GCD \( g_2 \) of \( 1 + 13i \) and 85. Find Gaussian integers \( x \) and \( y \) such that \( (1 + 13i)x + 85y = g_2 \).
   (b) In the ring \( \mathbb{Q}[i] \), use the Euclidean algorithm to find the GCD \( g_3 \) of \( t^3 + t \) and \( t^4 - 1 \). Find polynomials \( x(t) \) and \( y(t) \) such that \( (t^3 + t)x(t) + (t^4 - 1)y(t) = g_3 \).

(40) (a) Use the Euclidean algorithm to find polynomials \( f(t) \) and \( g(t) \) in \( \mathbb{Q}[t] \) such that
   \[ f(t)(3t^2 - 3t - 1) + g(t)(t^3 - 2) = 1. \]
   (b) Find rational numbers \( a, b, c \) such that
   \[ (3\sqrt[3]{4} - 3\sqrt[3]{2} - 1)^{-1} = a\sqrt[3]{4} + b\sqrt[3]{2} + c. \]

   Now you know how to rationalize denominators for algebraic numbers of degree greater than 2!

(41) Let \( R \) be an integral domain and let \( I \) be a nonzero ideal of \( R \). Cancelled, because problem was done in class.
   (a) Draw arrows indicating which implications exist between the following concepts. You need not provide proofs or counterexamples:
      \[ \begin{array}{c|c}
      \text{I is prime} & \text{I is maximal} \\
      \text{I is of the form \{f\} for \( f \) irreducible} & \text{I is of the form \{f\} for \( f \) prime} \\
      \end{array} \]
   (b) How would your answers change if we assume that \( R \) is a UFD?
   (c) How would your answers change if we assume that \( R \) is a PID?

(42) Let \( R \) be a commutative ring and \( x \) an element in \( R \). Let \( S = \{x^k : k \in \mathbb{Z}_{\geq 0}\} \subseteq R \).
   (a) Show that \( x \) is nilpotent if and only if \( S^{-1}R \) is the 0 ring.
   (b) If \( x \) is not nilpotent, show that there is some prime ideal of \( R \) not containing \( x \). Hint: Look at Problem 34.

(43) Let \( k \) be a field, \( f(t) \) a nonzero polynomial with coefficients in \( k \) and \( a \) an element of \( k \).
   (a) Show that \( t - a \) divides \( f(t) \) if and only if \( f(a) = 0 \).
   (b) Show that \( f(t) \) has at most \( \deg(f) \) roots in \( k \).
   (c) Suppose that the characteristic of \( k \) is not 2 and \( c \) is a nonzero element of \( k \). Show that \( c \) has either 0 or 2 square roots in \( k \).

(44) Let \( L \) be the additive subgroup of \( \mathbb{Z}^2 \) generated by \( [\frac{5}{1}] \) and \( [\frac{7}{1}] \). Show that there is a unique subgroup \( M \) with \( L \subset M \subset \mathbb{Z}^2 \) and \( |\mathbb{Z}^2/M| = 9 \). Give generators of \( M \).

(45) Let \( R \) be a UFD in which every nonzero prime ideal is maximal. In this problem we will show that \( R \) is a PID.
   (a) Let \( p_1 \) and \( p_2 \) be prime elements of \( R \) which generate distinct ideals. Show that \( (p_1) \) and \( (p_2) \) are comaximal.
   (b) Let \( f_1 \) and \( f_2 \) be elements of \( R \) with \( \gcd(f_1, f_2) = 1 \). Show that \( (f_1) \) and \( (f_2) \) are comaximal.
   (c) Let \( f_1 \) and \( f_2 \) be elements of \( R \) with \( \gcd(f_1, f_2) = g \). Show that \( (f_1, f_2) = (g) \).
   (d) Let \( f_1, f_2, \ldots, f_N \) be elements of \( R \) with \( \gcd(f_1, f_2, \ldots, f_N) = g \). Show that \( (f_1, f_2, \ldots, f_N) = (g) \).
   (e) Let \( I \) be an ideal of \( R \) with \( \gcd(I) = g \). Show that \( I = (g) \).

(46) This problem deals with various quadratic subrings of \( \mathbb{C} \) and shows how to deal with rings that are “not quite Euclidean”. Throughout, \( N(a + b\sqrt{-D}) \) denotes \( a^2 + Db^2 \), for \( D \in \mathbb{Z}_{>0} \) and \( a, b \in \mathbb{Q} \).
   (a) Let \( D \) be in \( \{1, 2, 3, 4, 5, 6\} \) and let \( a \) and \( b \in \mathbb{Z}[\sqrt{-D}] \) with \( b \neq 0 \). Show that, either, there are \( q \) and \( r \in \mathbb{Z}[\sqrt{-D}] \) with \( a = bq + r \) and \( N(r) < N(b) \), or else there are \( q \) and \( r \in \mathbb{Z}[\sqrt{-D}] \) with \( 2a = bq + r \) and \( N(r) < N(b) \). Show that the same conclusion holds if \( a \) and \( b \) are in \( \mathbb{Z} \left[ \frac{1+\sqrt{-E}}{2} \right] \) with \( E \in \{3, 7, 11, 15, 19, 23\} \). Hint: First prove a modified version of worksheet problem (69.)
   (b) Let \( R \) be \( \mathbb{Z}[\sqrt{-D}] \) or \( \mathbb{Z} \left[ \frac{1+\sqrt{-E}}{2} \right] \) with \( D \) or \( E \) as above and let \( I \) be an ideal of \( R \). Show that either \( I \) is principal, or else there is some \( f \in R \) with \( fR \subset I \subset (f/2)R \). Here \( (f/2)R \) may be a subset of \( \mathbb{C} \) not contained in \( R \).
   (c) We define two ideals \( I \) and \( J \) of \( R \) to be equivalent if there is some \( c \in \text{Frac}(R) \), \( c \neq 0 \), such that \( cI = J \).
      Describe all equivalence classes of ideals in \( \mathbb{Z}[\sqrt{-4}], \mathbb{Z}[\sqrt{-5}] \) and \( \mathbb{Z} \left[ \frac{1+\sqrt{-19}}{2} \right] \).

This problem is an instance of the Minkowski bound. Minkowski showed that, given any number ring \( R \), there is a positive integer \( K \) such that, for every ideal \( I \) of \( R \), there is an element \( f \in I \) with \( |fR/I| \leq K \).