E. Dummit's Math 5111 ~ Algebra 1, Fall 2020 ~ Homework 1, due Fri Sep 18th.

Justify all responses with proof and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers.

---

1. For each polynomial $p(x) \in F[x]$, either find a nontrivial factorization or prove it is irreducible:

   (a) $p(x) = x^3 + x^2 + 1$ in $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, and $\mathbb{Q}[x]$.

   (b) $p(x) = x^5 - 3x^3 + 15x^2 - 21x + 102$ in $\mathbb{Q}[x]$.

   (c) $p(x) = x^3 - 16x + 18$ in $\mathbb{Q}[x]$.

   (d) $p(x) = x^4 + 4x^3 + 6x^2 + 6x + 1$ in $\mathbb{Q}[x]$. [Hint: consider $p(x-1)$.]

   (e) $p(x) = x^4 + 1$ in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{F}_5[x]$, $\mathbb{F}_7[x]$, $\mathbb{Q}[x]$, and $\mathbb{R}[x]$.

---

2. Show that the given element u is invertible in $F[x]/p$, and find its multiplicative inverse in $F[x]/p$:

   (a) $F = \mathbb{Q}$, $p(x) = x^2 + 1$, $u = x + 3$.

   (b) $F = \mathbb{F}_2$, $p(x) = x^5 + x^2 + 1$, $u = x^3$.

   (c) $F = \mathbb{F}_3$, $p(x) = x^4 + 2x + 1$, $u = x^2 + 1$.

---

3. We have discussed a few general strategies for proving irreducibility in $\mathbb{Q}[x]$, such as Eisenstein's criterion and examining factorizations mod p. In other situations, substantially more cleverness can be required. The goal of this problem is to illustrate some trickier approaches.

   (a) Let $r_1, r_2, \dots, r_n$ be distinct integers and let $p(x) = (x - r_1)(x - r_2)\cdots(x - r_n) - 1$. Prove that $p(x)$ is irreducible in $\mathbb{Q}[x]$. [Hint: Suppose $p(x) = f(x)g(x)$ for $f, g \in \mathbb{Z}[x]$. Show that $f(r_i) = -g(r_i)$ for each $1 \le i \le n$, deduce that $f + g$ must be zero, and derive a contradiction.]

   (b) Let $p > 2$ be a prime. Prove that the polynomial $q(x) = x^{2020} + x + p$ is irreducible in $\mathbb{Q}[x]$. [Hint: First show that if $z \in \mathbb{C}$ has $q(z) = 0$, then $|z| > 1$. Then consider constant terms in a possible factorization.]

---

4. Let R be a commutative ring and define the binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ for integers $0 \le k \le n$. 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 $n > 0$.

---

5. Let R be a ring.

   (a) Show that the intersection of an arbitrary collection of subrings of R is a subring of R.

   (b) Show that the union of a collection of subrings of R is not necessarily a subring of R.

   (c) If $S_1 \subseteq S_2 \subseteq \cdots$ is an ascending chain of subrings of R, show that the union $\bigcup_i S_i$ is a subring of R.

   - Remark: The same results hold with "ideal" in place of "subring" everywhere.

---

6. Suppose R is a ring with 1 and let I be an ideal of R.

   (a) Prove that the following are equivalent:

      i. I is a proper ideal of R (i.e., $I \neq R$).
      ii. I contains no units.
      iii. I does not contain 1.

   (b) Now suppose R is also commutative. Show that the set of all nonunits of R forms an ideal M if and only if there exists a proper ideal M of R that contains every other proper ideal of R.

---

7. 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 all the ideals of R. (There are three.)

   (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 $p(x)$.

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