Profinite Groups and Complete Local Rings

The Big Picture. We use group homomorphisms

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(R),$$

where R is in some class of topological rings, to parametrize the homomorphisms that elliptic curves and modular forms produce. In this chapter we realize $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ as a topological group. Emulating this idea, we will give a description of the topological, and algebraic structure of the rings R. This, will give us the advantage of studying ρ, not only as a group homomorphism, but also as a continuous map.

0.1 Profinite Groups

In this section we describe the notion and basic properties of profinite groups, which will be useful in later chapters.

Definition 0.1. A *directed set* is a partially ordered set I such that for all $i, j \in I$ there is a $k \in I$ with $i \leq k$ and $j \leq k$.

Example: Let G be a group, and let I be the set of normal subgroups of G of finite index. Say $N_i \geq N_j$ if $N_i \subseteq N_j$. If $N_k = N_i \cap N_j$ then $N_i, N_j \leq N_k$, and so we have a directed set.

Definition 0.2. An inverse system, or projective system

$$\{G_i, \pi_{ij} \mid i, j \in I, i \geq j\}$$

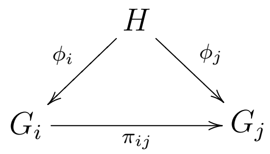
of groups indexed by a directed set I consists of :

- For each $i \in I$, a group G_i.
- For each pair $i \geq j$, a homomorphism $\pi_{ij} : G_i \to G_j$, such that

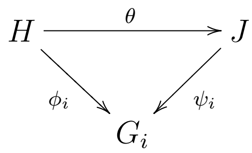
$$\pi_{ii} = \mathrm{Id}, \quad \pi_{jk} \circ \pi_{ij} = \pi_{ik} \quad \textit{whenever} \quad i \geq j \geq k.$$

Example: Index the normal subgroups of finite index by I as above. Setting $G_i = G/N_i$, and $\pi_{ij} : G_i \to G_j$ to be the natural quotient map whenever $i \geq j$, we get an inverse system of groups.

Given an inverse system $\{G_i, \pi_{ij}\}$ we now form a category $\mathcal{C}_{G_i}$, whose objects are pairs $(H, \{\phi_i : i \in I\})$, where H is a group and each $\phi_i : H \to G_i$ is a group homomorphism, with the property that



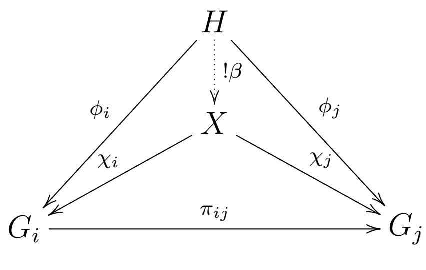
commutes whenever $i \geq j$. Given two objects $(H, \{\phi_i\})$ and $(J, \{\psi_i\})$ in $\mathcal{C}_{G_i}$, we define a morphism between them to be a group homomorphism $\theta : H \to J$ such that



commutes for all $i \in I$.

Example: Continuing our earlier example, $(G, \{\phi_i\})$ is an object of the new category, where $\phi_i : G \to G/N_i$ is the natural quotient map.

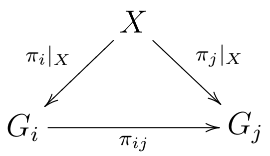
Proposition 0.3. *The* inverse limit*,* $\varprojlim G_i$*, is the terminal object of the category* $\mathcal{C}_{G_i}$*. That is,* $\varprojlim G_i$ *is the unique object* $(X, \{\chi_i\})$ *such that given any object* $(H, \{\phi_i\})$ *there is a unique morphism,* $\beta : (H, \{\phi_i\}) \to (X, \{\chi_i\})$*, such that the following diagram is commutative.*



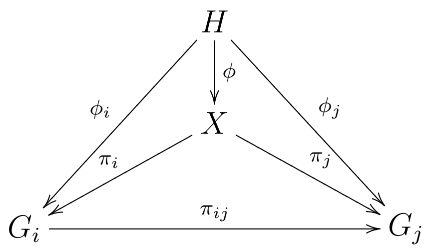
Proof. Let $C = \prod G_i$, and $\pi_i : C \to G_i$ be the ith projection. Let $X = \{c \in C \mid \pi_{ij}(\pi_i(c)) = \pi_j(c)\ \forall i \geq j\}$. We claim that $(X, \{\pi_i|_X\})$ is a terminal object for $\mathcal{C}_{G_i}$. First we must prove that $(X, \{\pi_i|_X\})$ is an object in our category. To this end, note that

$$X = \bigcap_{i \geq j} \{c \in C : \pi_{ij}(\pi_i(c)) = \pi_j(c)\}$$

and each of the π_{ij}, π_i, π_j is a group homomorphism, hence X is a group. By construction the following diagram



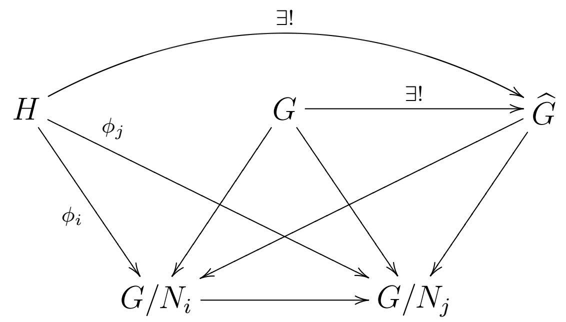
commutes for all $i \geq j$. It follows that $(X, \{\pi_i|_X\})$ is an object in the new category. To see why it is a terminal object, let $(H, \{\phi_i\})$ be an object of $\mathcal{C}_{G_i}$. Given $h \in H$ define $\phi(h) = (\phi_i(h))_{i \in I} \in X$. Since each ϕ_i is a group homomorphism, ϕ is homomorphism. By construction of ϕ the following diagram commutes.



where the condition $\pi_i \phi = \phi_i$ implies that ϕ is the unique such map. Since terminal objects are unique, $\varprojlim G_i = (X, \{\pi_i|_X\})$. $\square$

Example: In our earlier example, the group X above is the *profinite completion* $\widehat{G}$ of G. Since $\widehat{G}$ is terminal, there is a unique group homomorphism $G \to \widehat{G}$. If this is an isomorphism then we say that G is *profinite* (or *complete*). By definition of the profinite completion, we have the following commutative diagram for every object

$(H, \{\phi_i\})$ of $\mathcal{C}_{G/N_i}$ and every pair, $N_i \subseteq N_j$, of normal subgroups of G.



Our interest in profinite groups arise from the fact, shown below, that Galois groups are profinite groups, for instance $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is a profinite group.

Let $\mathcal{C}$ be a class of groups which is closed under images and subgroups. We call G a *pro-$\mathcal{C}$ group* if it is the inverse limit of $\mathcal{C}$-groups. Given G if we only use those finite quotients which are $\mathcal{C}$-groups, then we obtain the *pro-$\mathcal{C}$ completion* of G. For instance, if $\mathcal{C}$ consists of finite p-groups (finite solvable groups), then the pro-$\mathcal{C}$ completion is called the pro-p (respectively prosolvable) completion.

Example: One of the most important example of pro-completion is, *the p-adic group* $\mathbb{Z}_p$. It is the pro-p completion of $\mathbb{Z}$. We will give a more explicit description of $\mathbb{Z}_p$ later in this chapter.

0.2 The Topology of Profinite Groups

In this section we describe how profinite groups carry a natural topology. In particular since $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is a profinite group, to be shown below, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ has a topology which is a key ingredient, as we will see in further chapters, in the study of its representations. The motivation we give for choosing this topology, comes from the analogy between the construction of $\mathbb{R}$ from $\mathbb{Q}$-sequences and the following description of $\widehat{\mathbb{Z}}$. The finite quotients of $\mathbb{Z}$ are $\mathbb{Z}/n\mathbb{Z}$. Hence $\widehat{\mathbb{Z}} = \{(a_1, a_2, a_3, \ldots)|\ a_m \in \mathbb{Z}/m\mathbb{Z}$ and $a_m \equiv a_n \pmod{m}$ if $m|n\}$. Note that $\mathbb{Z}$ maps in to $\widehat{\mathbb{Z}}$ via the constant sequence homomorphism. In other words for $a \in \mathbb{Z}$, the map $a \mapsto (a, a, a \ldots) \in \widehat{\mathbb{Z}}$ is an injective homomorphism from $\mathbb{Z}$ into $\widehat{\mathbb{Z}}$.

Definition 0.4. A *topological group is a group G which is also a topological space with the property that multiplication and inversion are continuous maps.*

Whenever we are given two topological groups, we insist that homomorphisms between them to be continuous. In particular, an isomorphism of topological groups is a group isomorphism, that is at the same time a homeomorphism.

If we start with a collection of topological groups G_i, viewing $\varprojlim G_i$ as a subgroup of $\prod G_i$, we can give $\varprojlim G_i$ a structure of topological group as well. Let us assume that the groups G_i are all finite (as in our running example), and endow G_i with the discrete topology. Then G_i is certainly a totally disconnected Hausdorff space. Since these properties are preserved under taking products and subspaces, $\varprojlim G_i \subseteq \prod G_i$ is Hausdorff and totally disconnected as well. Furthermore, since $\prod G_i$ is compact by Tychonoff's theorem and $\varprojlim G_i$ is closed (see Exercise 0.1), it follows that any profinite group is a Hausdorff, compact, totally disconnected space. It turns out that these properties characterize profinite groups (see (Se)). The following lemma, often used in the theory of profinite groups, see for example Exercise 0.5 and Lemma 0.9, shows how the topological structure, can be used to study the algebraic structure of profinite groups.

Lemma 0.5. *Let $\{G_i, \pi_{ij}\}$ be an inverse system of finite groups, and let $(G, \{\phi_i : i \in I\})$ be an object in $\mathcal{C}_{G_i}$. Assume that G is a compact topological group and that the $\{\phi_i : i \in I\}$ are continuous surjective homomorphisms. Then the induced map, $\phi : G \to \varprojlim G_i$ is surjective.*

Proof. The surjectivity of the ϕ_i's implies that $\phi(G)$ is dense in $\varprojlim G_i$. Since ϕ is clearly continuous, $\phi(G)$ is a compact, dense subset of $\varprojlim G_i$. Since $\varprojlim G_i$ is Hausdorff, the result follows.

□

0.2.1 Galois Groups and Krull Topology

In this section we show why Galois groups are profinite. We start with an interpretation of $\widehat{\mathbb{Z}}$ as a Galois group of an algebraic extension of a finite field.

Example: Consider $\bar{\mathbb{F}}_p = \cup_n \mathbb{F}_{p^n}$. If $m|n$, there is a commutative diagram

$$\begin{array}{ccc}
\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) & \xrightarrow{\ \phi_n\ } & \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n \\
& \searrow^{\phi_m} & \downarrow{\scriptstyle \pi_{nm}} \\
& & \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \cong \mathbb{Z}/m
\end{array}$$

where $\phi_n(g) = g|_{\mathbb{F}_{p^n}}$, for all $g \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. Then we see that $(\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p), \{\phi_n\})$ is an object in the new category corresponding to the inverse system $\{\mathbb{Z}/n, \pi_{m,n}\}$, where $\pi_{m,n}$ is the natural projection for $m|n$. By Proposition 0.3 there is a map $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) \to \widehat{\mathbb{Z}}$. We claim that this map is an isomorphism, so that $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ is profinite. This follows from our next result and Lemma 0.5.

Theorem 0.6. *Let L/K be a (possibly infinite) Galois extension. Then $Gal(L/K) \cong \varprojlim Gal(L_i/K)$, where the limit runs over all finite Galois subextensions L_i/K ordered by inclusion.*

Proof. We have restriction homomorphisms:

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\phi_i} & \mathrm{Gal}(L_i/K) \\ & \searrow^{\phi_j} & \downarrow \pi_{ij} \\ & & \mathrm{Gal}(L_j/K) \end{array}$$

whenever $L_j \subseteq L_i$, i.e. $i \geq j$. We use the projection maps π_{ij} to form an inverse system, so, as before, $(\mathrm{Gal}(L/K), \{\phi_i\})$ is an object of the new category, and we get a group homomorphism

$$\mathrm{Gal}(L/K) \xrightarrow{\phi} \varprojlim \mathrm{Gal}(L_i/K).$$

We claim that ϕ is an isomorphism. (i) We may assume $L \neq K$. Suppose $1 \neq g \in \mathrm{Gal}(L/K)$. Then there is some $x \in L$ such that $g(x) \neq x$. Let L_i be the normal closure of $K(x)$. Since L/K is separable, this is a finite Galois extension of K, and $1 \neq g|_{L_i} = \phi_i(g)$, which yields that $1 \neq \phi(g)$. Hence ϕ is injective. (ii) Take $(g_i) \in \varprojlim \mathrm{Gal}(L_i/K)$ so that $L_j \subseteq L_i \Rightarrow g_i|_{L_j} = g_j$. Then define $g \in \mathrm{Gal}(L/K)$ by $g(x) = g_i(x)$ whenever $x \in L_i$. This is a well-defined field automorphism and $\phi(g) = (g_i)$. Thus ϕ is surjective. □

Let Fr be the element of $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ given by $Fr(x) = x^p$, i.e. the Frobenius automorphism. Since $\widehat{\mathbb{Z}}$ is not cyclic (see Exercise 0.6) Fr does not generate $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$, even though its image, via restriction, generates $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. However, the subgroup of $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ generated by Fr corresponds to the image of $\mathbb{Z}$ in $\widehat{\mathbb{Z}}$, and it is therefore dense (see Exercise 0.3). Then we say that $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ is *topologically generated* by one element, Fr, and so is *procyclic*.

0.2.2 The Fundamental theorem of infinite Galois theory

The topology we obtain on Gal(L/K), as a profinite group, is known as *the Krull topology.* For another description of this topology see Exercise 0.9. One of the most famous uses of this topology is a generalization of the classical fundamental theorem for finite Galois extensions.

Proposition 0.7. *Let L be Galois over K, with Galois group G.*

(i) The field L is Galois over every subfield M containing K. Moreover, $Gal(L/M)$ is closed in G, and $L^{Gal(L/M)} = M$.

(ii) For every subgroup H of G, $Gal(L/L^H)$ is the closure of H

Theorem 0.8. *Let L be Galois over K, with Galois group G. The maps*

$$H \mapsto L^H, \quad M \mapsto Gal(L/M)$$

are inverse bijections between the set of closed subgroups of G and the set of intermediate fields between L and K. Moreover,

(i) The correspondence is inclusion-reversing.

(ii) A closed subgroup H of G is open if and only if L^H has finite degree over K, in which case $(G : H) = [L^H : K]$.

(iii) For all $g \in G$, $L^{H^g} = g(L^H)$ and $Gal(L/g(M)) = Gal(L/M)^g$.

(iv) A closed subgroup H of G is normal if only if L^H is Galois over K, in which case $Gal(L/L^H) \cong G/H$.

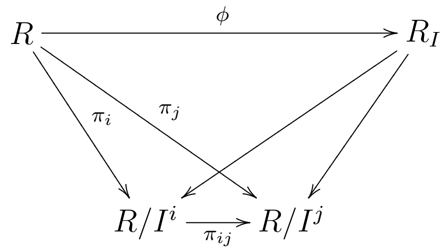
For proofs of these results see (F-J).

0.3 Complete Local Rings

We now carry out the same procedure with rings rather than groups and so define certain completions of them. Let R be a commutative ring with identity 1 and I any proper ideal of R. For $i \geq j$ we have a natural quotient map

$$R/I^i \xrightarrow{\pi_{ij}} R/I^j.$$

These rings and maps form an inverse system of rings. Proceeding as in the previous section, we can form a new category. Then the same proof gives that there is a unique terminal object, $R_I = \varprojlim R/I^i$, which is now a ring, together with a unique ring homomorphism, $R \xrightarrow{\phi} R_I$, such that the following diagram commutes:



Note that R_I depends on the ideal chosen. It is called the *I-adic completion of R*. (Do not confuse it with the localization of R at I). We call R (I-adically) *complete* if the map $\phi : R \to R_I$ is an isomorphism. In particular, R_I is complete. Note that ϕ is injective if and only if $\bigcap_{n\geq 1} I^n = \{0\}$. Thus a necessary condition for R to be I-adically complete is that this intersection is trivial. This is the case for instance, when R a Noetherian domain (Krull's intersection Theorem). In the situation, $\bigcap_{n\geq 1} I^n = \{0\}$, we can define a metric topology on R as follows:
Let x, y be elements of R and let c be a real positive number less than 1. Define $d(x,y) = c^n$ if $x - y \in I^n \setminus I^{n+1}$, and $d(x,x) = 0$. Then we have the following:

- $d(x,y) = d(y,x)$
- $d(x,z) \leq \max(d(x,y), d(y,z)) \leq d(x,y) + d(y,z)$
- $d(x,y) = 0$ iff $x - y \in \bigcap_{n\geq 1} I^n$ if and only if $x = y$

The topology defined is independent of c, and its topological completion is just the I-adic completion. If $\mathbf{m}$ is a maximal ideal, then $R_{\mathbf{m}}$ coincides with the completion of R localized at $\mathbf{m}$, and hence it is *local*, i.e. has a unique maximal ideal, namely $\mathbf{m}R_{\mathbf{m}}$ (see, (Bo)). In the case of $\mathbb{Z}_p$ this is an easy consequence of Exercise 0.7.

Example: If $R = \mathbb{Z}$, $\mathbf{m} = p\mathbb{Z}$, p prime, then $R_{\mathbf{m}} \cong \mathbb{Z}_p$, the *$p$-adic integers.* The additive group of this ring is the pro-p completion of $\mathbb{Z}$. In fact,

$$\mathbb{Z}_p = \{(a_1, a_2, ...)|\ a_i \in \mathbb{Z}/p^i\mathbb{Z}, a_i \equiv a_j \bmod p^j \text{ if } i \geq j\}.$$

Example: The group of invertible n by n matrices over $\mathbb{Z}_p$, $\mathrm{GL}_n(\mathbb{Z}_p)$ is a topological group that inherits its topology from $\mathbb{Z}_p^{n^2}$. Since $\mathbb{Z}_p^{n^2}$ is a compact, totally disconnected, Hausdorff space, and $\mathrm{GL}_n(\mathbb{Z}_p)$ is clearly closed it is also a profinite group.

The following lemma gives a more precise description of its structure as profinite group.

Lemma 0.9. $\mathrm{GL}_n(\mathbb{Z}_p) \cong \varprojlim \mathrm{GL}_n(\mathbb{Z}/p^n\mathbb{Z})$.

Proof. Consider the natural projection homomorphisms $\mathrm{GL}_n(\mathbb{Z}_p) \twoheadrightarrow \mathrm{GL}_n(\mathbb{Z}_p/p^n\mathbb{Z}_p)$. Since $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$, see Exercise 0.7, we get compatible homomorphisms

$$\mathrm{GL}_n(\mathbb{Z}_p) \twoheadrightarrow \mathrm{GL}_n(\mathbb{Z}/p^n\mathbb{Z}).$$

Hence, there exits a homomorphism $\mathrm{GL}_n(\mathbb{Z}_p) \to \varprojlim \mathrm{GL}_n(\mathbb{Z}/p^n\mathbb{Z})$. Since the only element in $\mathbb{Z}_p$ that reduces to 0 mod p^n for all n is 0, this map is injective. Surjectivity follows from Lemma 0.5. $\square$

One of our main aims is to understand continuous homomorphisms $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathcal{O})$, where $\mathcal{O}$ is some finite extension of $\mathbb{Z}_p$. Motivated by the structure of the rings $\mathcal{O}$, which we describe in the next chapter, we focus our interest in the category $\mathcal{C}_{\mathbb{F}}$, whose objects are complete local Noetherian rings with finite residue field $\mathbb{F}$. In this category, a morphism ϕ is required to make the following diagram commutative:

$$\begin{array}{ccc} R & \xrightarrow{\phi} & S \\ \downarrow & & \downarrow \\ \mathbb{F} & \xrightarrow[\mathrm{Id}]{} & \mathbb{F} \end{array}$$

Here the vertical maps are the natural projections. This is equivalent to requiring that $\phi(\mathbf{m}_R) \subseteq \mathbf{m}_S$, where $\mathbf{m}_R$ and $\mathbf{m}_S$ are the maximal ideals of R and S, respectively.

Example: If $\mathbb{F} = \mathbb{F}_p$, then $\mathbb{Z}_p$ and $\mathbb{F}_p[[T_1, \ldots, T_m]]$ are objects of $\mathcal{C}_{\mathbb{F}}$.

The next result, known as Cohen's structure theorem ((Mat)), gives an explicit description of the objects of $\mathcal{C}_{\mathbb{F}}$.

Theorem 0.10. *There exists $W(\mathbb{F})$ in $\mathcal{C}_{\mathbb{F}}$ with the following properties:*

1. *Every R in $\mathcal{C}_{\mathbb{F}}$ is a $W(\mathbb{F})$-algebra, via a morphism in $\mathcal{C}_{\mathbb{F}}$.*
2. *If $m_1, m_2, ..., m_n$ is a set of generators of the maximal ideal $\mathbf{m}$ of R. Then the induced map of $W(\mathbb{F}) - algebras$, $T_i \mapsto m_i$*

$$W(\mathbb{F})[[T_1, \ldots, T_m]] \to R$$

is surjective.

The ring $W(\mathbb{F})$ is called *the ring of infinite Witt vectors over* $\mathbb{F}$. For an explicit description of $W(\mathbb{F})$, see Definition **??**. In the case of $\mathbb{F} = \mathbb{F}_p$, p a prime, $W(\mathbb{F}_p) = \mathbb{Z}_p$.

Exercises

0.1. Show that if $f, g : A \to B$ are continuous with A, B Hausdorff topological spaces, then $\{x | f(x) = g(x)\}$ is closed. Deduce that

$$\varprojlim G_i = \bigcap_{i \geq j} \left\{ c \in \prod G_i : \pi_{ij}(\pi_i(c)) = \pi_j(c) \right\}$$

is closed in $\prod G_i$ and is therefore compact. In summary, $\varprojlim G_i$ is a compact, totally disconnected Hausdorff space.

0.2. Prove that $\widehat{G} \to \widehat{\widehat{G}}$ is an isomorphism, so that $\widehat{G}$ is complete.

0.3. Show that the natural inclusion $\mathbb{Z} \to \widehat{\mathbb{Z}}$ maps $\mathbb{Z}$ onto a dense subgroup. In fact, show that for any group G, its image in $\widehat{G}$ is dense. Give an example such that the kernel of $G \to \widehat{G}$ is not trivial. Moreover, show that this kernel is trivial if and only if G is *residually finite*, i.e. if the intersection of all its subgroups of finite index is trivial.

0.4. Let $R = \mathbb{Z}$ and $I = 6\mathbb{Z}$. Show that the I-adic completion of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$, and so is not local. This is an example of a *semilocal ring*, i.e a finite product of local rings. If n is a positive integer and $I = n\mathbb{Z}$, is the I-adic completion of $\mathbb{Z}$ always semilocal?

0.5. Let p be a rational prime. Show that there is a surjective group homomorphism $\phi : \widehat{\mathbb{Z}} \to \mathbb{Z}_p$ in the two different ways;

- By using Lemma 0.5.
- By proving that $\widehat{\mathbb{Z}}$ is isomorphic to $\prod \mathbb{Z}_q$ as groups, the product being over all rational primes.

0.6. Show that $\mathbb{Z}_2$ is uncountable. Deduce that $\widehat{\mathbb{Z}}$ is not a cyclic group.

0.7. Show that the ideals of $\mathbb{Z}_p$ are precisely $\{0\}$ and $p^i\mathbb{Z}_p$ for $i \geq 0$. Deduce that the kernel of the projection map $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ is $p^n\mathbb{Z}_p$.

0.8. If R is a ring that is I-adically complete, show that $\mathrm{GL}_n(R) \cong \varprojlim \mathrm{GL}_n(R/I^i)$ where the maps $\mathrm{GL}_n(R/I^i) \to \mathrm{GL}_n(R/I^j)$ are the natural ones.

Note that the topology on R induces the product topology on $M_n(R)$, and hence the subspace topology on $\mathrm{GL}_n(R)$.

0.9. Let L/K be a Galois extension. Show that $\mathrm{Gal}(L/L_i)$ is a basis of open neighborhoods of the identity, where the L_i/K runs over all finite subextensions of L/K.

References

[Bo] Bourbaki,N, *Commutative algebra. Chapters 1–7*, Springer-Verlag, Berlin, 1998.

[F-J] , Fried, Michael D. and Jarden, Moshe *Field Arithmetic*, Springer-Verlag, Berlin, 2005, 11, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics.

[Mat] Matsumura, Hideyuki, *Commutative algebra*, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1990, Mathematics Lecture Note Series 56, second edition.

[Se] Serre,J.-P, *Galois Cohomology*, Springer-Verlag, New York-Berlin, 2001, Monographs in Mathematics.