Pro-p Groups

Simon Stead

University of York

June 4, 2015

Profinite Groups

Definition

A *directed set* is a non-empty partially ordered set $(S, \leq)$ such that for all $i, j \in S$ there exists $k \in S$ such that $i \leq k$ and $j \leq k$.

Profinite Groups

Definition

A *directed set* is a non-empty partially ordered set $(S, \leq)$ such that for all $i, j \in S$ there exists $k \in S$ such that $i \leq k$ and $j \leq k$.

Definition

An *inverse system of groups* is a collection of groups $(G_i)_{i \in S}$ (S being a directed set as above) along with a family of homomorphisms $\phi_{kj} : G_k \to G_j$ whenever $j \leq k$, such that $\phi_{ji} \circ \phi_{kj} = \phi_{ki}$ whenever $i \leq j \leq k$. An *inverse limit* is then the set of all objects in the Cartesian product $\prod_{k \in S} G_k$ such that $\phi_{kj}(g_k) = g_j$ whenever $j \leq k$.

Profinite Groups

Definition

A *directed set* is a non-empty partially ordered set $(S, \leq)$ such that for all $i, j \in S$ there exists $k \in S$ such that $i \leq k$ and $j \leq k$.

Definition

An *inverse system of groups* is a collection of groups $(G_i)_{i \in S}$ (S being a directed set as above) along with a family of homomorphisms $\phi_{kj} : G_k \to G_j$ whenever $j \leq k$, such that $\phi_{ji} \circ \phi_{kj} = \phi_{ki}$ whenever $i \leq j \leq k$. An *inverse limit* is then the set of all objects in the Cartesian product $\prod_{k \in S} G_k$ such that $\phi_{kj}(g_k) = g_j$ whenever $j \leq k$.

Definition

A *projection* is a homomorphism ϕ_i from the Cartesian product $\left(\prod_{k \in S} G_k\right) \to G_i$, for some i, such that for $g \in \prod_{k \in S} G_k$, $\phi_i(g) = g_i$.

Profinite Groups

Definition

A *profinite group* G is an inverse limit of finite groups. That is $G = \varprojlim (G_i)_{i \in S}$. This is equivalent to saying G is a compact Hausdorff topological group whose open subgroups form a base for the neighbourhoods of the identity.

Pro-p Groups

Definition

Let $N \lhd_O G$ be an open normal subgroup of a profinite group G. G is said to be a *pro-p group* if G/N is a (finite) p-group for all N. Since in a profinite group all open subgroups are closed and have finite index, the quotient group G/N is always finite.

Pro-p Groups

Definition

Let $N \lhd_O G$ be an open normal subgroup of a profinite group G. G is said to be a *pro-p group* if G/N is a (finite) p-group for all N. Since in a profinite group all open subgroups are closed and have finite index, the quotient group G/N is always finite.

The prototypical example of a pro-p group is the (additive) group of p-adic integers.

Definition

$$\mathbb{Z}_p = \varprojlim \left(\mathbb{Z}/p^n\mathbb{Z}\right).$$

$\mathbb{Z}_p$ - The p-adic Integers

All finite p-groups are pro-p groups, but $\mathbb{Z}_p$ is the simplest kind of infinite pro-p group we can construct, as it's parts are the cyclic groups of p^n elements. In fact for this reason, $\mathbb{Z}_p$ is said to be *pro-cyclic*.

$\mathbb{Z}_p$ - The p-adic Integers

All finite p-groups are pro-p groups, but $\mathbb{Z}_p$ is the simplest kind of infinite pro-p group we can construct, as it's parts are the cyclic groups of p^n elements. In fact for this reason, $\mathbb{Z}_p$ is said to be *pro-cyclic*.

Definition

An element α of $\mathbb{Z}_p$ is written $\sum_{i=0}^{\infty} a_i p^i$ where $a_i \in \mathbb{F}_p$, the finite field of p elements.

$\mathbb{Z}_p$ - The p-adic Integers

All finite p-groups are pro-p groups, but $\mathbb{Z}_p$ is the simplest kind of infinite pro-p group we can construct, as it's parts are the cyclic groups of p^n elements. In fact for this reason, $\mathbb{Z}_p$ is said to be *pro-cyclic*.

Definition

An element α of $\mathbb{Z}_p$ is written $\sum_{i=0}^{\infty} a_i p^i$ where $a_i \in \mathbb{F}_p$, the finite field of p elements.

$\mathbb{Z}_p$ is actually more than just a topological space as we might expect. We can endow it with a metric (in fact a complete metric) in order to determine distances between two elements of $\mathbb{Z}_p$. This is given by $|\sum_{i=k}^{\infty} a_i p^i|_p = p^{-k}$.

Examples

Theorem

$GL_d(\mathbb{Z}_p)$ is profinite.

Examples

Theorem

$GL_d(\mathbb{Z}_p)$ is profinite.

Proof.

For each $n \in \mathbb{N}$ there exists a natural projection

$$\theta_n \; : \; GL_d(\mathbb{Z}_p) \to GL_d(\mathbb{Z}_p/p^n\mathbb{Z}_p),$$

explicitly written as

$$\theta_n(g) = g \mod p^n.$$

It is simple enough to then show that
$\varprojlim GL_d(\mathbb{Z}_p/p^n\mathbb{Z}_p) = GL_d(\mathbb{Z}_p)$*.*

Examples

Theorem

$GL_d(\mathbb{Z}_p)$ is profinite.

Proof.

For each $n \in \mathbb{N}$ there exists a natural projection

$$\theta_n \ : \ GL_d(\mathbb{Z}_p) \to GL_d(\mathbb{Z}_p/p^n\mathbb{Z}_p),$$

explicitly written as

$$\theta_n(g) = g \mod p^n.$$

It is simple enough to then show that $\varprojlim GL_d(\mathbb{Z}_p/p^n\mathbb{Z}_p) = GL_d(\mathbb{Z}_p)$. This is most clear by considering $GL_d(\mathbb{Z}_p)$ as a subset of the set of matrices of dimension d, $M_d(\mathbb{Z}_p)$. This is isomorphic to $\mathbb{Z}_p^{d^2}$, and as subsets of profinite groups are profinite, $GL_d(\mathbb{Z}_p)$ is profinite. $\square$

Examples

Theorem
$SL_d(\mathbb{Z}_p)$ is profinite.

Proof.
Again, as closed subgroup of a profinite group is profinite, $SL_d(\mathbb{Z}_p)$ is a closed subgroup of $GL_d(\mathbb{Z}_p)$. $\square$

Formal Power Series

Definition

Let R be a commutative ring with identity. We define $R[[t]]$ to be the set of formal power series in some indeterminate variable t.

Formal Power Series

Definition

Let R be a commutative ring with identity. We define $R[[t]]$ to be the set of formal power series in some indeterminate variable t.

Definition

The field of fractions of $R[[t]]$ is denoted $R((t))$.

Formal Power Series

Definition

Let R be a commutative ring with identity. We define $R[[t]]$ to be the set of formal power series in some indeterminate variable t.

Definition

The field of fractions of $R[[t]]$ is denoted $R((t))$.

Abstractly we can think of $R[[t]]$ as the completion of the polynomial ring $R[t]$ equipped with a particular metric. Since this forms a complete metric space, this automatically gives $R[[t]]$ the structure of a topological ring. We've already seen this; the p-adic valuation induce a metric (and hence a topology) on $\mathbb{Z}_p$, but it can be different for different groups.

Formal Power Series

The topological ring $R[[t]]$ has multiplication and addition, defined as

$$\sum_{k=1}^{\infty} a_k t^k \; + \; \sum_{k=1}^{\infty} b_i t^i = \sum_{k=1}^{\infty} (a_k + b_k) t^k$$

Formal Power Series

The topological ring $R[[t]]$ has multiplication and addition, defined as

$$\sum_{k=1}^{\infty} a_k t^k \; + \; \sum_{k=1}^{\infty} b_i t^i = \sum_{k=1}^{\infty} (a_k + b_k) t^k$$

and

$$\left(\sum_{k=1}^{\infty} a_i t^i \right) \times \left(\sum_{k=1}^{\infty} b_i t^i \right) = \sum_{k=1}^{\infty} (\sum_{j=0}^{n} a_j b_{n-j}) t^k .$$

Formal Power Series

Let $f(t) = \sum_{k=1}^{\infty} a_k t^k$ and let $g(t) = \sum_{j=1}^{\infty} b_j t^j$. We can form the composition in the ring of formal power series as below.

$$g(f(t)) = \sum_{j=1}^{\infty} b_j (f(t))^j, = \sum_{j=1}^{\infty} b_j (\sum_{k=1}^{\infty} a_k t^k)^j = \sum_{n=1}^{\infty} c_n (t)^n.$$

The constants c_n are determined by multiplying out the power series explicitly, and can be written in the formula

$$c_n = \sum_{k=1}^{\infty} b_k a_{j_1} a_{j_2} \dots a_{j_k}$$

such that

$$j_1 + \cdots + j_k = n.$$

The Nottingham Group

Definition

Let A denote the group of continuous automorphisms of $\mathbb{F}_p((t))$ the group operation of function composition. An element of this group can be defined by its action on an indeterminate t, thusly.

$$tg = \sum_{i=0}^{\infty} a_i t^i, \quad a_i \in \mathbb{F}_p.$$

The Nottingham Group

Definition

Let A denote the group of continuous automorphisms of $\mathbb{F}_p((t))$ the group operation of function composition. An element of this group can be defined by its action on an indeterminate t, thusly.

$$tg = \sum_{i=0}^{\infty} a_i t^i, \quad a_i \in \mathbb{F}_p.$$

The Nottingham group $\mathcal{J} = \mathcal{J}(\mathbb{F}_p)$ is defined to be the subgroup of A which acts trivially on $(t)/(t^2)$, that is those automorphisms which have $a_0 = 0$ and $a_1 = 1$. Hence an element of $\mathcal{J}$ is written

$$tg = t + \sum_{i=2}^{\infty} a_i t^i, \quad a_i \in \mathbb{F}_p.$$

Subgroups of the Nottingham Group

Take some subset $I \subseteq \mathbb{N}$. We will call this an *admissable index set* if

$$\left\{ t + \sum_{i \in I} a_i t^i : a_i \in \mathbb{F}_p \right\}$$

forms a subgroup of $\mathcal{J}$. If it does, we call the subgroup and index subgroup of $\mathcal{J}$, denoted $\mathcal{J}[I]$.

The Fesenko groups are a special kind of index subgroup. Let $q = p^r$ for some $r \in \mathbb{N}$ and prime p. Then $T = T(r)$ is defined

$$\left\{ t + \sum_{k \geq 1} a_{q^{k+1}} t^{q^{k+1}} : a_{q^{k+1}} \in \mathbb{F}_p \right\}.$$

Subgroups of the Nottingham Group

This, among others, are generalised and classified by Barnea, and Klopsch, and the 4 types of index subgroups that appear are as follows:

$$\begin{aligned}
\mathcal{A}_x &:= J[x\mathbb{N}], \quad x \in \mathbb{N}. \\
\mathcal{B}_{r,s} &:= J[p^r\mathbb{N} \cup (p^s\mathbb{N} - 1)], \quad r, s \in \mathbb{N}; r \geq s. \\
\mathcal{C}_s &:= J[p^s\mathbb{N} - 1], \quad s \in \mathbb{N}. \\
\mathcal{D}_r &:= J[\{p^n - 1 : n \in \mathbb{N}\}].
\end{aligned}$$

References

- Johnson, D. L., *The Group of Formal Power Series Under Substitution*. J. Austral. Math. Soc. (Series A) 45 (1988), 296-302.
- Fesenko, I, *On just infinite pro-p-groups and arithmetically profinite extensions of local fields*.
- J.D. Dixon, M.P.F. du Sautoy, A. Mann, and D. Segal, (1991). *Analytic pro-p Groups*. Londom Mathematical Society Lecture Note Series 157.
- Rachel Camina, 1997. *Some Natural Subgroups of the Nottingham Group*, Proceedings of the Edinburgh Mathematical Society (1999) 42, 333-339.

The End

Any Questions?

The Nottingham Group

Theorem

Every finite p-group can be embedded as a closed subgroup into $\mathcal{J}$.

The Nottingham Group

Theorem

Every finite p-group can be embedded as a closed subgroup into $\mathcal{J}$.

Proof.

Let H be a finite p-group. Then "Witt's Algorithm" tells us there exists an extension field K of $\mathbb{F}_p((t))$ such that $H \cong \mathrm{Gal}(K/\mathbb{F}_p((t)))$.

The Nottingham Group

Theorem

Every finite p-group can be embedded as a closed subgroup into $\mathcal{J}$.

Proof.

Let H be a finite p-group. Then "Witt's Algorithm" tells us there exists an extension field K of $\mathbb{F}_p((t))$ such that $H \cong \mathrm{Gal}(K/\mathbb{F}_p((t)))$. We would then have a Galois extension field $\hat{K}$, but in fact we can simplify this, as K is a finite, totally ramified extension of $\mathbb{F}_p((t))$, which means $K \cong \mathbb{F}_p((t))$. Thus we have that $H \leq \mathrm{Aut}(\mathbb{F}_p((t)))$. Plus, $\mathcal{J}$ has index $p-1$ in $\mathrm{Aut}(\mathbb{F}_p((t)))$ and since $p-1$ is prime to p and $|H| = p^n$, for some n, we must have that $H \leq J$, as required. □

Witt's Algorithm

Theorem

Let Ω *be a subgroup of* k^+, *such that* $\mathcal{P}k \leq \Omega \leq k^+$ *and* $|\Omega/\mathcal{P}k|$ *is finite. Then* $\mathrm{Gal}(k(\mathcal{P}^{-1}\Omega)k) \cong \Omega/\mathcal{P}k$. *Further, for every abelian extension* K *of* k, *of exponent* p, *there exists a group* Ω *such that* $K = k(\mathcal{P}^{-1}\Omega)$.

Witt's Algorithm

The map $\mathcal{P}$ works as when in a field of characteristic p it is a subgroup of the additive group k^+ of k, by virtue of the fact that $x^p - x + y^p - y = (x + y)^p - (x + y)$. By ensuring the existence of the subgroup Ω, it allows us to use its preimage under $\mathcal{P}$ to define a Galois group which will be isomorphic to $\Omega/\mathcal{P}k$. We can reverse the process by choosing a such a group (p-groups identify naturally with abelian extensions) and embed the group into the Galois extension field. We now need to ensure that there is such a field.

Witt's Algorithm

Theorem

Let H be a finite p-group and $d(H)$ its minimal number of generators. For a field of characteristic p, let $[k : \mathcal{P}k] = p^N$ if it is finite, or ∞ if it is unbounded. Then there is a Galois extension field $\hat{K}$ such that $\mathrm{Gal}(\hat{K}/k) \cong H$ if and only if $d(H) \leq N$.

Index of $\mathcal{J}$

Theorem

i) $\mathcal{J}$ is profinite. ii) $\mathcal{J}$ is a normal subgroup of index $p-1$ in A.

Proof.

Define a chain of subsets $\mathcal{J}_n = \left\{g \in \mathcal{J} : tg \equiv t \mod t^{n+1}\right\}$. $\mathcal{J}_n \lhd \mathcal{J}$ and $|\mathcal{J}/\mathcal{J}_n| = p^{n-1}$ It can then be proved that $\mathcal{J} = \varprojlim \mathcal{J}/\mathcal{J}_n$. So $\mathcal{J}$ is a pro-p group, in fact, a finitely generated pro-p group. □

Proof.

Since $[t + at^i, t + bt^j] = t + ab(i-j)t^{i+j-1} + ...$, we can see $[\mathcal{J}_i, \mathcal{J}_j] \leq \mathcal{J}_{i+j-1}$ □