E. Dummit's Math 4527 ~ Number Theory 2, Spring 2024 ~ Homework 5, due Fri Feb 16th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Identify all pages containing each problem when submitting the assignment.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. Determine, with brief reasons, whether each subset S is an ideal of the given ring R:

   (a) $R = F[x]$, $S =$ the set of polynomials whose coefficient of x is zero.
   (b) $R = \mathbb{Z}/18\mathbb{Z}$, $S = \{0, 3, 6, 9, 12, 15\}$.
   (c) $R = \mathbb{Z}/15\mathbb{Z}$, $S = \{0, 4, 8, 12\}$.
   (d) $R = \mathbb{Z} \times \mathbb{Z}$, $S = \{(a, a) : a \in \mathbb{Z}\}$.
   (e) $R = \mathbb{Z} \times \mathbb{Z}$, $S = \{(0, a) : a \in \mathbb{Z}\}$.
   (f) $R = F[x]$, $S = F[x^2]$, the polynomials in which only even powers of x appear.
   (g) $R = F[x]$, $S =$ the set of polynomials whose coefficients sum to zero.

---

2. Let $R = \mathbb{Z}[\sqrt{7}]$ and consider the ideals $I = (3)$ and $J = (3, 1 + \sqrt{7})$.

   (a) Show that R/I contains exactly 9 residue classes. [Hint: They are $p + q\sqrt{7} + I$ for $p, q \in \{0, 1, 2\}$. Explain why.]
   (b) Write down the multiplication table for R/I, and identify which elements are units and which elements are zero divisors. Is I a prime ideal? A maximal ideal?
   (c) Show that R/J contains exactly 3 residue classes and identify them. Is J a prime ideal? A maximal ideal?

Part II: Solve the following problems. Justify all answers with rigorous, clear arguments.

3. Let R be a commutative ring with 1.

   (a) If S is a not necessarily finite set of ideals of R, show that the intersection $T = \bigcap_{I \in S} I$ is an ideal of R.
   (b) Show via an explicit example that the union of a collection of ideals of R is not necessarily an ideal of R.
   (c) If $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ is a not necessarily finite increasing chain of ideals of R, show that the union $T = \bigcup_{i=1}^{\infty} I_i$ is an ideal of R.

---

4. Let R be a commutative ring with 1 and let I and J be ideals of R.

   (a) Show that $I + J = \{a + b : a \in I, b \in J\}$, the set of all sums of elements of I and J, is an ideal of R.
   (b) Show that $I + J$ is the smallest ideal of R that contains both I and J. Deduce that if $I = (a_1, \dots, a_n)$ and $J = (b_1, \dots, b_m)$ then $I + J = (a_1, \dots, a_n, b_1, \dots, b_m)$.
   (c) Let a and b be positive integers with greatest common divisor d. Show that $(a) + (b) = (d)$ in $\mathbb{Z}$.
   (d) Show that $IJ = \{a_1 b_1 + \cdots + a_n b_n, : a_i \in I, b_i \in J\}$, the set of finite sums of products of an element of I with an element of J, is an ideal of R.
   (e) If $I = (a_1, \dots, a_n)$ and $J = (b_1, \dots, b_m)$, show that $IJ = (a_1 b_1, a_1 b_2, \dots, a_n b_1, a_1 b_2, \dots, a_n b_m)$.
   (f) Show that IJ is an ideal contained in $I \cap J$, and give an example where $IJ \neq I \cap J$.
   (g) If $I + J = R$, show that $IJ = I \cap J$. [Hint: There exist $x \in I$ and $y \in J$ with $x + y = 1$.]

---

5. Let R be a commutative ring with 1 and define the binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ for integers $0 \leq k \leq n$. Prove the binomial theorem in R: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$ for any $x, y \in R$ and any $n > 0$.

---

6. Let R be a commutative ring with 1. We say $x \in R$ is nilpotent if $x^n = 0$ for some positive integer n.

   (a) Find the nilpotent elements of $\mathbb{Z}/12\mathbb{Z}$.

   (b) If m is a positive integer, show that a is nilpotent in $\mathbb{Z}/m\mathbb{Z}$ if and only if every prime divisor of m also divides a.

   (c) Show that the set of nilpotent elements of R forms an ideal of R; this ideal is called the nilradical of R. [Hint: Use the binomial theorem to establish closure under subtraction.]

   (d) If x is nilpotent, show that $1 + x$ is a unit. [Hint: What is $(1+x)(1-x+x^2-x^3+\cdots)$?]

---

7. Suppose R is a finite ring with $1 \neq 0$. If R has a prime number of elements p, show that R is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ as a ring. [Hint: Use Lagrange's theorem on the additive group of R to show 1 has additive order p, then consider the map $\varphi : \mathbb{Z} \to R$ with $\varphi(n) = n1_R$.]

---

8. [Challenge] Let F be a field and define $R = F[\epsilon]/(\epsilon^2)$, a ring known as ring of dual numbers over F. Intuitively, one can think of the element $\epsilon \in R$ as being like an "infinitesimal": a number so small that its square is zero.

   (a) Show that the zero divisors in R are the elements of the form $b\epsilon$ with $b \neq 0$, and the units in R are the elements of the form $a + b\epsilon$ with $a \neq 0$.

   (b) Find the three ideals of R.

   (c) Let $p(x) \in F[x]$. Show that $p(x+\epsilon) = p(x) + \epsilon p'(x)$ in $R[x]$, where $p'(x)$ denotes the derivative of $p(x)$.

   (d) Let $p(x), q(x) \in F[x]$ and set $P(x) = p(x)q(x)$. Show that $P'(x) = p'(x)q(x) + p(x)q'(x)$. [Hint: Use (c).]

   Remark: Part (c) shows how to use dual numbers to give a purely algebraic way to compute the derivative of a polynomial (in fact, some computer systems actually do differentiation this way), and (d) illustrates that they yield a formal proof of the product rule. In fact, the dual numbers are essentially the same object used in the construction of cotangent spaces in differential geometry.
