MATH 8510 - Fall 2014

Homework 8

Due: Thursday, November 20

1. The characteristic of a ring R (with identity) is the smallest positive integer n such that $1 + 1 + \cdots + 1 = 0$ where there are n copies of 1. If no such integer exists we say the characteristic is 0.

   (a) Prove that the map $\mathbb{Z} \to R$ defined by
   $$m \mapsto \begin{cases} 1 + 1 + \cdots + 1 \ (m \text{ copies}) & \text{if } m > 0 \\ 0 & \text{if } m = 0 \\ -1 - 1 - \cdots - 1 \ (-m \text{ copies}) & \text{if } m < 0 \end{cases}$$
   is a ring homomorphism whose kernel is $n\mathbb{Z}$, where n is the characteristic of R.

   (b) Determine the characteristic of the rings $\mathbb{Q}$, $\mathbb{Z}[x]$, and $(\mathbb{Z}/n\mathbb{Z})[x]$.

   (c) Prove that if p is prime and if R is a commutative ring of characteristic p, then $(a + b)^p = a^p + b^p$ for all $a, b \in R$.

2. (a) Solve the simultaneous system of congruences
   $$x \equiv 1 \pmod 8, \quad x \equiv 2 \pmod{25}, \quad x \equiv 3 \pmod{81}.$$

   (b) Let $f_1(x), f_2(x), \ldots, f_r(x)$ be polynomials in $\mathbb{Z}[x]$, each with degree d. Let $n_1, n_2, \ldots, n_r$ be integers that are relatively prime in pairs. Use the Chinese Remainder Theorem to prove that there exists a polynomial $f(x) \in \mathbb{Z}[x]$ of degree d with
   $$f(x) \equiv f_1(x) \pmod{n_1}, \quad f(x) \equiv f_2(x) \pmod{n_2}, \quad \cdots \quad , f(x) \equiv f_r(x) \pmod{n_r}.$$

3. Let R and S be rings.

   (a) Prove that every ideal of $R \times S$ is of the form $I \times J$ for I an ideal of R and J an ideal of S.

   (b) Prove that if R and S are nonzero rings then $R \times S$ cannot be a field.

4. Prove that any subfield of $\mathbb{R}$ must contain $\mathbb{Q}$.

5. Let p be a prime, $I = \mathbb{Z}_{>0}$, and $G_i = \mathbb{Z}/p^i\mathbb{Z}$. Let φ_{ji} be the natural projection maps
   $$\varphi_{ji} : a \pmod{p^j} \mapsto a \pmod{p^i}.$$

   The inverse limit of these groups with the natural projection maps is called the ring of p-adic integers and denoted $\mathbb{Z}_p$.

   (a) Show that every element of $\mathbb{Z}_p$ may be written uniquely as an infinite formal sum $a_0 + a_1 p + a_2 p^2 + \cdots$ with each $a_i \in \{0, 1, \ldots, p-1\}$. Describe the rules for adding and multiplying such formal sums corresponding to the addition and multiplication in the ring $\mathbb{Z}_p$.

   (b) Prove that $\mathbb{Z}_p$ is an integral domain that contains a copy of $\mathbb{Z}$.

   (c) Prove that $a_0 + a_1 p + a_2 p^2 + \cdots$ is a unit in $\mathbb{Z}_p$ if and only if $b_0 \neq 0$.

   (d) Prove that $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$ and $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ where $p = 0 + 1p + 0p^2 + 0p^3 + \cdots$. Prove that every nonzero ideal of $\mathbb{Z}_p$ is of the form $p^n\mathbb{Z}_p$ for some integer $n \geq 0$.

   (e) Show that if $a_1 \not\equiv 0 \pmod p$ then there is an element $a = (a_i) \in \mathbb{Z}_p$ satisfying $a_j^{p-1} \equiv 1 \pmod{p^j}$ and $\varphi_{j1}(a_j) = a_1$ for all j. Deduce that $\mathbb{Z}_p$ contains $p - 1$ distinct $(p-1)^{\text{st}}$ roots of 1.

   (*For the inverse limit of groups refer to either Ex. 10 Chap 6.7 of Dummit and Foote or to Dr. Brown's notes* `http://www.ces.clemson.edu/~jimlb/CourseNotes/AbstractAlgebra/Chapter3.pdf`)