Math 581g, Fall 2011, Homework 1

William Stein (wstein@uw.edu)

Due: Friday, October 7, 2011

There are 5 problems. Turn your solutions in Friday, October 7, 2011 in class. You may work with other people and can find the LaTeX of this file at http://wstein.org/edu/2011/581g/hw/. Ask me questions during my generous office hours 11:00am-3:15pm on Thursday, October 6 in Sieg 311.

1. Let d be a positive integer, $\mathbb{R}$ the field of real numbers, and $\mathbb{Z}$ the ring of integers. Prove that $(\mathbb{R}^d/\mathbb{Z}^d)[n] \approx (\mathbb{Z}/n\mathbb{Z})^d$.

2. Read somewhere and write down (in a way that makes sense to you) a precise definition of direct and inverse limits of a family of abelian groups (with maps). You can give a definition that involves either sequences of elements with certain properties or a universal property.

3. If A is an abelian group and n is a positive integer, let $A[n] = \{P \in A : nP = 0\}$. What is the cardinality of each of the following abelian groups?
   (a) $\mathbb{Z}[5]$.
   (b) $\mathbb{Q}[5]$.
   (c) $(\mathbb{Q}/\mathbb{Z})[5]$.
   (d) $(\mathbb{Q}_3/\mathbb{Z}_3)[5]$, where $\mathbb{Z}_3$ is the ring of 3-adic numbers and $\mathbb{Q}_3$ the field of 3-adics.
   (e) $(\mathbb{Q}_5/\mathbb{Z}_5)[5]$.
   (f) $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)[\ell^\nu]$, where ℓ is a prime and ν is a positive integer.
   (g) $(\mathbb{Z}/125\mathbb{Z})[5]$.
   (h) $(K^*)[n]$, for K any algebraically closed field of characteristic coprime to n. (Since K^* is multiplicative, $(K^*)[n] = \{x \in K^* : x^n = 1\}$.)
   (i) Let X be any infinite set and let $(\mathbb{Q}/\mathbb{Z})^X$ be the set of all set-theoretic functions $X \to \mathbb{Q}/\mathbb{Z}$. Is the group $((\mathbb{Q}/\mathbb{Z})^X)[n]$ finite or infinite?

4. Let E be an elliptic curve defined over $\mathbb{Q}$, and let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n])$ be the map given by restricting an automorphism of $\overline{\mathbb{Q}}$ to $E[n]$. Prove that
$$\overline{\mathbb{Q}}^{\ker(\rho)} = \mathbb{Q}(E[n]),$$

where $\mathbb{Q}(E[n])$ is *by definition* the field extension of $\mathbb{Q}$ generated by all x and y coordinates of the points in $E[n]$, and $\overline{\mathbb{Q}}^{\ker(\rho)}$ is the subfield of elements in $\overline{\mathbb{Q}}$ fixed by all elements of $\ker(\rho)$.

5. Show that there exists a *non-continuous* homomorphism

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\},$$

where $\{\pm 1\}$ has the discrete topology; equivalently, show there is a non-closed subgroup of index two in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. To accomplish this, produce a map $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$ such that

   (a) ρ is a homomorphism, and

   (b) ρ does not factor through $\mathrm{Gal}(K/\mathbb{Q})$ for any *finite* Galois extension $K/\mathbb{Q}$.

   Don't be afraid to use the Axiom of Choice.