Mathematics 111

Spring 2009

Homework 1

1. For a positive integer m, let $\mathbb{Z}/m\mathbb{Z}$ denote the usual ring of integers modulo m. We wish to consider the existence of ring homomorphisms $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ and their properties. Note that this will also inform us of properties of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$.

   (a) For positive integers m, n show that if $\gcd(m, n) = 1$, then (viewed as set of group or $\mathbb{Z}$-module homomorphisms), $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \{0\}$.

   (b) If m, n are positive integers, show that if $n \mid m$ there is a natural surjective ring homomorphism $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Show that φ induces a group homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$ which is also surjective.

2. **Inverse limits.** Let I be a partially ordered set (see Appendix I if unsure of the definition), and for each $i \in I$, let A_i be a group (also works in other categories). Suppose that for each $i, j \in I$, $i \le j$ we are given a homomorphism $\varphi_{ji} : A_j \to A_i$ satisfying:

   - $\varphi_{ji} \circ \varphi_{kj} = \varphi_{ki}$ whenever $i \le j \le k$, and
   - φ_{ii} is the identity map for all $i \in I$.

   Let $P = \{(a_i) \in \prod_{i\in I} A_i \mid a_i = \varphi_{ji}(a_j) \text{ whenever } i \le j\}$; P is denoted $P = \varprojlim A_i$, and is called the *inverse* or *projective* limit of the A_i.

   (a) Show that $\varprojlim A_i$ is a group under the operations inherited from the direct product.

   (b) (Universal mapping property). For each $k \in I$, let $\varphi_k : \varprojlim A_i \to A_k$ be the standard projection. Suppose that G is any group such that for each $i \in I$ there is a homomorphism $\pi_i : G \to A_i$ so that $\pi_i = \varphi_{ji} \circ \pi_j$ whenever $i \le j$. Show that there is a unique homomorphism $\pi : G \to \varprojlim A_i$ such that $\varphi_i \circ \pi = \pi_i$ for all $i \in I$.

3. **Examples of inverse limits.**

   (a) Let p be a prime, $I = \mathbb{Z}_+$ with the usual partial ordering, and put $A_i = \mathbb{Z}/p^i\mathbb{Z}$. For $i \le j$, let $\varphi_{ji} : A_j \to A_i$ be the ring homomorphism defined in 1b. The inverse limit of the A_i, $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$, is denoted $\mathbb{Z}_p$ and called the ring of p-adic integers.

      i. Show that every element of $\mathbb{Z}_p$ can be written uniquely as a formal sum $b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots$ where each $b_i \in \{0, 1, \ldots, p-1\}$. Represent each element in $A_i = \mathbb{Z}/p^i\mathbb{Z}$ as a least residue $\bmod p$ and express the element in its base p expansion. Characterize the action of the maps φ_{ji} on these representations. Note that this implies that $\mathbb{Z}_p$ is an uncountable set.

      ii. Show that an element $\alpha = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots \in \mathbb{Z}_p$ is a unit (in the ring) if and only if $b_0 \ne 0$.

(b) Let $I = \mathbb{Z}_+$ and partially order I by divisibility: that is "$n \leq m$" iff $n \mid m$. Let $A_n = \mathbb{Z}/n\mathbb{Z}$ and for $n \mid m$, let $\varphi_{mn} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the ring homomorphism in 1b. The inverse limit is denoted $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$.

Now consider a field F and fix an algebraic closure $\overline{F}$ of F. Let I denote the set of finite Galois extensions K/F where $F \subseteq K \subseteq \overline{F}$. Partially order I by inclusion, that is $K_1 \leq K_2$ iff $K_1 \subseteq K_2$. For each $K \in I$, let $A_K = Gal(K/F)$.

i. For $K \subseteq L$ (elements of I), define the natural group homomorphisms $\varphi_{LK} : A_L \to A_K$ and justify (via Galois theory) that they are surjective group homomorphisms.

ii. Now let $F = \mathbb{F}_p$. Give a more complete description of the elements of I and the corresponding A_i, and a refined notion of the partial order. Justify that the Galois group of $\overline{F}/F$, $Gal(\overline{F}/F) := \varprojlim Gal(K/F) \cong \widehat{\mathbb{Z}}$.

iii. Use this characterization of $\widehat{\mathbb{Z}}$ to show that that for any prime q, $\mathbb{Z}_q \subset \widehat{\mathbb{Z}}$.