ABSTRACT ALGEBRA: A PRESENTATION ON PROFINITE GROUPS

JULIA PORCINO

Our brief discussion of the p-adic integers earlier in the semester intrigued me and lead me to research further into this topic. That research lead to the main focus of this project, profinite groups. This project traces the connections between several different algebraic ideas in group theory. It is a culmination of old and new material. Beginning with familiar topics such as topology and the p-adics, I approached several of these ideas in new ways that allowed me to deepen my understanding of these areas. This provided a secure point of departure to explore completely new algebraic topics such as profinite groups and some introductory Galois theory (Appendix B).

Topology

Since this project is directed towards students in an abstract algebra course with no other assumptions about background, I will begin by reviewing certain basic topological ideas that will be necessary as we progress through the material. We will begin with the definition of a topological group:

> A *topological group* G is a group that is also a topological space such that the product map:
>
> $$p : G \times G \to G$$
>
> $$(g, g') \mapsto gg'$$
>
> and the inverse map:
>
> $$i : G \to G$$
>
> $$g \mapsto g^{-1}$$
>
> are continuous functions (with respect to the topology).

Throughout this paper we will take G to be a topological group, and we will let X represent the more general topological space. A space X could be equipped with a wide variety of topologies, including the subspace topology, the product topology, or the quotient topology. One topology that we will be concerned with later on is the discrete topology:

> A topological space X is equipped with the *discrete topology* if every subset of X is open.

Sometimes the definition of the topological group includes that G must be Hausdorff, but as this notion is important in later discussions, we will define it separately here. The property of being a Hausdorff space (sometimes also known as a T_2-*space*) is one of the separation axioms.

> A topological space X is *Hausdorff* if for all $x, y \in X$ there exist open sets $U, V \subseteq X$ such that $x \in U$, $y \in V$ and the intersection of U and V is empty.

Related to the separation axioms is the idea of connectedness:

> A topological space X is *connected* if it cannot be written as the union of two disjoint nonempty open sets. Otherwise, X is called *disconnected*.

Later on we will be most concerned with the idea of a topological space that is totally disconnected:

> X is *totally disconnected* if the only connected subsets of X are the one-element sets.

The final key definition to review is compactness:

> X is *compact* if every open cover of X has a finite subcover.

Here, we take a cover of X to refer to a collection of subsets of X whose union is X, and an open cover requires those subsets to be open.

The p-adic Integers

Before moving on to the discussion of profinite groups, I would like to briefly review a topic that we saw earlier in the semester, the p-adic integers. The p-adic integers, $\mathbb{Z}_p$ for p prime, were first introduced during our discussion of group products since an algebraic way to define these integers is as the limit of group products:

$$\mathbb{Z}_p = \lim_{e} \mathbb{Z}/p^e$$

We later compared this construction of the p-adic integers with the more classical definition as the completion of $\mathbb{Z}$ under the p-adic metric, a review of which is included in the first appendix below. Under this classical construction, it might be easier to think of the p-adic integers as an extension of the integers, and so retains some of the algebraic structure of $\mathbb{Z}$. It is important to note that different metrics can give rise to the same topology. Thus, the topology that is uniquely determined by the product topologies on $\lim_e \mathbb{Z}/p^e$ is the same topology as the one that arises from the p-adic metric.

One of our motivations for introducing the limit construction of $\mathbb{Z}_p$ was that some of the properties of the p-adics are more evident from this construction as compared to the set-theoretic definition. In particular, we discussed that the compactness of $\mathbb{Z}_p$ is easily inherited from the group products, yet this topological property is much more difficult to tease out from the classical construction. Certain other topological properties are inherent in $\mathbb{Z}_p$ as an extension of the integers or from the classical construction such as $\mathbb{Z}_p$ being totally disconnected. The fact that $\mathbb{Z}_p$ is Hausdorff also follows from the classical definition since the Hausdorff property relies on open sets, which the metric helps to define.

Profinite Groups

With the idea of p-adic integers in mind, we now turn our focus to profinite groups. The group of p-adic integers under addition is a profinite group, and many of the properties of the p-adics discussed in the previous section will be important in contributing to the group being profinite.

There are two equivalent ways to define profinite groups. The first relies on the topology introduced in the earlier section, and so we will focus our attention on this definition first.

> A *profinite group* is a compact, Hausdorff, and totally disconnected topological group.

These topological properties that define profinite groups unsurprisingly affect other properties of the groups and their subgroups. The product of arbitrarily many profinite groups is again profinite, and the product topology matches the topology inherent from the groups' profinite properties. Closed subgroups of profinite groups are also profinite, and similarly, the subspace topology is consistent with the profinite topology. If a closed subgroup is also normal, then the quotient group will be profinite with the quotient topology consistent with the profinite topology. Profinite groups are particularly useful for the property of being compact Hausdorff, which is useful as a measuring property.

A profinite group can also be constructed from a finite group if the finite group is given the discrete topology. This leads us to the other definition for profinite groups. This second definition requires us to first define some new algebraic objects:

> A *directed partially ordered set* is a set I with a partial order $\geq$ such that for any two elements $i, j \in I$ there exists a $k \in I$ such that $k \geq i$ and $k \geq j$.

> A *projective system* is a collection of groups G_i, $i \in I$, with group homomorphisms $f_{i,j} : G_j \to G_i$ for $i, j, \in I$ and $j \geq i$

such that $f_{i,i} = \mathrm{id}_{G_i}$ for all $i \in I$ and $f_{i,j} \circ f_{j,k} = f_{i,k}$ for $k \geq j \geq i$.

Given a projective system $(G_i, f_{i,j})$, the *projective limit* is a particular subgroup of the direct product of G_i's:

$$\varprojlim G_i = \{(g_i) \in \prod G_i \mid g_i = f_{i,j}(g_i)\ \forall j \geq i\}.$$

With these terms in place, the equivalent definition for a profinite group follows:

A *profinite group* is a topological group that is isomorphic to the inverse (or projective) limit of finite groups.

Returning again to the example of the p-adic integers, since $\mathbb{Z}/p^n\mathbb{Z}$ is a finite group for $n \in \mathbb{N}$, it clearly follows that $\mathbb{Z}_p$ is the projective limit of these groups. As examined earlier, $\mathbb{Z}_p$ is a topological group, and thus we find that the p-adic integers also satisfy this definition of the profinite group. In fact, since this definition of profinite groups is algebraic in structure, the algebraic construction of the p-adic integers complements this definition well.

With the p-adic integers as a motivation, we can create other profinite groups with constructions similar to those of the p-adics. The best way to do so is by generalizing the projective limit for any $a \in \mathbb{Z}_{\geq 1}$:

$$\mathbb{Z}_a = \varprojlim \mathbb{Z}/a^n\mathbb{Z}.$$

We refer to $\mathbb{Z}_a$ as the a-adic integers. From this definition, the following isomorphism holds:

$$\mathbb{Z}_a \approx \prod_{p|a} \mathbb{Z}_p.$$

Since $a \in \mathbb{Z}$ and $p \mid a$, let $a = p^i b$, where $b \in \mathbb{Z}$ such that p does not divide b,

$$\begin{aligned}\mathbb{Z}_a &= \varprojlim \mathbb{Z}/a^n\mathbb{Z} \\ &= \varprojlim \mathbb{Z}/(p^i b)^n\mathbb{Z} \\ &= \varprojlim \mathbb{Z}/p^{in}b^n\mathbb{Z}\end{aligned}$$

Then by the Sun-Ze Theorem, $\varprojlim \mathbb{Z}/p^{in}b^n\mathbb{Z} = \varprojlim(\mathbb{Z}/p^{in}\mathbb{Z} \times \mathbb{Z}/b^n\mathbb{Z}) \approx \mathbb{Z}_p\mathbb{Z}_b$. With induction on b we reach the desired relation.

Appendix A: The Classical Analytic Construction of the p-adic Integers

Let p be prime and let $x \in \mathbb{Z}$ such that $x = p^n a$, $a \in \mathbb{Z}/p\mathbb{Z}$ and $n \in \mathbb{Z}$. Then we define the p-adic norm to be:

$$|x|_p = p^{-n}.$$

For all $x, y \in \mathbb{Z}$, the p-adic norm has the following properties:

$|0|_p = 0$,
$|x \cdot y|_p = |x|_p \cdot |y|_p$,
$|x + y|_p \leq \max\{|x|_p, |y|_p\}$, equality if $|x|_p \neq |y|_p$.

This allows us to define a metric d_p:

$$d_p(x, y) = |x - y|_p.$$

This metric does satisfy the following three properties as necessary:

$d_p(x, y) \geq 0$ with equality iff $x = y$,
$d_p(x, y) = d_p(y, x)$,
$d_p(x, y) \leq d_p(x, z) + d_p(y, z),\ \forall x, y, z \in \mathbb{Z}$.

Then the p-adic integers $\mathbb{Z}_p$ are defined as the completion of the metric space $(\mathbb{Z}, d_p)$.

Appendix B: Profinite Groups in Relation to Galois Theory

We ended the semester with a brief glimpse into Galois theory. As it turns out, the research on profinite groups is also related to Galois theory. However, since the ideas needed to discuss profinite groups in Galois theory are not directly related to the main body of this project, I am including the topic in a fairly brief overview, similar to how we ended the semester.

When we saw Galois theory briefly at the end of the semester, we were constructing the $17th$-root of unity by introducing the roots of quadratics. In fact, what we were doing was creating extension fields:

> A field E is an *extension field* of a field F if $F \subseteq E$ and the operations of F are those of E restricted to F.

We've seen other examples of field extensions before, although we may not have recognized them. One example is the complex number field, which is isomorphic to the extension field of the reals, $\mathbb{R}[x]/ < x^2 + 1 >$.

Field extensions are particularly helpful for creating finite fields of specific orders since an extension field E will have a degree:

> Let E be an extension field of a field F. Then E *has degree* n *over* F and write $[E : F] = n$ if E has dimension n as a vector space over F. If $[E : F]$ is finite, E is called a *finite extension* of F. Otherwise, E is an *infinite extension* of F.

This extension field is sometimes referred to as algebraic, which can then be related to the Galois extension:

> An algebraic field extension E/F is a *Galois extension* if it is normal and separable.

Normal and separable are two properties of extension fields:

> A field extension E/F is *normal* if E is the splitting field of a family of polynomials in $F[x]$, i.e. for $f(x) \in F[X]$, $f(x)$ can be factored as a product of linear factors in $E[x]$, but in no proper subfield of $E[x]$.

> An extension field E of F is *separable* if and only if for every $e \in E$ the minimal polynomial of e over F is a separable polynomial (i.e., has distinct roots). Otherwise, the extension is called inseparable.

This leads to the definition of the Galois group:

> Let E be an extension field of the field F such that E/F is a Galois extension. The *Galois group* of E over F , $\mathrm{Gal}(E/F)$, is the set of all automorphisms of E that take every element of F to itself, where an automorphism of E is understood to be a ring automorphism from E onto E.

Consider the collection of Galois groups, $\mathrm{Gal}(E_i/F)$, such that each E_i/F is a finite extension field. Then taking the projective limit of these finite groups, we have:

$$\varprojlim \mathrm{Gal}(E_i/F) = \mathrm{Gal}(E/F)$$

where the group homomorphisms are the mappings

$$\mathrm{Gal}(E_i/F) \to \mathrm{Gal}(E_j/F),\ E_j \subseteq E_i.$$

Thus, the resulting Galois group $\mathrm{Gal}(E/F)$ over the infinite extension field E/F is profinite.