Math 581g, Fall 2011, Homework 1: SOLUTIONS

William Stein (wstein@uw.edu)

November 4, 2011

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

   Solution. We have natural maps

$$(\mathbf{R}^d/\mathbf{Z}^d)[n] = (\mathbf{Q}^d/\mathbf{Z}^d)[n] = \left(\left(\frac{1}{n}\mathbf{Z}\right)^d / \mathbf{Z}^d\right)[n] \cong \mathbf{Z}^d/n\mathbf{Z}^d \cong (\mathbf{Z}/n\mathbf{Z})^d.$$

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.

   Solution. Let I be an ordered (index) set and $\{A_i\}_{i\in I}$ a family of abelian groups. Suppose they are equipped with homomorphisms $\varphi_{i,j} : A_i \to A_j$ whenever $j > i$ (the structure of directed system), and also with homomorphisms $\pi_{i,j} : A_i \to A_j$ when $i > j$ (the structure of inverse system) that satisfy the natural compatibility relations: $\varphi_{j,k} \circ \varphi_{i,j} = \varphi_{i,k}$ and $\pi_{j,k} \circ \pi_{i,j} = \pi_{i,k}$. The *direct limit* $\varinjlim A_i$ is the set of equivalence classes of elements of the disjoint union of the A_i, where two elements x_i and x_j are equivalent if there is some $k \in I$ with $k \geq i$ and $k \geq j$ such that $\varphi_{i,k}(x_i) = \varphi_{j,k}(x_j)$. Let G be an arbitrary abelian group. In terms of a universal property, to give a homomorphism $\varinjlim A_i \to G$ is the same as giving compatible homorphisms $\psi_i : A_i \to G$, i.e., homomorphisms such that whenver $i < j$ we have $\psi_i = \psi_j \circ \varphi_{i,j}$.

   The *inverse limit* $\varprojlim A_i$ is the set of sequences $\{x_i\}_{i\in I}$, with $x_i \in A_i$, such that whenever $i > j$ we have $\pi_{i,j}(x_i) = x_j$. In terms of universal properties, to give a homomorphism $G \to \varprojlim A_i$ is the same as giving a compatible family of homomorphisms $\psi_i : G \to A_i$, where compatible means that $\pi_{i,j} \circ \psi_i = \psi_j$.

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) $\mathbf{Z}[5]$.
   Solution. 1

   (b) $\mathbf{Q}[5]$.
   Solution. 1

   (c) $(\mathbf{Q}/\mathbf{Z})[5]$.
   Solution. 5

   (d) $(\mathbf{Q}_3/\mathbf{Z}_3)[5]$, where $\mathbf{Z}_3$ is the ring of 3-adic numbers and $\mathbf{Q}_3$ the field of 3-adics.
   Solution. 1, since $\frac{1}{5} \in \mathbf{Z}_3$, since 5 is a 3-adic unit.

(e) $(\mathbf{Q}_5/\mathbf{Z}_5)[5]$.
Solution. 5

(f) $(\mathbf{Q}_\ell/\mathbf{Z}_\ell)[\ell^\nu]$, where ℓ is a prime and ν is a positive integer.
Solution. ℓ^ν

(g) $(\mathbf{Z}/125\mathbf{Z})[5]$.
Solution. 5

(h) $(K^*)[n]$, for K any algebraically closed field of characteristic coprime to n. (Since K^* is multiplicative, $(K^*)[n] = \{x \in K^* : x^n = 1\}$.)
Solution. n

(i) Let X be any infinite set and let $(\mathbf{Q}/\mathbf{Z})^X$ be the set of all set-theoretic functions $X \to \mathbf{Q}/\mathbf{Z}$. Is the group $((\mathbf{Q}/\mathbf{Z})^X)[n]$ finite or infinite?
Solution. infinite, since if $x \in X$ then the function $x \mapsto \frac{1}{n}$ and all other $y \in X$ go to 0 is in that group.

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

$$\overline{\mathbf{Q}}^{\ker(\rho)} = \mathbf{Q}(E[n]),$$

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

Solution. We have $\mathbf{Q}(E[n]) \subset \overline{\mathbf{Q}}^{\ker(\rho)}$, since if $\rho(\sigma) = 1$, then σ fixes all x and y coordinates of $E[n]$, hence fixes the generators of the field $\mathbf{Q}(E[n])$. Since the elliptic curve E is defined over $\mathbf{Q}$, the field $\mathbf{Q}(E[n])$ is a Galois extension of $\mathbf{Q}$. Let $H \subset \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be the corresponding normal subgroup, so by Galois theory we have $\overline{\mathbf{Q}}^H = \mathbf{Q}(E[n]) \subset \overline{\mathbf{Q}}^{\ker(\rho)}$. Thus by Galois theory we also have $\ker(\rho) \subset H$. But if $\sigma \in H$, then σ fixes each point in $E[n]$, so $\rho(\sigma) = 1$, hence $H = \ker(\rho)$, as required.

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

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

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

(a) ρ is a homomorphism, and

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

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

Solution. Let $M = \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots, \sqrt{p_i}, \ldots)$ be the infinite extension of $\mathbf{Q}$ generated by all square roots of prime numbers. The automorphisms of M are given by specifying independently $\sqrt{p_i} \mapsto \pm\sqrt{p_i}$, so $\mathrm{Gal}(M/\mathbf{Q}) \cong \prod \mathbf{F}_2$, where we view $(\mathbf{F}_2, +1)$ as a group of order 2 under addition, and the product is over the prime numbers. The product $\prod \mathbf{F}_2$ is the set of all sequences of elements of $\mathbf{F}_2$, and we also view it as a commutative ring R with unity. Note that every element $x \in R$ satisfies $x^2 = x$. Inside R there is an ideal $\oplus \mathbf{F}_2$ consisting of all sequences with finitely many nonzero entries. By Zorn's Lemma (which is a consequence of the Axiom of Choice), there is a maximal ideal $\mathfrak{m}$ in R that contains I. The quotient $R/\mathfrak{m}$ is a field for which every element satisfies $x^2 = x$, so $R/\mathfrak{m} \cong \mathbf{F}_2$. We have thus obtained a surjective homomorphism $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{F}_2$ of groups as the composition

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(M/\mathbf{Q}) \to R/\mathfrak{m} \cong \mathbf{F}_2.$$

Suppose, for the sake of contradiction, that ρ factors through the Galois group of a finite extension K of $\mathbf{Q}$, so we have a diagram

$$\begin{tikzcd} \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \arrow[r, "\rho"] \arrow[dr] & \mathbf{F}_2 \\ & \mathrm{Gal}(K/\mathbf{Q}) \arrow[u] \end{tikzcd}$$

where all maps in the diagram are surjective homomorphisms of groups. We may replace K by its fixed field under $\ker(\mathrm{Gal}(K/\mathbf{Q}) \to \mathbf{F}_2)$, and hence assume that $K = \mathbf{Q}(\sqrt{d})$ is a quadratic field. Then any automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ that fixes all primes $p_i \mid d$ will also act trivially on K, so because the diagram commutes we have $\rho(\sigma) = 1$. Suppose $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is an automorphism such that $\rho(\sigma) \neq 1$. We can modify σ by a lift of any element of the ideal I without changing $\rho(\sigma)$, so modify σ by an element of I so that σ acts trivially on the finitely many $p_i \mid d$. Then $\rho(\sigma) = 1$, as explained above, a contradiction.