Problem Set 7 : Due Thursday, March 16

See the course website for homework policy.

1. Let $\mathbb{F}_2$ be the field with two elements. Set

$$\begin{aligned} d(x) &= x^8 + x + 1 \\ f(x) &= x^{10} + x^9 + x^8 + x^3 + 1 \\ g(x) &= x^{11} + x^9 + x^8 + x^4 + x^3 + x^2 + 1 \end{aligned}$$

   (a) Show that $d(x) = GCD(f(x), g(x))$.
   (b) Show that $d(x)$ is not divisible by the square of a nonconstant polynomial.
   (c) Show that $\mathbb{F}_2[x]/d(x)$ is isomorphic (as a ring) to a direct sum of fields.

2. This problem is all logical formalities, but it is useful in a surprising number of contexts. Let X and Y be sets and let $\sim$ be a relation between X and Y. For $A \subseteq X$, define $\sigma(A)$ to be $\{y \in Y : x \sim y \text{ for all } x \in A\}$. Similarly, for $B \subseteq Y$, define $\tau(B)$ to be $\{x \in X : x \sim y \text{ for all } y \in B\}$.
   (a) Show that, if $A_1 \subseteq A_2 \subseteq X$, then $\sigma(A_1) \supseteq \sigma(A_2)$.
   (b) For $A \subseteq X$, show that $A \subseteq \tau(\sigma(A))$.
   (c) For $A \subseteq X$, show that $\sigma(A) = \sigma(\tau(\sigma(A)))$.

3. Let k be any field. Define the map $\frac{d}{dx} : k[x] \to k[x]$ by $\frac{d}{dx} \sum f_n x^n = \sum n f_n x^{n-1}$. Purely algebraically, verify that:
   (a) $\frac{d}{dx}(f \cdot g) = f \cdot \frac{dg}{dx} + \frac{df}{dx} \cdot g$.
   (b) If $f(x)^r$ divides $g(x)$, then $f(x)^{r-1}$ divides dg/dx.

4. (a) Let $a(x)$ and $b(x)$ be polynomials with coefficients in $\mathbb{Z}$, let p be prime, and suppose that every coefficient of $a(x)b(x)$ is divisible by p. Show that either p divides every coefficient of a or else p divides every coefficient of b.
   (b) Let $c(x)$ and $d(x)$ be polynomials with coefficients in $\mathbb{Q}$ and suppose that $c(x)d(x) \in \mathbb{Z}[x]$. Show that there is a nonzero rational number r so that $rc(x)$ and $r^{-1}d(x) \in \mathbb{Z}[x]$.
   (c) Let $f(x) = f_n x^n + \cdots + f_1 x + f_0$ be a polynomial with integer coefficients and suppose that p/q is a rational number in lowest terms with $f(p/q) = 0$. Show that p divides f_0 and q divides f_n.
   (d) Let $g(x) = x^n + g_{n-1}x^{n-1} + \cdots + g_1 x + g_0$ be a polynomial with integer coefficients. Suppose that p is prime, that p divides every g_i, and p^2 does not divide g_0. Show that $g(x)$ is irreducible.

5. In this problem (and the rest of the course), you may assume the standard fact that, for a field K, if $f(x)$ is a nonzero polynomial of degree d, then $f(x)$ has at most d zeroes in K.

   Let $f(x_1, x_2, \ldots, x_n)$ be a nonzero polynomial in $K[x_1, \ldots, x_n]$. Let d be the largest exponent to which any x_i is raised in f. Let $X \subseteq K$ have $|X| > d$. Show that there is f is not zero when restricted to $X \times X \times \cdots \times X$.