MODERN ALGEBRA (MATH 210) PROBLEM SET 3

1. (a) Must any finite integral domain be a field? (b) *(The field \( \mathbb{F}_4 \).) Ex. 3.14 (p. 125). Ex. 3.44 (ii) (p. 149).*

2. Prove that the quotient ring \( \mathbb{Z}[i]/I \) is finite for any nonzero ideal \( I \) of \( \mathbb{Z}[i] \). *(Hint: Use the fact that \( I = (\alpha) \) for some nonzero \( \alpha \) and then use the division algorithm to see that every coset of \( I \) is represented by an element of norm less than \( N(\alpha) \).)*

3. (a) Prove that if an integer is the sum of two rational squares, then it is the sum of two integer squares (for example, \( 13 = (1/3)^2 + (18/5)^2 = 2^2 + 3^2 \)).
(b) Determine all the representations of the integer \( 2130797 = 17^2 \cdot 73 \cdot 101 \) as the sum of two squares.
(c) Find a generator for the ideal \( (47 - 13i, 53 + 56i) \) in \( \mathbb{Z}[i] \).

4. Let \( I \) and \( J \) be ideals of a commutative ring \( R \).

   (a) Prove that \( I + J \) is the smallest ideal of \( R \) containing both \( I \) and \( J \).
   (b) Prove that \( IJ \) is an ideal contained in \( I \cap J \).
   (c) Given an example where \( IJ \neq I \cap J \).
   (d) Prove that if \( I + J = R \) then \( IJ = I \cap J \).

5. A commutative ring \( R \) is called a *local ring* if it has a unique maximal ideal. Prove that if \( R \) is a local ring with maximal ideal \( m \) then every element of \( R - m \) is a unit. Prove conversely that if \( R \) is a commutative ring with 1 in which the set of nonunits forms an ideal \( m \), then \( R \) is a local ring with unique maximal ideal \( m \).

6. Let \( \omega \) be the cube-root of unity \( \frac{-1 + \sqrt{-3}}{2} \). Show that the ring \( R = \mathbb{Z}[\omega] \) (sometimes called the *Eisenstein integers*) has unique factorization. *(Hint: see the proof for the Gaussian integers in Sec. 3.6.) Factor 2, 3, 5, and 7 into primes in \( R \). (Which one of them has a repeated prime factor? This prime factor is key to an elementary proof of Fermat’s Last Theorem for \( n = 3 \). If you’d like to see it, just ask me.)*

7. Let \( K \) be a field. A *discrete valuation* on \( K \) is a function \( v : K^* \to \mathbb{Z} \) satisfying

   (i) \( v(ab) = v(a) + v(b) \) (i.e., \( v \) is a homomorphism from the multiplicative group of nonzero elements of \( K \) to \( \mathbb{Z} \)),
   (ii) \( v \) is surjective, and
   (iii) \( v(x + y) \geq \min\{v(x), v(y)\} \) for all \( x, y \in K^* \) with \( x + y \neq 0 \).

*Date: Tuesday, October 22, 2002.*
The set \( R = \{ x \times K^x : v(x) \geq 0 \} \cup \{ 0 \} \) is called the valuation ring of \( v \).

(a) Prove that \( R \) is a subring of \( K \) which contains the identity. (In general, a ring \( R \) is called a discrete valuation ring if there is some field \( K \) and some discrete valuation \( v \) on \( K \) such that \( R \) is the valuation ring of \( v \). In fact \( K = \text{Frac}(R) \).)
(b) Prove that for each nonzero element \( x \in K \) either \( x \) or \( x^{-1} \) is in \( R \).
(c) Prove that an element \( x \) is a unit of \( R \) if and only if \( v(x) = 0 \).
(d) The \( p \)-adic valuation \( v_p \). Let \( p \) be a prime. One example of a discrete valuation is \( v_p : \mathbb{Q}^x \to \mathbb{Z} \) given by \( v_p(a/b) = \alpha \) where \( a/b = p^\alpha c/d \), with \( (p, cd) = 1 \). Describe the element of the corresponding valuation ring. Describe the units of the valuation ring.

Remark: There is a theorem that the only valuations on \( \mathbb{Z} \) are these and the usual one. You can do analysis on \( \mathbb{Q} \) using these valuations; they and their generalizations are central in number theory.

8. Let \( F \) be a field. Define the ring \( F((x)) \) of formal Laurent series with coefficients in \( F \) by

\[
F((x)) = \left\{ \sum_{n \geq N} a_n x^n : a_n \in F, N \in \mathbb{Z} \right\}.
\]

(Every element of \( F((x)) \) is a power series in \( x \) plus a polynomial in \( 1/x \), i.e. each element of \( F((x)) \) has only a finite number of terms with negative powers of \( x \).)

(a) Prove that \( F((x)) \) is a field.
(b) Define a discrete valuation on \( F((x)) \) whose discrete valuation ring is \( F[[x]] \), the ring of formal power series with coefficients in \( F \).

Hence \( F((x)) = \text{Frac}(F[[x]]) \). (This can be shown directly as well.)

9. Let \( D \) be a squarefree integer, and let \( \mathcal{O} = \mathbb{Z}[\omega] \) be the ring of integers in the quadratic field \( \mathbb{Q}(\sqrt{D}) \), where \( \omega = (1 + \sqrt{D})/2 \) if \( D \equiv 1 \) (mod 4), and \( \omega = \sqrt{D} \) otherwise. For any positive integer \( f \) prove that the set \( \mathcal{O}_f = \mathbb{Z}[f\omega] = \{ a + bf\omega : a, b \in \mathbb{Z} \} \) is a subring of \( \mathcal{O} \). Prove that \( [\mathcal{O} : \mathcal{O}_f] = f \) (where the index is as additive abelian groups). Prove conversely that a subring of \( \mathcal{O} \) containing the identity and having finite index \( f \) in \( \mathcal{O} \) is equal to \( \mathcal{O}_f \). (The ring \( \mathcal{O}_f \) is called the order of conductor \( f \) in the field \( \mathbb{Q}(\sqrt{D}) \). The ring of integers \( \mathcal{O} \) is called the maximal order in \( \mathbb{Q}(\sqrt{D}) \).)

10. An example of a non-commutative ring. Suppose \( G \) is a finite group. The group ring of \( G \) with coefficients in a commutative ring \( R \), denoted \( RG \), is defined on p. 521 (where it is called a group algebra). Warning: this is a non-commutative ring if \( G \) is not abelian!

1. Let \( K = \{ k_1, \ldots, k_m \} \) be a conjugacy class in \( G \). Prove that the element \( K := k_1 + \cdots + k_m \) is in the center of \( RG \).
2. Let \( K_1, \ldots, K_r \) be the conjugacy classes of \( G \), and for each \( K_i \) let \( \hat{K}_i \) be the element of \( RG \) that is the sum of the members of \( K_i \). Prove that an element \( \alpha \in RG \) is in the center of \( RG \) if and only if \( \alpha = a_1 K_1 + a_2 \hat{K}_2 + \cdots + a_r \hat{K}_r \) for some \( a_1, \ldots, a_r \in R \).
11. Let \( R \) be the ring of all continuous functions from \( \mathbb{R} \) to \( \mathbb{R} \), and for each \( c \in \mathbb{R} \) let \( M_c \) be the ideal \( \{ f \in R : f(c) = 0 \} \).

(a) Show that \( M_c \) is a maximal ideal.
(b) Let \( I \) be the collection of functions \( f(x) \) in \( R \) with compact support (i.e. \( f(x) = 0 \) for \(|x| \) sufficiently large) Prove that \( I \) is an ideal of \( R \) that is not a prime ideal.
(c) Let \( M \) be a maximal ideal of \( R \) containing \( I \). Prove that \( M \neq M_c \) for any \( c \in \mathbb{R} \).

12. A universal side divisor \( u \) is a non-zero, non-unit element of \( R \) such that for every \( x \in R \), either \( u|x \) or \( u|(x + z) \) for some unit \( z \).

A Euclidean domain has universal side divisors: fix the norm \( N \), and let \( u \) be an element of \( R \) \( \setminus \{0, \text{units}\} \) of minimal norm. Then for any \( x \in R \), write \( x = qu + r \) where \( r = 0 \) or \( N(r) < N(u) \) (i.e. \( r \) is a unit). Thus \( u \) divides \( x \) in the first case, and \( x - r \) in the second.

(This argument is given in Prop. 3.63 on p. 154.)

Suppose \( R = \mathbb{Z}[\alpha] \) where \( \alpha = (1 + \sqrt{-19})/2 \). Prove that \( R \) is not a Euclidean domain by showing that it has no universal side divisors as follows.

(a) Find the units of \( R \).
(b) Take the usual norm \( N \) on \( R \) \((N(z) = z\overline{z})\). Show that the only elements of norm less than 5 are \( \{0, \pm1, \pm2\} \).
(c) Taking \( x = 2 \) in the definition of a universal side divisor, show that any universal side divisor must be a nonunit divisor of 2 or 3.
(d) Find all nonunit divisors of 2 and 3.
(e) Now taking \( x = \alpha \) in the definition of universal side divisor, find a contradiction.
(f) Repeat the argument for \( \alpha = (-1 + \sqrt{-163})/2 \).

It is not hard to show that \( \mathbb{Q}(\alpha) \) is a Principal Ideal Domain, so this shows that not every Principal Ideal Domain is a Euclidean Domain.

The set is due Tuesday, October 29 at 3:30 pm in Pierre Albin’s mailbox (opposite the elevator on the first floor of Building 380).