Pro-p Groups

Books: "Profinite Groups", by J.S. Wilson, (OUP)
"Analytic pro-p groups", by Dixon, du Sautoy, Mann, Segal, (CUP)

Motivation:
- They arise naturally as Galois groups of infinite algebraic extensions.
- They allow study of a family of p-groups in one go. (Eg, coclass conjectures.)
- Increasingly, people are interested in pro-p groups in their own right.

Pro-p groups are topological groups.

1. Topological Groups.

Definition: A topological group is a set G such that
(i) G is a group
(ii) G is a topological space.
(iii) the map $G \times G \to G$, $(x,y) \mapsto xy^{-1}$, is continuous.

Lemma 1.1. G, a topological group.
(a)
- the map $G \times G \to G$, $(x,y) \mapsto xy$ is continuous (ie, multiplication).
- the map $G \to G$, $x \mapsto x^{-1}$ is a homeomorphism.
- for each $g \in G$, the maps $G \to G$, $x \mapsto xg$ and $x \mapsto gx$ are homeomorphisms

Proof: Recall, if $\theta : G \to G$ and $\varphi : G \to G$ are continuous, then $G \to G \times G$, $x \mapsto (\theta(x), \varphi(x))$ is.
Inversion: $x \xmapsto{\text{cts}} (1,x) \xmapsto{\text{cts}} 1 \cdot x^{-1} = x^{-1}$, its own inverse, so a homeomorphism.
Multiplication: $(x,y) \xmapsto{\text{cts}} (x,y^{-1}) \mapsto xy$
Fix g: $x \mapsto (x,g^{-1}) \mapsto xg$

(b) $H \leq G$. If H is open (resp. closed) then every coset Hg is open (resp. closed).
Proof: From (a), since $H \to Hg$, $h \mapsto hg$ is a homeomorphism.

(c)
- Every open subgroup of G is closed.
- Every closed subgroup of finite index is open
- If G compact, every open subgroup of G has finite index.

Proof: exercise.

(d) $\emptyset \neq U \subseteq_o H \leq G \Rightarrow H$ open in G.
Proof: $H = \bigcup \{Uh : h \in G\}$ = union of open sets.

(e) $H \leq G$, $K \trianglelefteq G$.
- Then H is a topological group wrt subspace topology.
- G/K is a topological group wrt the quotient topology, and the quotient map $q : G \to G/K$ is open (ie, maps open sets to open sets)

Proof: (H - clear) Prove q open. Let $V \subseteq_o G$. By (a), $kV \subseteq_o G$ for each $k \in K$
$\Rightarrow V_1 = KV = \bigcup_{k \in K} kV$ is open. Now, $q(V) = q(V_1)$ and $q^{-1}(q(V_1)) = V_1$, open.
So $q^{-1}(q(V))$ open $\Rightarrow q(V)$ open by definition of quotient topology.

$$\begin{array}{ccc} G/K \times G/K & \longrightarrow & G/K \\ \uparrow q\times q,\ \text{open} & & \uparrow q,\ \text{cts} \\ G\times G & \xrightarrow[\text{cts}]{m} & G \end{array} \qquad \Rightarrow xy^{-1} \text{ is continuous in } G/K.$$

(f) • G is Hausdorff iff $\{1\}$ is a closed subset of G.
• $K \trianglelefteq G$, then G/K is Hausdorff iff K is a closed subset of G.
• G totally disconnected $\Rightarrow$ G Hausdorff.

Proof: • Recall, 1-element subsets in Hausdorff spaces are closed.
Need to prove: $\{1\}$ closed $\Rightarrow$ G Hausdorff. Let $a \neq b \in G$. From (a), any 1-element subset is closed, so $\{a^{-1}b\}$ is closed. So, $\exists\ U \leq_o G$ with $1 \in U$, $a^{-1}b \notin U$. Since $(x,y) \mapsto xy^{-1}$ continuous, the inverse image of U is open. So $\exists\ V, W \leq_o G$ with $1 \in V$, $1 \in W$ s.t. $VW^{-1} \leq U$.
So, $a^{-1}b \notin VW^{-1} \Rightarrow aV \cap bW = \phi$, ie disjoint open nbhds of a, b, ie. G Hausdorff.
• Statement about G/K follows - q is an open map.
• Finally, recall that in totally disconnected sets, all ~~subsets~~ singletons are closed.

(g) G compact, Hausdorff, then C, D closed $\Rightarrow$ CD closed.

Proof: Have C, D compact $\Rightarrow$ image of $C \times D \xrightarrow{\text{cts}} CD$ is compact $\Rightarrow$ CD closed (since G is Hausdorff).

(h) G compact, $(X_\lambda, \lambda \in \Lambda)$ a family of closed subsets s.t.
$\forall\ \lambda_1, \lambda_2 \in \Lambda$, $\exists\ \mu \in \Lambda$ s.t. $X_\mu \leq X_{\lambda_1} \cap X_{\lambda_2}$.
• If U closed subset of G then $\left(\bigcap_{\lambda\in\Lambda} X_\lambda\right) U = \bigcap_{\lambda\in\Lambda} X_\lambda U$.

Proof: Clearly $\left(\bigcap_{\lambda\in\Lambda} X_\lambda\right) U \leq \bigcap_{\lambda\in\Lambda} X_\lambda U$.
So we need to prove that $\bigcap_{\lambda\in\Lambda} X_\lambda U \leq \left(\bigcap_{\lambda\in\Lambda} X_\lambda\right) U$.
Suppose $g \notin \bigcap X_\lambda U$, then $gU^{-1} \cap (\bigcap X_\lambda) = \phi$. Now, G is compact, gU^{-1}, X_λ closed, so $\exists\ \lambda_1, \ldots, \lambda_n$ s.t. $gU^{-1} \cap X_{\lambda_1} \cap \cdots \cap X_{\lambda_n} = \phi$.
By the property (& induction), $\exists\ X_\mu \leq X_{\lambda_1} \cap \cdots \cap X_{\lambda_n} \Rightarrow gU^{-1} \cap X_\mu = \phi \Rightarrow g \notin X_\mu U$.

Examples: (a) Any abstract group with the discrete topology is a topological group.
(b) $(\mathbb{R}, +)$ wrt usual topology. It's connected, Hausdorff, not compact.
$(\mathbb{Z}, +)$ wrt subspace topology - discrete topology.
$(\mathbb{Q}, +)$ " " " - not discrete topology.
Also, $(\mathbb{Q}, +)$ is totally disconnected.
(c) $(\mathbb{R}^*, \times)$ wrt usual topology.
$(\mathbb{C}^*, \times)$ " " "
(d) $GL_n(\mathbb{R}) \leq \mathbb{R}^{n^2}$, subspace topology
- multiplication, inversion given by rational functions in $2n^2$ or n^2 variables $\Rightarrow$ continuous.
$GL_n(\mathbb{C})$.
(e) orthogonal group, $O_n(\mathbb{R}) \leq GL_n(\mathbb{R})$ - two connected components.
$SO_n = O_n^+ = \{M \in O_n(\mathbb{R}) : \det M = 1\}$ - connected component.

Note: Many people define topological groups by saying multiplication and inversion are continuous. In this case, it is important that both of these hold.

Eg: give $\mathbb{Z}$ the topology $\{\phi, \mathbb{Z}, [n,\infty)\}$.
'+' is continuous, but '$-$' is not continuous.

Lemma 1.2: G a compact topological group, $1 \in C \subseteq G$, C closed and open. Then C contains an open normal subgroup.

Proof: Let $x \in C$. Define $W_x = Cx^{-1}$, an open nbhd of 1 with $W_x x \subseteq C$.
Multiplication continuous, so $\exists$ open nbhds L_x, R_x with $1 \in L_x, 1 \in R_x$, s.t. $L_x R_x \subseteq W$. Let $S_x = L_x \cap R_x$, then $S_x S_x \subseteq W_x$. C is compact and $C = \bigcup_{x \in C} S_x x$, so $C = \bigcup_{i=1}^{n} S_{x_i} x_i$. Also, $1 \in S = \bigcap_{i=1}^{n} S_{x_i}$, open.

$(*)$ $SC \subseteq \bigcup_{i=1}^{n} S S_{x_i} x_i \subseteq \bigcup_{i=1}^{n} W_{x_i} x_i \subseteq C \Rightarrow SC \subseteq C$.

Let $T = S \cap S^{-1}$, open (inversion continuous). So $T = T^{-1}$, $1 \in T$.
Define $T^1 = T$, $T^n = T.T^{n-1}$, $H = \bigcup_{n \geq 1} T^n$. Ie, $H = \langle T \rangle$, open (union of cosets of T).
By $(*)$ and induction, $T^n \subseteq C$, so $H \subseteq C$. By 1.1(c), H has finite index.
Then, by orbit-stabiliser theorem, H has a finite number of conjugates (since $N_G(H) \geq H$ has finite index), call them $H^{g_1}, H^{g_2}, \ldots, H^{g_n}$, all open. Then $\bigcap_{i=1}^{n} H^{g_i}$ is open, normal.

Proposition 1.3: G a compact, totally disconnected, topological group.

(a) Every open set in G is a union of cosets of open normal subgroups.

(b) A subset of G is both open and closed iff it is a union of finitely many cosets of open normal subgroups.

(c) $X \subseteq G$, then $\overline{X} = \{XN : N \trianglelefteq_o G\}$.
In particular, if C closed, $C = \{CN : N \trianglelefteq_o G\}$ and $\{1\} = \bigcap \{N : N \trianglelefteq_o G\}$.

Proof: (a) By 1.1(f), G is Hausdorff. Let $\phi \neq U \subseteq_o G$. $x \in U \Rightarrow 1 \in Ux^{-1} \subseteq_o G$.
Handout (0.21) $\Rightarrow Ux^{-1} = \bigcup V_i$, V_i open and closed. $1 \in V_1$, say. Apply 1.2 to V_1.
Then $Kx \trianglelefteq_o Ux^{-1}$, $Kx \subseteq U$, so $U = \bigcup_{x \in U} K_x x$.

(b) Suppose P is both open and closed. By (a), $P = \bigcup K_i x_i$ with K_i open and normal
P compact, so $P = K_1 x_1 \cup \cdots \cup K_n x_n$.
Conversely, suppose $P = K_1 x_1 \cup \cdots \cup K_n x_n$. K_i open $\Rightarrow K_i x_i$ open $\Rightarrow P$ open.
Also, K_i open $\Rightarrow K_i$ closed $\Rightarrow P$ closed.

(c) Suppose $y \notin \overline{X}$. $\exists$ an open nbhd U of y s.t. $U \cap X = \phi$. Proof of (a) $\Rightarrow \exists N \trianglelefteq_o G$ s.t. $N \subseteq Uy^{-1}$, so $Ny \subseteq U$, so $Ny \cap X = \phi \Rightarrow y \notin NX$.

Lemma 1.4: Let $(G_\lambda : \lambda \in \Lambda)$ be a family of topological groups, and let $C = \Pi(X_\lambda : \lambda \in \Lambda)$, Cartesian product, elements (x_λ), $x_\lambda \in X_\lambda$. Define multiplication pointwise, ie $(x_\lambda)(y_\lambda) = (x_\lambda y_\lambda)$. Then C is a topological group.

Proof: Follows from definition of product topology, since G_λ is a topological group and pointwise multiplication ensures projections continuous.

Definition: A compact, totally disconnected topological group is called profinite.

Remark: To analysts, a profinite group is a compact, Hausdorff, topological group, modulo the connected component at the identity.

More commonly, one thinks of a profinite group as an "inverse limit of finite groups". The name comes from "projective limit of finite groups", where projective limit is an inverse limit with associated maps surjective. (Due to Serre).

2. Inverse Limits.

Definition: A directed set is a partially ordered set I s.t. $\forall i_1, i_2 \in I, \exists j \in I$ s.t. $j \geq i_1, j \geq i_2$.

Definition: An inverse system (X_i, φ_{ij}) of topological spaces indexed by a directed set I consists of:

- $(X_i, i \in I)$, a family of topological spaces
- $(\varphi_{ij} : X_j \to X_i, \ j \geq i)$, a family of continuous maps, s.t. $\varphi_{ii} = id_{X_i}\ \forall i$, and $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ for $i \leq j \leq k$.

Remarks: (a) If X_i are topological groups, φ_{ij} continuous homomorphisms, talk about inverse system of topological groups, etc.

(b) If X_i has no topology, give it the discrete topology.

Examples: (i) $I = \mathbb{N}$, $(X_i : i \in \mathbb{N})$ finite sets. $\varphi_{i,i+1} : X_{i+1} \to X_i$ arbitrary maps. Define $\varphi_{ii} = id_{X_i}$, $\varphi_{ij} = \varphi_{i,i+1}\varphi_{i+1,i+2}\cdots\varphi_{j-1,j}$, for $j \geq i$. Then (X_i, φ_{ij}) is an inverse system of finite sets. (We often think of towers.)

(ii) $I = \mathbb{N}$, p prime, $G_i = \mathbb{Z}/p^i\mathbb{Z}$. For $j \geq i$, $\varphi_{ij} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$, $n + p^j\mathbb{Z} \mapsto n + p^i\mathbb{Z}$. (G_i, φ_{ij}) inverse system of finite rings / groups. (Important example - see p-adic integers later.)

(iii) More generally, G a group, I a family of normal subgroups s.t. given $N_1, N_2 \in I$, $\exists M \in I$ s.t. $M \leq N_1 \cap N_2$. Define order on I: $N \geq M$ if $M \leq N$. Then we have natural maps $q_{NM} : G/M \to G/N$, $gM \mapsto gN$, for $M \geq N$, and $(G/N, q_{MN})$ is an inverse system.

Note: If G/M finite $\forall M \in I$, we can give G/M discrete topology. Then q_{MN} continuous and we have an inverse system of topological groups.

Definition: (X_i, φ_{ij}) an inverse system of topological spaces, Y a topological space. A family $(\psi_i : Y \to X_i)$ of continuous maps is compatible if ψ_j, ψ_i commutes. ($j \geq i$)

ie., $\varphi_{ij}\psi_j = \psi_i$.

Definition: Given an inverse system, we define the inverse limit to be the "universal" compatible object.

An *inverse limit* (X, φ_i) of an inverse system (X_i, φ_{ij}) of topological spaces (groups, rings) is a topological space (group, ring) X together with a compatible family $(\varphi_i : X \to X_i)$ of continuous maps (homomorphisms) with the following *universal property*:

- Given a space (group, ring) Y and $(\psi_i : Y \to X_i)$ a compatible family of continuous maps (homomorphisms), $\exists$ a unique continuous map (homomorphism) $\Psi : Y \to X$ s.t. $\begin{array}{ccc} & Y & \\ \Psi \swarrow & & \searrow \psi_i \\ X & \xrightarrow[\varphi_i]{} & X_i \end{array}$ commutes. Ie, $\varphi_i \Psi = \psi_i \ \forall i$.

The next result shows that inverse limits exist and are unique.

Proposition 2.1: (X_i, φ_{ij}) an inverse system.

(a) If (X, φ_i) and (Y, ψ_i) are inverse limits of (X_i, φ_{ij}), then $\exists$ an isomorphism $\bar{\varphi} : X \to Y$ s.t. $\psi_i \bar{\varphi} = \varphi_i \ \forall i$. (Ie, inverse limits are unique.)

(b) $C = \prod (X_i, i \in I)$, Cartesian product, $\pi_i : C \to X_i$, projection.
Define $X = \{ c \in C : \varphi_{ij} \pi_j(c) = \pi_i(c) \ \forall j \geq i \}$, and $\varphi_i = \pi_i|_X$.
Then (X, φ_i) is an inverse limit of (X_i, φ_{ij}). (Ie, they exist.)

(c) If X_i are topological groups, φ_{ij} group homomorphisms, ..., then X and φ_i ....

Notation: An inverse limit is denoted by $\varprojlim (X_i, \varphi_{ij})$, or just $\varprojlim X_i$.

Remark: Part (b) gives a useful way to visualise the inverse limit: $X \leq \prod X_i$ (subspace top'y; product top'y)
Those 'vectors' (x_i) s.t. $\varphi_{ij}(x_j) = x_i$.
So if we have a tower: $(x_1, x_2, \ldots, \underset{\varphi_{ij}}{\overset{\longleftarrow}{x_i}}, \ldots, x_j, \ldots)$.

Proof of 2.1: (a). By universality of (X, φ_i), $\exists$ map $\alpha : Y \to X$ s.t. $\varphi_i \alpha = \psi_i$.
By universality of (Y, ψ_i), $\exists$ map $\beta : X \to Y$ s.t. $\psi_i \beta = \varphi_i$.
By universal property for X, $\exists$ a unique map $\gamma : X \to X$ s.t. $\varphi_i \gamma = \varphi_i$;
but both $\gamma = \alpha\beta$ or id_X, so $\alpha\beta = id_X$. Similarly, $\beta\alpha = id_Y$. So α, β isomorphisms

(b) & (c). $X \leq \prod X_i$, then $\varphi_i = \pi|_X$, continuous, and $\varphi_{ij}\varphi_j = \varphi_i$ $(j \geq i)$, by definition of X. Ie, a compatible family.
Most of (c) follows - see lemma 1.4.
Need to check the universal property. Let $(\psi_i : Y \to X_i)$ is another compatible family of maps. Must show $\exists$ unique (continuous) map $\Psi : Y \to X$ s.t. $\varphi_i \Psi = \psi_i$.
Let $\bar{\Psi} : Y \to X$, $y \mapsto (\psi_i(y)) \in \prod X_i$. Then $\pi_i \bar{\Psi} = \psi_i \Rightarrow \bar{\Psi}$ continuous, since Ψ is.
Need $Y \to X$, if $j \geq i$. $\pi_i \bar{\Psi} = \psi_i = \varphi_{ij}\psi_j = \varphi_{ij}\pi_j\bar{\Psi}$. Ie, $\bar{\Psi} : Y \to X$.
And $\varphi_i \bar{\Psi} = (\pi_i|_X)\bar{\Psi} = \psi_i$.
Need uniqueness. Suppose $\Psi' : Y \to X$, $\varphi_i \Psi' = \psi_i$. Let $y \in Y$, then $(\pi_i|_X)\Psi'(y) = \psi_i(y)$, ie. the entry of y in X_i is $\psi_i(y) \Rightarrow \Psi'(y) = \Psi(y)$.
Finally, if (X_i, φ_{ij}) an inverse system of groups and maps $\psi_i : Y \to X_i$ group homomorphisms, then $\bar{\Psi} : Y \to \prod X_i$, $y \mapsto (\psi_i(y))$ is a group homomorphism, since each ψ_i is.

Definition:- (a) A profinite group is an inverse limit of finite groups.
(b) A pro-p group is an inverse limit of finite p-groups.

Example: • Γ group, I family of normal subgroups (of finite index) s.t. given $N_1, N_2 \in I$, $\exists\, M \leq N_1 \cap N_2$, $M \in I$, then $\hat{\Gamma}_I = \varprojlim (\Gamma/N)_{N\in I}$ - a profinite completion of Γ.
Note, natural homomorphism $\Gamma \to \pi(\Gamma/N)$, $g \mapsto gN$, kernel $= \cap N$.
• When $I = \{$all normal subgroups of finite index$\}$, $\hat{\Gamma}_I =$ the profinite completion.
• when $I = \{$all normal subgroups of p-power index$\}$, $\hat{\Gamma}_I = \hat{\Gamma}_p =$ the pro-p completion of Γ, a pro-p group.

Proposition 2.2: (X_i, φ_{ij}) an inverse system. Let $X = \varprojlim X_i$.
(a) each X_i Hausdorff $\Rightarrow$ X Hausdorff
(b) each X_i totally disconnected $\Rightarrow$ X totally disconnected
(c) each X_i Hausdorff $\Rightarrow$ $X = \{c \in C : \varphi_{ij}\pi_j(c) = \pi_i(c) \ \forall j \geq i\} \leq \pi X_i$.
Ie, X is closed in πX_i.
(d) each X_i Hausdorff and compact $\Rightarrow$ X Hausdorff and compact
(e) each X_i Hausdorff and $X_i \neq \phi \Rightarrow X \neq \phi$.

Prof: (a) & (b) follow since πX_i is Hausdorff and totally disconnected.
(c) Use: $f, g : X \to Y$ continuous maps, Y Hausdorff, then $\{x : f(x) = g(x)\}$ closed in X.
Then $X = \bigcap_{j\geq i} \{c \in C : \underbrace{\varphi_{ij}\pi_j(c)}_{\text{(cts)}} = \underbrace{\pi_i(c)}_{\text{(cts)}}\}$ - intersection of closed sets, so is closed.

(d) By (c), X closed in compact in πX_i, so is compact.
(e) $j > i$, set $D_{ij} = \{c \in \pi X_i : \varphi_{ij}\pi_j(c) = \pi_i(c)\}$, closed.
Suppose (for a contradiction), $X = \phi$, so $\bigcap D_{ij} = \phi$. Since πX_i compact, $\exists\, n$ s.t. $\bigcap_{r=1}^{n} D_{i_r j_r} = \phi$, some (i_r, j_r). I a directed set, so $\exists\, k \in I$, $k \geq j_r\ \forall r$.
Choose $x_k \in X_k$, define $x_l = \varphi_{lk}(x_k)$, $l \leq k$, and x_l arbitrarily if $l > k$.
So $(x_i) \in \bigcap_{r=1}^{n} D_{i_r j_r}$. #.

Proposition 2.3: $(X, \varphi_i) = \varprojlim (X_i, \varphi_{ij})$, $\phi \neq X_i$, compact, Hausdorff. Then,
(a) $\varphi_i(X) = \bigcap_{j\geq i} \varphi_{ij}(X_j)$
(b) The sets $\varphi_i^{-1}(U)$, U open in X_i, form a base for the topology on X.
(c) If $Y \leq X$ s.t. $\varphi_i(Y) = X_i$, then Y is dense in X, ie $\overline{Y} = X$.
(d) If $\theta : Y \to X$, then θ is continuous iff $\varphi_i\theta$ is continuous for each i.

Prof: (a) $\varphi_i(X) = \underset{\text{compatible}}{\varphi_{ij}\varphi_j(X)} \leq \varphi_{ij}(X_j)$, so $\varphi_i(X) \leq \bigcap_{j\geq i} \varphi_{ij}(X_j)$.
The other way: fix i, let $a \in \bigcap_{j\geq i} \varphi_{ij}(X_j)$. Aim to find b s.t. $\varphi_i(b) = a$.
Set $Y_j = \{y \in X_j : \varphi_{ij}(y) = a\} \leq X_j$, closed (inverse image of $\{a\}$, closed).
X_j compact $\Rightarrow$ Y_j compact. If $i \leq j \leq k$ and $y_k \in Y_k$, then $\varphi_{ij}(\varphi_{jk}(y_k)) = \varphi_{ik}(y_k) = a$.
$\Rightarrow$ $\varphi_{ik}(y_k) \in Y_j$. Ie $\varphi_{jk} : Y_k \to Y_j$. So $\{Y_j : j \geq i\}$ is an inverse system of non-empty, compact, Hausdorff spaces, so $\exists (b_j) \in \varprojlim Y_j$.
So, $\varphi_{jk}(b_k) = b_j$, $i \leq j \leq k$, and $b_i = a$. If $l \in I$, $l \not\leq k$, $\exists\, j \geq i, l$, so define $b_l = \varphi_{lj}(b_j)$ (defined since $j \geq i$). This is well-defined, since if $j' \geq i, l$, then $\exists\, k \geq j, j'$, and $\varphi_{lj}(b_j) = \varphi_{lj}(\varphi_{jk}(b_k)) = \varphi_{lj'}(\varphi_{j'k}(b_k)) = \varphi_{lj'}(b_{j'})$. So, $\varphi_{jk}(b_k) = b_j\ \forall\ j \leq k$.
$\Rightarrow$ $b = (b_j)_{j\in I} \in X$, and $\varphi_i(b) = b_i = a \Rightarrow a \in \varphi_i(X)$.

(b). Open set in X is union of sets of form $P = X \cap \pi_{i_1}^{-1}(U_1) \cap \cdots \cap \pi_{i_r}^{-1}(U_r)$, some $U_{i_r} \subseteq_o X_r$ (definition of product and subspace topology).
Need to prove: $a \in P$, $\exists\, U$ open in X_k s.t. $a \in \varphi_k^{-1}(U) \subseteq P$.
Let $a = (a_i) \in P$, choose $k \geq i_1, \ldots, i_n$. Then $\varphi_{i_r k}^{-1}(U_r) \subseteq_o X_k$, and $\varphi_{ik}(a_k) = a_i$
$\Rightarrow a_k \in \varphi_{i_r k}^{-1}(U_r)$.
Set $U = \bigcap_{r=1}^{n} \varphi_{i_r k}^{-1}(U_r) \subseteq_o X_k$, and $a_k \in U$. $\Rightarrow \varphi_k^{-1}(U)$ an open nbhd of a in X.
Need $\varphi_k^{-1}(U) \subseteq P$. Let $b = (b_i) \in \varphi_k^{-1}(U) \Rightarrow b_k \in U \Rightarrow b_{i_r} = \varphi_{i_r k}(b_k) \in U_r$.
Ie, $\varphi_k^{-1}(U) \subseteq P$, as required.

(c) Take $\phi \neq U \subseteq_o X_i$, then $\varphi_i(Y) \cap U \neq \phi$. $\Rightarrow Y \cap \varphi^{-1}(U_i) \neq \phi$. So by (b), Y meets all open sets of basis $\Rightarrow \overline{Y} = X$.

(d) • θ continuous $\Rightarrow \varphi_i \theta$ continuous since φ_i is.
• $\varphi_i \theta$ continuous, composition with each projection continuous $\Rightarrow \theta$ continuous
(Or use (b)).

Proposition 2.4: X compact, Hausdorff, totally disconnected space. Then X is the inverse limit of its discrete quotient spaces.

Proof: Let $I = \{$partitions of X into finitely many open & closed sets$\}$. For $i \in I$, let X_i be the corresponding quotient space, $= X/p_i$ - elements are closed & open subsets of partition.
Quotient map, $q_i : X \to X_i$. Note, X compact, so a discrete quotient is finite.
So the X_i above are precisely the quotient spaces which are discrete in the quotient topology.
Define $i \leq j$ iff $\exists$ map $q_{ij} : X_j \to X_i$ s.t. $q_i = q_{ij} q_j$. q_i surjective $\Rightarrow q_{ij}$ unique.
I is a partially ordered set: $i = \{U_r : 1 \leq r \leq m\}$, $j = \{V_s : 1 \leq s \leq n\}$, then let
$k = \{U_r \cap V_s : 1 \leq r \leq m,\ 1 \leq s \leq n\} \in I$. $i, j \leq k$, $q_{ik} : X_k \to X_i$, $U_r \cap V_s \to U_r \Rightarrow I$ a directed set.
q_{ij} uniquely determined $\Rightarrow (X_i, q_{ij})$ is an inverse system, and (X, q_i) a compatible family.
Let $Y = \varprojlim X_i$, $\hat{q}_i : Y \to X_i$. Universal property $\Rightarrow \exists$ continuous $\nu : X \to Y$, $\hat{q}_i \nu = q_i$.
(Aim: show ν is a homeomorphism.) ν is injective: $x_1, x_2 \in X$. Suppose $\nu(x_1) = \nu(x_2)$
$\Rightarrow q_i(x_1) = q_i(x_2)\ \forall i$. Ie, no closed & open set contains just one of x_1 & $x_2 \Rightarrow x_1 = x_2$.
And ν is surjective: Since $\hat{q}_i(\nu(X)) = q_i(X) = X_i$. (2.3)(c) $\Rightarrow \nu(X)$ dense in Y.
ν continuous, X compact, Y Hausdorff $\Rightarrow \nu(X)$ closed, ie $\nu(X) = Y$.
Use: $f : X \to Y$ continuous bijection from compact X to Hausdorff Y then f a homeomorphism.
$\Rightarrow \nu$ a homeomorphism, as required.

3. Characterisations of Profinite Groups.

Definition: A family I of normal subgroups of a group G is called a **filter base** if
$\forall\, K_1, K_2 \in I$, $\exists\, K_3 \in I$ s.t. $K_3 \subseteq K_1 \cap K_2$

Proposition 3.1: $(G, \varphi_i) = \varprojlim G_i$, G_i compact, Hausdorff groups. Let $L \trianglelefteq_o G$.
Then $\ker \varphi_i \leq L$, some i, $\Rightarrow$ • $G/L \cong$ a quotient group of some subgroup of G_i,
• further if φ_i surjective for each i, then $G/L \cong$ a quotient group of a G_i.

Proof: $1 \in L$ open $\Rightarrow \varphi_i^{-1}(U) \subseteq L$, some i and some $U \subseteq_o G_i$, $1 \in U$, by (2.3)(b). $\Rightarrow \ker \varphi_i \leq L$.
$\Rightarrow G/L \cong (G/\ker\varphi_i)/(L/\ker\varphi_i) \cong \operatorname{im}\varphi_i/(L/\ker\varphi_i)$.

Proposition 3.2: G a topological group, I a filter base of closed normal subgroups. Then $(G/K, \varphi_{LK})$ is an inverse system (as before). Let $(\hat{G}, \varphi_K) = \varprojlim G/K$. Then $\exists$ continuous $\theta: G \to \hat{G}, g \mapsto (gK)$, with $\ker\theta = \bigcap_{K\in I} K$, and $\overline{\theta G} = \hat{G}$. Also, $\varphi_K\theta$ is the quotient map $G \to G/K$.
If G compact, then θ is surjective. G compact, $\cap K = 1 \Rightarrow \theta$ an isomorphism of topological groups

Proof: Seen most of this before. Note, $\varphi_K\theta$ continuous $\forall K \Rightarrow \theta$ continuous. Also, $\varphi_K\theta(G) = G/K$ $\Rightarrow \overline{\theta G} = \hat{G}$, by (2.3)(c). (1.1)(f) $\Rightarrow G/K$ Hausdorff (K closed). G compact $\Rightarrow \theta(G)$ compact (as θ continuous) $\Rightarrow \theta(G)$ closed ($\hat{G}$ Hausdorff) $\Rightarrow \theta G = \hat{G}$.

Let $\mathcal{C}$ denote all finite (or p-) groups (Closed under subgroups, direct products, quotients.)
G is a pro$\mathcal{C}$ group if it is an inverse limit of finite $\mathcal{C}$-groups.

Theorem 3.3. G a ~~profinite~~ topological group. The following are equivalent.

(i) G is a pro-$\mathcal{C}$ group.

(ii) G isomorphic (as a topological group) to a closed subgroup of a Cartesian product of $\mathcal{C}$-groups.

(iii) G compact and $\bigcap(N: N \trianglelefteq_o G,\ G/N \in \mathcal{C}) = 1$.

(iv) G compact, totally disconnected and $G/L \in \mathcal{C}\ \forall\ L \trianglelefteq_o G$.

Proof: (i) $\Rightarrow$ (ii): By (2.2)(c) - closure.

(ii) $\Rightarrow$ (iii): Suppose $G \cong \hat{G} \leq_o \prod G_i$, G_i finite $\mathcal{C}$-groups. Let $K_i = \ker\pi_i$, π_i projection: $\prod G_i \to G_i$. $\prod G_i$ compact $\Rightarrow \hat{G}$ compact. Let $N_i = K_i \cap \hat{G}$. $K_i \trianglelefteq_o \prod G_i$. $\Rightarrow N_i \trianglelefteq_o \hat{G}$.
Also, $\cap K_i = 1$, $\Rightarrow \cap N_i = 1$. But $\hat{G}/N_i \cong \hat{G}/K_i \cap \hat{G} \cong \hat{G}K_i/K_i \leq \prod G_i/K_i \cong G_i \in \mathcal{C}$.

(iii) $\Rightarrow$ (i) Let $I = \{N \trianglelefteq_o G: G/N \in \mathcal{C}\}$. Claim I is a filter base. Let $N_1, N_2 \in I$, and $\theta: G \to G/N_1 \times G/N_2$, $g \mapsto (gN_1, gN_2)$ - $\mathcal{C}$-group. θ continuous and $\ker\theta = N_1 \cap N_2 \trianglelefteq G$ $\Rightarrow N_1 \cap N_2 \in I$. Then use (3.2).

(i) $\Rightarrow$ (iv) (2.2) $\Rightarrow$ G compact, totally disconnected. The rest by (3.1).

(iv) $\Rightarrow$ (iii) By (1.3)

Remark: (a) If $\mathcal{C}$ is the class of all finite groups (ie, talking about profinite groups), then (iv) becomes: "G compact and totally disconnected".

(b) Another interesting class is procyclic groups (& inverse limits of cyclic groups), but note that the proof of (iii) $\Rightarrow$ (i) goes wrong.

Theorem 3.4: (a) G a profinite group, I a filter base of normal closed subgroups s.t. $\cap\{N: N \in I\} = 1$. Then $G \cong \varprojlim G/N$. For each $H \leq_c G$, $H \cong \varprojlim H/H\cap N$, and for $K \trianglelefteq_c G$, $G/K \cong \varprojlim G/KN$.

(b) Cartesian products, inverse limits, and quotients (by closed normal subgroups), subgroups, of profinite / pro-p groups, are profinite / pro-p groups.

Proof: (a) See (3.2) for G, H. For G/K, claim $J = \{KN: N \in I\}$ is a filter base of closed, normal subgroups containing K. Since $N_3 \leq N_1 \cap N_2 \Rightarrow KN_3 \leq K(N_1 \cap N_2) \leq KN_1 \cap KN_2$.
By (1.1)(h), $\cap\{M: M \in J\} = K \cap \{N: N \in I\} = K$.

(b) See (a) for subgroups and quotients. Note, Cartesian products of Cartesian products are Cartesian products - so use (3.3) ((i) $\Rightarrow$ (iii)). Note, inverse limits $\cong$ closed subgroups of Cartesian products.

4. Examples.

(1). $\mathbb{Z}_p$, the p-adic integers, "prototype of all pro-p groups".

Let $\mathbb{Z}_p = \{$ formal infinite sums $\sum_{j=0}^{\infty} a_j p^j$, $0 \le a_j < p \}$.

Define $\theta_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$, $\sum a_j p^j \mapsto \sum_{j=0}^{i-1} a_j p^j + p^i\mathbb{Z}$, and $\theta : \mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^i\mathbb{Z}$, $z \mapsto (\theta_i(z), i \ge 1)$.

Clearly injective. Surjective? ~~Let~~ $x = \{x_i + p^i\mathbb{Z}, i \ge 0\} \in \varprojlim \mathbb{Z}/p^i\mathbb{Z}$. Since $x_{i+1} + p^{i+1}\mathbb{Z} \mapsto x_i + p^i\mathbb{Z}$
$\Rightarrow p^i \mid (x_{i+1} - x_i)$, ie, $x_{i+1} - x_i = a_i p^i$, some $0 \le a_i < p$. This is how to find the a_i.

Addition: $\theta^{-1}(\theta(z_1) + \theta(z_2))$, multiplication: $\theta^{-1}[\theta(z_1)\theta(z_2)]$ – componentwise.

Then $\mathbb{Z}_p$ is a pro-p ring, or additively a pro-p group.

Also, $\mathbb{Z} \to \mathbb{Z}_p$. (What is -1?), and $\hat{\mathbb{Z}} = \mathbb{Z}_p$, and addition and multiplication defined above extends the usuals in $\mathbb{Z}$.

Remark: G a pro-p group. The following are equivalent.

(i) G is procyclic

(ii) G is either finite and cyclic, or $G \cong \mathbb{Z}_p$ (topologically).

Alternatively, we take the completion of $\mathbb{Q}$ wrt the p-adic absolute value.

$x = p^n a/b \in \mathbb{Q}$, $n \in \mathbb{Z}$, $(a,b) = 1$, $p \nmid ab$.

$\nu_p(x) = n$, $|x|_p = p^{-n}$ (and $|0|_p = 0$).

This satisfies: $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$, and (N1) $|x|_p \ge 0$, equality iff $x = 0$.

(N2) $|1|_p = 1$, $|xy|_p \le |x|_p |y|_p$

(N3) $|x+y|_p \le \max\{|x|_p, |y|_p\}$.

So it is a norm on $\mathbb{Q}$, and $(x,y) \mapsto |x-y|_p$ is a metric on $\mathbb{Q}$.

The completion of $\mathbb{Q}$ wrt this metric is $\mathbb{Q}_p$, the p-adic field.

If $\alpha \in \mathbb{Q}_p$, $\alpha = \lim_{i\to\infty} x_i$, x_i a Cauchy sequence in $\mathbb{Q}$. Set $|\alpha|_p = \lim_{i\to\infty} |x_i|_p$.

The valuation ring in $\mathbb{Q}_p$ is the subring of p-adic integers. $\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : |\alpha|_p \le 1\}$.

(2) p-adic analytic groups.

Definition: G is p-adic analytic if G has the structure of a p-adic manifold and $G \times G \to G$, $(x,y) \mapsto xy^{-1}$ is analytic. A manifold – locally looks like $\mathbb{Z}_p$.

We can replace the analytic definition with an algebraic one.

Theorem: A topological group is p-adic analytic iff G has an open subgroup which is a uniform pro-p group.

ie, a p-adic analytic group is virtually pro-p.

Definition: G is virtually <property> if $\exists N \trianglelefteq G$, G/N finite and N has <property>.

Examples of p-adic analytic pro-p groups.

(i) $\{g \in GL_n(\mathbb{Z}_p),\ g \equiv I_n \pmod{p^i}\} = \Gamma_i$, $i \geq 1$.

(ii) p-adic space groups, G. $T \trianglelefteq_o G$, $G/T \cong P$, finite p-group. Point group.

Definition: A group G is linear if $\exists\ \varphi: G \hookrightarrow GL_n(\mathbb{F})$, injective homomorphism, some n, some field $\mathbb{F}$.

Aim: Uniform pro-p groups are linear.

$\Rightarrow$ p-adic analytic groups are linear.

(3) Λ-analytic pro-p groups.

These are pro-p groups with an analytic structure over some pro-p ring Λ.

Eg, $\Lambda = \mathbb{Z}_p[[t_1, \ldots, t_n]]$ or $\mathbb{F}_p[[t_1, \ldots, t_n]]$

Conjecture: such pro-p groups are linear.

Recent results $\Rightarrow$ $\mathbb{Z}_p[[t_1, \ldots, t_n]]$ - analytic pro-p groups are linear. But $\mathbb{F}_p[[t_1, \ldots, t_n]]$ - analytic pro-p groups are still unknown.

(4) Nottingham group, J.

Elements are formal power series of the form $f = t\left(1 + \sum_{k=1}^{\infty} a_k t^k\right) \in \mathbb{F}_p[[t]]$, $a_i \in \mathbb{F}_p$.

Operation is formal substitution: $fg = g\left(1 + \sum_{k=1}^{\infty} a_k g^k\right)$.

Eg. If $f = t + t^2$, $g = t + t^3$, then $fg = (t+t^3) + (t+t^3)^2 = t + t^2 + t^3 + 2t^4 + t^6$.

(Think about inverses.)

$J_n = \{f \in J : f \equiv t \pmod{t^{n+1}}\} \trianglelefteq J$. $\quad (f = t + a_n t^{n+1} + a_{n+1} t^{n+2} + \ldots)$

Let $e_n = t + t^{n+1}$, $J = \overline{\langle e_1, e_2 \ldots \rangle}$, and $[e_n, e_m] \equiv t(1 + (n-m)t^{n+m}) \bmod \langle t^{m+n+2} \rangle$

$\equiv e_{n+m}^{n-m} \bmod \langle t^{m+n+2} \rangle$

And $J \cong \varprojlim J/J_n$, a pro-p group. ($J/J_n$ are finite p-groups.)

J has nice commutator structure, but unwieldy p-power structure.

We can also think of J as a group of automorphisms of the field $\mathbb{F}_p((t)) = \left\{\sum_{i=-k}^{\infty} a_i t^i\right\}$, the finitely-tailed Laurent Series. Now think of f as the map $f: t \mapsto t\left(1 + \sum_{k=1}^{\infty} a_k t^k\right)$, then fg is the usual composition of maps. Number theorists call this the group of wild automorphisms.

Using this setting we can prove that every finite p-group arises as a subgroup of J.

$\Rightarrow$ J is not linear.

(Since, suppose J linear, $J \hookrightarrow GL_n(k)$ $\Rightarrow$ soluble subgroups of J have bounded derived length. But derived length of finite p-groups is unbounded.)

(5) Grigorchuk group.

Let T be a binary tree. Let A be $\mathrm{Aut}(T)$. We can give A a topology.

Define depth(vertex) = p, distance to root. Let $M_p = \{\alpha \in A : \alpha \text{ fixes every vertex of depth } p\} \leq A$.

Then $\{M_p : p \geq 0\}$ is a basis of nbhds of 1. In this way, A becomes a profinite group.

$T =$ 

, $T_1, T_2 \cong T$.

If $f \in M_1$, write f as (f_1, f_2) with $f_1 \in Aut(T_1)$, $f_2 \in Aut(T_2)$.
Define $f, g, h \in A$ recursively: $f = (g, \pi)$, $g = (h, \pi)$, $h = (f, 1)$.
Let $G = \langle \pi, f, g, h \rangle \leq A$, an infinite 2-group. $\overline{G}$ is a pro-2 group - contains every 2-group, not linear.
Gupta & Sidki have constructed similar groups for odd primes.

(6) Free pro-p groups

X a finite set, $F = F(X)$, the free group on X. Then the pro-p completion, $\hat{F}_p$, is a free pro-p group. ie, it satisfies the following universal property:

- given map $\varphi : X \to G$, G a pro-p group, $\exists$ a continuous homomorphism $\bar{\varphi} : \hat{F}_p \to G$ which extends φ.

5. Basic Properties.

Definition: $X \subseteq G$, a topological group. X generates G topologically if $\overline{\langle X \rangle} = G$.
The topological group is finitely-generated (f.g.) if $G = \overline{\langle X \rangle}$ and $|X|$ finite.
If $|X| = d$, we say $d(G) = d$, if this d is minimal.

Proposition 5.1: G profinite, $H \leq_c G$.
(i) $\overline{\langle X \rangle} = H$ iff XN/N generates HN/N $\forall N \trianglelefteq_o G$.
(ii) $d \in \mathbb{Z}^+$. If $d(HN/N) \leq d$ $\forall N \trianglelefteq_o G$ then $d(H) \leq d$.

Proof: (i) Recall $\overline{X} = \bigcap_{N \trianglelefteq_o G} XN$. So '$\Rightarrow$' clear. For '$\Leftarrow$', $\overline{\langle X \rangle} = \bigcap \langle X \rangle N = \bigcap HN = H$.
(ii) Each $N \trianglelefteq_o G$. Let $Y_N = \{(y_1 N, \dots, y_d N) \in (G/N)^d : \langle y_1 N, \dots, y_d N \rangle = HN/N\} \neq \phi$, finite.
$\pi_{MN} : G/M \to G/N$, $M \leq N$, $M, N \trianglelefteq_o G$, then $\pi_{MN}(Y_M) \subseteq Y_N$. ie, Y_M form an inverse system.
So the inverse limit $\neq \phi$, so let $(X_N) \in \varprojlim Y_N$. So $\exists x_1, \dots, x_d \in G$ s.t. for each $N \trianglelefteq_o G$, $X_N = (x_1 N, \dots, x_d N) \Rightarrow \overline{\langle x_1, \dots, x_d \rangle} = H$, by (i).

Proposition 5.2: G a f.g. profinite group, then every open subgroup of G is f.g.
Proof: Let $X \subseteq G$, $|X|$ finite, $G = \overline{\langle X \rangle}$, suppose wlog $X^{-1} = X$.
$H \trianglelefteq_o G$. T = transversal to the right cosets of H containing 1.
$T = \{1, t_1, \dots, t_n\}$ s.t. $G = H \cup Ht_1 \cup \dots \cup Ht_n$. For $x \in X$, $t \in T$, $\exists\, s = s(t,x) \in T$ s.t. $Htx = Hs$. Let $Y = \{tx.s(t,x)^{-1} : t \in T, x \in X\} \subseteq H$. Claim $\overline{\langle Y \rangle} = H$.
Let $M = \overline{\langle Y \rangle}$. If $a \in M$, $t \in T$, $x \in X$, then $at.x = atxs(t,x)^{-1}.s(t,x) \in MT$.
ie $MTX = MT$. Since $1 \in MT \Rightarrow X \subseteq MT$, so induction $\Rightarrow X^n \subseteq MT$. But $X = X^{-1} \Rightarrow \langle X \rangle \subseteq MT$.
T is finite, so $MT = \bigcup Mt_i$, so it is closed. $\Rightarrow G = \overline{\langle X \rangle} = MT$.
But $M \leq H \Rightarrow H = MT \cap H = M(T \cap H) = M$.

Definition: G a profinite group. The Frattini subgroup of G is $\Phi(G) = \bigcap \{M : M \text{ maximal, proper } \leq_o G\}$.

Proposition 5.3: G a profinite group.

(i) $\Phi(G) \trianglelefteq_c G$.

(ii) $K \trianglelefteq_c G$, $K \leq \Phi(G) \Rightarrow \Phi(G/K) = \Phi(G)/K$.

(iii) For $X \subseteq G$, the following are equivalent:

(a) $\overline{\langle X \rangle} = G$

(b) $X \cup \Phi(G)$ generates G topologically.

(c) $X\Phi(G)/\Phi(G)$ generates $G/\Phi(G)$ topologically. (Ie, $\Phi(G)$ known as "non-generators" of G.)

Proof: (i) M closed $\Rightarrow$ $\Phi(G)$ closed. Clearly a subgroup. If M maximal, open, so is $g^{-1}Mg$.

(ii) Ie, L/K maximal in G/K, write $L = M$, M maximal in G, since $\Phi(G) \leq K$.

(iii) (a) $\Rightarrow$ (b) is okay.

(b) $\Rightarrow$ (c) $X\Phi(G) \geq X \cup \Phi(G)$

(c) $\Rightarrow$ (a) Let $K \leq_o G$, suppose $X \subseteq K$. If $K \neq G \Rightarrow K \leq M$, some maximal open M.

$\Rightarrow \overline{\langle X \rangle}\Phi(G)/\Phi(G) \leq M/\Phi(G) \neq G/\Phi(G)$ ↯.

So $K = G \Rightarrow \overline{\langle X \rangle} = G$ by exercise 5.

Recall: In a finite p-group, $\Phi(G) = [G,G]G^p$, where $G^p = \langle g^p : g \in G \rangle$

Proposition 5.4: If G is a pro-p group, then $\Phi(G) = \overline{G^p[G,G]}$

Proof: Let M be a maximal open proper subgroup of G. $\exists\, N \trianglelefteq_o G$ s.t. $N \leq M$ (by 1.2). So M/N is maximal, proper in G/N. Recall, in a finite p-group, maximal open subgroups are normal and of index p. $\Rightarrow M \trianglelefteq G$ and $|G:M| = p$, $\Rightarrow G^p[G,G] \leq M$.

$\Rightarrow \Phi(G) = \bigcap M \geq G^p[G,G]$. $\Phi(G)$ closed (by 5.3) $\Rightarrow \Phi(G) \geq \overline{G^p[G,G]}$.

Now, let $Q = G/\overline{G^p[G,G]}$ - a pro-p group. (1.3) $\Rightarrow$ open normal subgroups of Q intersect in $\{1\}$. If $N \trianglelefteq_o Q \Rightarrow Q/N$ finite elementary abelian p-group ($\cong C_p \times \cdots \times C_p$).

$\Rightarrow \Phi(Q/N) = 1$ (by result about finite p-groups). $\therefore \Phi(Q) = \bigcap_{N \trianglelefteq_o Q} N = 1$.

By (5.3)(ii), $\Phi(G)/\overline{G^p[G,G]} = \Phi(Q) = 1$.

Proposition 5.6: G a pro-p group. G f.g. $\Leftrightarrow$ $\Phi(G)$ open in G.

Remark:
- Nottingham group J has $d(J) = 2$.
- Grigorchuk group $\bar{G}$ has $d(\bar{G}) = 3$.

Notes (i) We defined $\varphi_{ij} : X_j \to X_i$, $j \geq i$, written on left. Then $\varphi_{ij}\varphi_{jk} : X_k \to X_j \to X_i$, $k \geq j \geq i$. If we write f on the right, the indices change $x_j f_{ji}$, $x_k f_{kj} f_{ji} = x_i$, $k \geq j \geq i$. (Hence $\pi_{MN} : G/M \to G/N$.)

(ii) Proposition 5.1(ii) should read: If $d(HN/N) \leq d$ $\forall$ $N \trianglelefteq_o G \Rightarrow d(H) \leq d$.

Proof of 5.6: ($\Leftarrow$). $\Phi(G)$ is open $\Rightarrow G/\Phi(G)$ is finite. So $\exists\, X \subseteq G$ s.t. $|X|$ finite and $G = X\Phi(G)$

$\Rightarrow \overline{\langle X \rangle} = G$ by (5.3)

($\Rightarrow$) Suppose $G = \overline{\langle X \rangle}$, $|X| = d$. If $\Phi(G) \leq N \trianglelefteq_o G \overset{(5.4)}{\Rightarrow} G/N$ is an elementary abelian p-group, and can be generated by d elements. $\Rightarrow |G:N| \leq p^d$.

Among all such N, choose one, N_0 say, of maximal index. Then $N_0 \leq N$ whenever $\Phi(G) \leq N \trianglelefteq_o G$ (since we can take intersections). Since $\Phi(G)$ closed and normal in G.

$\Rightarrow \Phi(G) = \overline{\Phi(G)} = \bigcap \{N : \Phi(G) \leq N \trianglelefteq_o G\} = N_0$. Ie, $\Phi(G)$ open.

Commutators.

Definition: G a group, $x, y \in G$. The **commutator** $[y,x] = y^{-1}x^{-1}yx \in G$.
If $x_1, \dots, x_n \in G$, the **left-normed commutator** $[x_1, \dots, x_k] = [[x_1, \dots, x_{k-1}], x_k]$, inductively.

Commutator Identities:

(a) $[xy, z] = [x,z]^y [y,z]$, & $[x, yz] = [x,z][x,y]^z$.

(b) $[x^n, y] = [x,y]^{x^{n-1}} [x,y]^{x^{n-2}} \cdots [x,y]^x [x,y]$.
$[x, y^n] = [x,y][x,y]^y \cdots [x,y]^{y^{n-1}}$.

(c) $(xy)^n \equiv x^n y^n [y,x]^{n(n-1)/2} \mod \gamma_3(G)$ - 3rd term of lower central series.

(d) $[x, y^{-1}] = [y,x]^{y^{-1}}$, $[x^{-1}, y] = [y,x]^{x^{-1}}$.

(e) Hall-Witt identity: $[y, z^{-1}, x]^z \cdot [z, x^{-1}, y]^x \cdot [x, y^{-1}, z]^y = 1$.

(f) $[x,y]^g = [x^g, y^g]$.

Proof of (e): Let $u = yxz^y$, $v = zyx^z$, $w = xzy^x$. Then $[y, z^{-1}, x]^z = u^{-1}v$, etc.

Definition: If $X, Y, Z \leq G$, then $[X,Y] = \langle [x,y] : x,y \in G \rangle = [Y,X]$,
and $[X,Y,Z] = [[X,Y],Z] = [\langle [x,y] : x \in X, y \in Y \rangle, Z]$, $\left(\neq \langle [x,y,z], x \in X, y \in Y, z \in Z \rangle, \text{in general}\right)$

Lemma: (a) $X \leq G \Rightarrow [X,G] \trianglelefteq G$.
(b) $M, N \leq G \Rightarrow [MN, G] = [M,G][N,G]$.

Proof: Use commutator identities.

Lemma: $N \trianglelefteq G$, $X, Y, Z \leq G$. If $[x,y,z] \in N \ \forall x \in X, y \in Y, z \in Z$, then $[X,Y,Z] \leq N$.

3-subgroup lemma: $X, Y, Z \leq G$, $N \trianglelefteq G$. If $[Y,Z,X] \leq N$ and $[Z,X,Y] \leq N$, then $[X,Y,Z] \leq N$.

Proof: By previous lemma, sufficient to prove that $[x,y,z] \in N \ \forall x \in X, y \in Y, z \in Z$.
By Hall-Witt identity, with x, y^{-1}, z: $[x,y,z] = \left([z,x^{-1}y^{-1}]^{xy}\right)^{-1} \left([y^{-1}, z^{-1}, x]^{zy}\right)^{-1} \in N$.

Definition: G a pro-p group. Let $P_1(G) = G$, and $P_{i+1}(G) = \overline{P_i(G)^p [P_i(G), G]}$ - the **lower p-series of G**.

Remark: (i) Note $P_i(G)$ are topologically characteristic subgroups in G. (ie, continuous automorphisms leave subgroups fixed.)

(ii) Also known as the **Frattini Series**. Note $P_2(G) = \overline{G^p [G,G]} = \overline{\Phi(G)}$, $P_{i+1}(G) \geq \Phi(P_i(G))$.

(iii) $\{P_i(G)\}$ is the fastest descending series of closed normal subgroups such that each factor is central and has exponent dividing p.
If $G = G_1 \geq G_2 \geq \dots \geq G_i \geq G_{i+1} \geq \cdots$ is another such series, then $G_i \geq P_i(G)$.

Let's return to chapter 5!

Proposition 5.7: G a pro-p group.

(i) $P_i(G/K) = P_i(G)K/K \quad \forall\, K \trianglelefteq_c G$

(ii) $[P_i(G), P_j(G)] \leq P_{i+j}(G)$

(iii) G f.g. then $P_i(G)$ open and $\{P_i(G)\}$ define a basis of nbhds of the identity. (Ie, every open set containing 1 contains a $P_i(G)$.)

Proof: Here, let $G_i = P_i(G)$.

(i) $K \trianglelefteq_c G$. Note G_iK/K is a series of closed normal subgroups of G/K such that each factor is central and has exponent dividing $p \Rightarrow P_i(G/K) \leq G_iK/K$.
Suppose, for some n, $P_n(G/K) = G_nK/K$. Let $M/K = P_{n+1}(G/K)$.
M is closed and $M \geq G_n^p[G_n, G]K \Rightarrow M \geq G_{n+1}K \Rightarrow M = G_{n+1}K$, so true by induction.

(ii) By definition, $[G_i, G_1] \leq G_{i+1}\ \forall i$. Suppose inductively that $[G_i, G_{n-1}] \leq G_{i+n-1}\ \forall i$.
Fix m. Want to show $[G_m, G_n] \leq G_{m+n}$.
Since $[G_m, G_n]$ is closed, it is sufficient to prove $[G_m, G_n] \leq N\ \forall\, G_{m+n} \leq N \trianglelefteq_o G$.
By (i), consider the finite p-group G/N, and assume $G_{m+n} = 1$. By induction, $[G_m, G_{n-1}] \leq G_{m+n-1}$, so $[G_m, G_{n-1}]$ is central and has exponent dividing p.
If $g \in G_m$, $x \in G_{n-1}$, then $[g, x^p] = [g, x]^p = 1 \Rightarrow [G_m, G_{n-1}^p] = 1$.
(Note: $G_{n-1}^p = \langle g^p : g \in G_{n-1} \rangle$). By 3-subgroup lemma,
$[G_m, [G_{n-1}, G]] \leq [G, [G_m, G_{n-1}]].[G_{n-1}, [G, G_m]]$ — normal
$\leq [G, G_{m+n-1}].[G_{n-1}, G_{m-1}] \leq G_{m+n} = 1$.
$\Rightarrow [G_m, G_{n-1}^p[G_{n-1}, G]] = 1 \Rightarrow [G_m, G_n] = 1$, since G finite. (ie, G/N)

Remark: (1.3) said that every open set in G (a compact, totally disconnected topological group) is a union of cosets of open normal subgroups.
$\Rightarrow$ every open set containing 1 contains an open normal subgroup.
Ie, open normal subgroups form a base for the nbhds of 1.

Proof of 5.7(iii): Let $G_i = P_i(G)$. For $n \geq 1$, suppose G_n open and f.g. in G.
(5.6) $\Rightarrow \Phi(G_n)$ open in G_n. $\Phi(G_n) \leq G_{n+1} \leq G_n \Rightarrow G_{n+1}$ open in G_n, hence open in G.
(5.2) $\Rightarrow G_{n+1}$ f.g.
To show that $\{G_i : i \geq 1\}$ is a base of nbhds of 1, it suffices to show that each open normal subgroup of G contains a G_i. By (i), $N \trianglelefteq_o G$, G/N finite $\Rightarrow P_i(G/N) = 1$, for some i big enough. $\Rightarrow P_i(G) \leq N$. (Since $P_i(G)$ strictly descending for finite p-groups.)

Theorem 5.8: If G is a f.g. pro-p group, then every subgroup of finite index is open.

Remark: (a) For a f.g. pro-p group, topology is completely determined by the group structure
(b) N. Nikolai & D. Segal have recently announced that this also holds for f.g. profinite groups.

Lemma: G a pro-p group and K a subgroup of finite index, then $|G:K| = p^k$, some k.

Proposition: G a f.g. pro-p group, then $[G, G]$ is closed.

Proof of (5.8): Let $G^{\{p\}} = \{g^p : g \in G\}$, the image of the continuous map $g \mapsto g^p$, so is compact and closed. $G/[G,G]$ is abelian, and so $G^p[G,G] = G^{\{p\}}[G,G]$.
So, the proposition $\Rightarrow$ $G^p[G,G]$ closed, and $= \Phi(G)$, open, by (5.6).
Let K be a proper normal subgroup of G of finite index. Argue by induction on $|G:K|$.
So assume K open in M whenever M is a f.g. pro-p group, $K \leq M < G$.
Let $M = G^p[G,G]K \geq K$ (note - M closed, finite index, so a f.g. pro-p group).
By the lemma, G/K is a finite p-group $\Rightarrow M \neq G$, and M is open.
So, by inductive hypothesis, K is open in M, and so K is open in G. Since any open subgroup contains an open normal subgroup, we've done.

Corollary 5.9: G a f.g. pro-p group. Then $\Phi(G) = G^p[G,G]$ and $P_{i+1}(G) = P_i(G)^p[P_i(G), G]$.
(ie, "we can remove bars")

Proof: The proof of (5.8) shows us that $\Phi(G) = G^p[G,G]$. Let $G_i = P_i(G)$.
(5.8) $\Rightarrow$ G_i open (i.e. closed), so a pro-p group of finite index $\Rightarrow$ f.g.
(5.7) $\Rightarrow$ $\Phi(G_i)$ open in G_i. So, $\Phi(G_i) = G_i^p[G_i, G_i] \leq G_i^p[G_i, G]$.
$\Rightarrow G_i^p[G_i, G]$ is open in G_i, so open in G. Therefore, closed as required.

Corollary (5.10): (i) Every (abstract) homomorphism from a f.g. pro-p group to a profinite group is continuous.
(ii) The topology of a f.g. pro-p group is determined by its group structure.

Proof: (i) $\theta : \underset{(\text{f.g. pro-}p)}{G} \to \underset{(\text{profinite})}{H}$. If $K \trianglelefteq_o H$, $\theta^{-1}(K) = \{g \in G : \theta(g) \in K\} \leq G$. Also $|G : \theta^{-1}(K)| \leq |H : K|$.
ie, $\theta^{-1}(K)$ is of finite index in G, so $\theta^{-1}(K)$ is open in G, by (5.8). $\Rightarrow \theta$ continuous.
(ii) Let $\theta : G \to G$ be the identity map, where G could possibly have a different topology.
(i) $\Rightarrow \theta$ continuous bijection $\Rightarrow \theta$ a homeomorphism, since G compact & Hausdorff.

6. Procyclic Groups

Definition: (a) (g_i) converges to g in profinite G if, given a nbhd U of g, $\exists\, k$ s.t. $g_i \in U \ \forall\, i \geq k$.
(b) (g_i) is a Cauchy sequence in profinite G if, for each $N \trianglelefteq_o G$, $\exists\, n = n(N)$ s.t. $g_i^{-1} g_j \in N \ \forall\, i, j \geq n$.

Lemma 6.1: A sequence (g_i) converges in profinite G iff it is Cauchy.
Proof: Exercise.

Lemma 6.2: G a pro-p group, $g \in G$, and $(a_i), (b_i)$ convergent sequences in $\mathbb{Z}_p$ with the same limit. Then the sequences $(g^{a_i}), (g^{b_i})$ both converge in G and their limits are equal.

Proof: Let $N \trianglelefteq_o G$. So $|G/N| = p^j$, some j. Then $a_i \equiv a_k \bmod p^j \ \forall\, i,k$ sufficiently large.
$\Rightarrow g^{a_i} \equiv g^{a_k} \bmod N \Rightarrow (g^{a_i})$ a Cauchy sequence in G, so converges to some limit, $g_1 \in G$.
Similarly (g^{b_i}) converges to some limit $g_2 \in G$. As $(a_i), (b_i)$ converge to the same limit, we have $a_k \equiv b_k \bmod p^j \ \forall$ sufficiently large k, and $g^{a_k} \equiv g_1 \bmod N$, $g^{b_k} \equiv g_2 \bmod N$.
$\Rightarrow g_1 g_2^{-1} \equiv g^{a_k - b_k} \equiv 1 \bmod N$. N arbitrary $\Rightarrow g_1 = g_2$. Thus we can define "p-adic exponentiation".

Definition: G a pro-p group, $g \in G$, $\lambda \in \mathbb{Z}_p$. Then $g^\lambda = \lim g^{a_i}$, where $\{a_i\}$ is a sequence of integers and $\lim a_i = \lambda$.

Proposition 6.3: G a pro-p group, $g, h \in G$, $\lambda, \mu \in \mathbb{Z}_p$.

(i) $g^{\lambda+\mu} = g^\lambda g^\mu$ and $(g^\lambda)^\mu = g^{\lambda\mu}$.

(ii) $gh = hg \Rightarrow (gh)^\lambda = g^\lambda h^\lambda$.

(iii) $\theta : \mathbb{Z}_p \to G$, $\nu \mapsto g^\nu$, fixed $g \in G$, then $\operatorname{Im}\theta = g^{\mathbb{Z}_p} = \overline{\langle g \rangle}$.

Proof: $N \trianglelefteq_o G$, $|G/N| = p^j$, some j. So (i), (ii) hold modulo N, $\forall N \trianglelefteq_o G \Rightarrow$ hold in G.

(iii) By (i), θ is a group homomorphism and continuous (by 5.10). $\Rightarrow g^{\mathbb{Z}_p}$ compact, so closed. Clearly $g^{\mathbb{Z}_p} \geq \langle g \rangle \Rightarrow g^{\mathbb{Z}_p} \geq \overline{\langle g \rangle}$. Also, $g^{\mathbb{Z}_p} \leq \overline{\langle g \rangle}$ since each element of $g^{\mathbb{Z}_p}$ is a limit of elements in $\langle g \rangle$.

Proposition 6.4: G a pro-p group. The following are equivalent.

(a) G is procyclic.

(b) G can be topologically generated by 1 element

(c) $G = g^{\mathbb{Z}_p}$ for some $g \in G$

(d) G is either cyclic and finite or isomorphic to $\mathbb{Z}_p$.

Proof: (a) $\Rightarrow$ (b): Assume G has two maximal proper open subgroups, M, N. Then by definition $MN \supseteq \Phi(G) \supseteq [G,G]G^p$. So G/M abelian and exponent p.
M maximal $\Rightarrow M \trianglelefteq G$, $|G:M| = p$. (N similarly.) $\Rightarrow G/M \cap N$ abelian, exponent p, order p^2. Therefore it is not cyclic. So either $G = 1$ or G has a unique maximal proper open subgroup $\Rightarrow \Phi(G)$ open and $G/\Phi(G)$ cyclic. $\Rightarrow$ (b), by (5.3).

(b) $\Rightarrow$ (c) Proposition 6.3 (iii)

(c) $\Rightarrow$ (d) Suppose $G = g^{\mathbb{Z}_p}$. Let $\theta : \mathbb{Z}_p \to G$, $\nu \mapsto g^\nu$. θ is surjective and continuous (5.10), and if $K = \ker\theta$, $\mathbb{Z}_p/K \cong G$ (and quotients of $\mathbb{Z}_p$ are finite and cyclic, or just $\mathbb{Z}_p$).

(d) $\Rightarrow$ (a) Similar.

7. Powerful p-groups

G a finite p-group.

Definition: (i) G is powerful if $[G,G] \leq G^p$ (p odd), or $\leq G^4$ ($p = 2$)

(ii) $N \trianglelefteq G$. N is powerfully embedded in G (N p.e. G) if $[N,G] \leq N^p$ (p odd), $\leq N^4$ ($p = 2$)

These definitions are due to A. Mann (1980s), with results due to Mann & Lubotzky.

Remarks: (i) $[G,G] \leq G^2$ always (all elements have order 2 $\Rightarrow$ abelian), hence a different definition for $p = 2$.

(ii) powerful = "full of powers".

(iii) powerful $\Rightarrow G/G^p$ is abelian.

(iv) $p \neq 2$, powerful $\Rightarrow \Phi(G) = G^p$.

Lemma 7.1: (i) G is powerful iff G p.e. G.
(ii) N p.e. G then $N \trianglelefteq G$ and N powerful.
(iii) $K \trianglelefteq G$, N p.e. G, then NK/K p.e. G/K (ie, quotients of powerful groups are powerful)
(iv) N p.e. G, $x \in G$, let $H = \langle x \rangle N$. Then H is powerful.
(v) $N = \langle x \rangle^G$, N p.e. G, then $N = \langle x \rangle$.

Proof: (iv) Note that $[N,H] = [H,H]$
(v) $x^g = x[x,g]$ and $[x,g] \in \Phi(N)$, $x \in X$, $g \in G$.

Lemma 7.2: $p \neq 2$. Suppose $|G/\Phi(G)| = p^d$. If $\exists\, a_1, \dots, a_d \in G$ s.t. $G = \langle a_1 \rangle \cdots \langle a_d \rangle$, then G powerful.
Proof: $g \in G$, $g = a_1^{n_1} \cdots a_d^{n_d} \bmod G^p$, $0 \leq n_i < p$. Also, $\Phi(G) = [G,G]\,G^p$. Hence $p^d \geq |G/G^p| \geq |G/\Phi(G)| \geq p^d$.

Lemma 7.3: $N \leq G$. Then: $p \neq 2$, N p.e. G iff $N/[N,G,G]$ p.e. $G/[N,G,G]$.
$p = 2$, N p.e. G iff $N/[N,G,G][N,G]^2$ p.e. $G/[N,G,G][N,G]^2$.

Proof: ($\Rightarrow$) is 7.1 (iii)
($\Leftarrow$) p odd. Suppose $N/[N,G,G]$ p.e. $G/[N,G,G]$ but N not p.e. G. Ie, $[N,G] \leq N^p[N,G,G]$, but $[N,G] \not\leq N^p$. Then $N/[N,G,G] \trianglelefteq G/[N,G,G] \Rightarrow N \trianglelefteq G$ ($[N,G] \geq [N,G,G]$).
Now, $[N,G] \cap N^p \subsetneq [N,G]$. (In a finite p-group G, if $M \leq N$, $M, N \trianglelefteq G$, $|N/M| = p^r$, then for each $0 \leq k \leq r$ $\exists\, M_k \trianglelefteq G$ with $M \leq M_k \leq N$ and $|M_k/M| = p^k$)
$\Rightarrow \exists\, K \trianglelefteq G$ s.t. $[N,G] \cap N^p \leq K < [N,G]$ and $[N,G]/K = p$. So $[N,G]/K \leq G/K$ and of order p.
$\Rightarrow [N,G]/K$ is central in G/K (since a union of conjugacy classes). $\Rightarrow [N,G,G] \leq K$.
Hence $K \geq ([N,G] \cap N^p)[N,G,G] = [N,G] \cap N^p[N,G,G]$.
$\Rightarrow [N,G] \geq K \geq [N,G] \cap N^p[N,G,G] = [N,G]$ ⚡.
($p = 2$ is similar - replace N^p with N^4.)

Remark: To prove N p.e. G we can work modulo $[N,G,G]$. Ie, assume $[N,G,G] = 1$ (p odd)

Proposition 7.4: N p.e. $G \Rightarrow [N,G]$ p.e. G.
Proof: p odd. By (7.3), we can assume $[N,G,G,G] = 1$. If $n \in N$, $x \in G$, then by ex. 1.2 (handout), $[x,n^p] = [x,n]^p[x,n,n]^{\binom{p}{2}} \in [N,G]^p$. So $[N,G]^p \geq [N^p,G] \geq [N,G,G]$ since N p.e. G.
(ex. 1.10 (handout): $M, N \trianglelefteq G \Rightarrow [M^n, N] = [M^{[n]}, N]$.)

Corollary 7.5: G a powerful p-group.
(i) $\gamma_i(G)$ p.e. G $\forall i$
(ii) If $H \leq G$, $\gamma_{i+1}(G) \leq H \leq \gamma_i(G)$ for some $i \geq 2$ $\Rightarrow H$ powerful.
Proof: (i) Induction & (7.4)
(ii) Let $p' = p$ (p odd), $= 4$ ($p = 2$). Then $H^{p'} \geq (\gamma_{i+1}(G))^{p'} \geq [\gamma_{i+1}(G), G]$ by (i).
Now, $\gamma_{i+2}(G) \geq [\gamma_i(G), \gamma_i(G)]$ since $i \geq 2$. ($[\gamma_i, \gamma_j] \leq \gamma_{i+j}$).
So, $H^{p'} \geq [\gamma_{i+1}(G), G] = \gamma_{i+2}(G) \geq [H,H]$.

Corollary 7.6: M, N p.e. G, then MN and $[M,N]$ p.e. G.
Proof: p odd. $(MN)^p \geq M^p N^p \geq [M,G][N,G] = [MN,G]$. Ie, MN p.e. G. For $[M,N]$, assume $[M,N,G,G] = 1$.
If $m \in M$, $n \in N$, by ex. 1.2, $[m,n^p] = [m,n]^p[m,n,n]^{\binom{p}{2}} \in [M,N]^p$, $[m^p,n] = ([n,m]^p[n,m,m]^{\binom{p}{2}})^{-1} \in [M,N]^p$.
Ex 1.10 $\Rightarrow [M,N]^p \geq [M^p,N][M,N^p] \geq [M,G,N][M,[N,G]] \geq [M,N,G]$, by the 3-subgroup lemma.
($[G,M,N] = [N,G,M]$)

Proposition 7.7: N p.e. $G \Rightarrow N^p$ p.e. G

Proof: p odd. By (7.3), assume $[N^p, G, G] = 1 \Rightarrow [N, G, G, G] = 1$. As in (7.6), $\Rightarrow [N, G]^p \geq [N^p, G]$.
So $(N^p)^p \geq [N, G]^p \geq [N^p, G]$.

Corollary 7.8: G a powerful p-group. Then G^p and $\Phi(G)$ p.e. G.

Proof: Use 7.5, 7.7, 7.6.

Aside: "regular"

Definition: A finite p-group G is regular if $\forall x, y \in G$ and any $\alpha \in \mathbb{Z}$, $\exists\, i \geq 0$ s.t. $s_1, \ldots, s_i \in \gamma_2(G)$ s.t. $(xy)^{p^\alpha} = x^{p^\alpha} y^{p^\alpha} s_1^{p^\alpha} \ldots s_i^{p^\alpha}$?

Remark: (i) Definition due to P. Hall (1933) and is a 'generalisation' of abelian.
(ii) It is equivalent to: $\forall x, y \in G$, $\exists\, s \in \gamma_2(\langle x, y \rangle)$ s.t. $(xy)^p = x^p y^p s^p$.

Results: (a) If G is a p-group and has nilpotency class $< p$, then G regular.
(b) If G is regular and $x_1, \ldots, x_r \in G$ then $o(x_1 \ldots x_r) = \max\{o(x_1), \ldots, o(x_r)\}$.

Theorem 7.9: G a powerful p-group. Then $(G^{p^\alpha})^p = G^{p^{\alpha+1}}$ and G^{p^α} p.e. G $\forall\, \alpha \geq 0$.

Proof: Clearly $G^{p^{\alpha+1}} \leq (G^{p^\alpha})^p$. p odd. Use induction on $|G|$. If $|G| = p$ or $G^{p^\alpha} = \langle 1 \rangle$, done.
Assume $|G| > p$ and that the result holds $\forall \alpha$, for smaller powerful p-groups, and so for proper quotients of G. If $G^{p^\alpha} > \langle 1 \rangle$, by (2.1.3)(ii) (handout), $\exists\, N \trianglelefteq G$ s.t. $G^{p^{\alpha+1}} < N \leq G^{p^\alpha}$, and $N/G^{p^{\alpha+1}}$ of order p and central in $G/G^{p^{\alpha+1}}$. Hence $[N, G] \leq G^{p^{\alpha+1}}$.
Induction $\Rightarrow ((G/N)^{p^\alpha})^p = (G/N)^{p^{\alpha+1}} = \langle 1 \rangle$, $\Rightarrow (G^{p^\alpha})^p \leq N$. Also, induction $\Rightarrow (G/N)^{p^\alpha}$ p.e. G/N.
So, $\langle 1 \rangle = ((G/N)^{p^\alpha})^p \geq [(G/N)^{p^\alpha}, G/N] \Rightarrow [G^{p^\alpha}, G] \leq N \Rightarrow [G^{p^\alpha}, G, G] \leq [N, G] \leq G^{p^{\alpha+1}}$.
So, nilpotency class of $G^{p^\alpha}/G^{p^{\alpha+1}} \leq 2$ and p odd $\Rightarrow G^{p^\alpha}/G^{p^{\alpha+1}}$ is regular.
But $G^{p^\alpha}/G^{p^{\alpha+1}}$ is generated by elements of order p and is regular, so has exponent p.
Hence $(G^{p^\alpha})^p \leq G^{p^{\alpha+1}}$. Thus they are equal. (For p.e., use induction and 7.7.)

Corollary 7.10: G a powerful p-group
(i) $(G^{p^\alpha})^{p^\beta} = G^{p^{\alpha+\beta}}$ $\forall\, \alpha, \beta \geq 0$.
(ii) $G^{p^{\alpha+1}} \geq [G^{p^\alpha}, G]$ and hence $G^{p^\alpha} \geq \gamma_{\alpha+1}(G)$ $\forall\, \alpha \geq 0$. For 2-groups, $G^{2^{\alpha+1}} \geq [G^{2^\alpha}, G]$.
(iii) $G^{p^{\alpha+1}} = \Phi(G^{p^\alpha})$ $\forall\, \alpha \geq 0$.

Proof: exercise.

Remark: We can define lower p-series for finite p-group G: $P_1(G) = G$, $P_{i+1}(G) = P_i(G)^p [P_i(G), G]$.
For a powerful p-group, $P_i(G) = G^{p^{i-1}}$.

Lemma 7.11: G a powerful p-group. Then $\theta : G/G^p \to G^p/G^{p^2}$, $xG^p \mapsto x^p G^{p^2}$ is a surjective homomorphism.

Proof: p odd. By (7.10)(iii), $\gamma_3(G) \leq G^{p^2}$, and $(\gamma_2(G))^p \leq (G^p)^p = G^{p^2}$. Hence $(xy)^p \equiv x^p y^p \bmod G^{p^2}$, $\forall\, x, y \in G$. Also, if $y \in G^p$, $y^p \in (G^p)^p = G^{p^2}$. So θ is a well-defined, surjective homomorphism.

Remark: $\theta : G^{p^i}/G^{p^{i+1}} \to G^{p^{i+1}}/G^{p^{i+2}}$, $xG^{p^{i+1}} \mapsto x^p G^{p^{i+2}}$ is a surjective homomorphism.
This follows from (7.11) replacing G with G^{p^i}.

Theorem 7.12: G a powerful p-group. Then $G^{p^\alpha} = G^{\{p^\alpha\}}$ $\forall\ \alpha \geq 1$.

Proof: Let $\alpha = 1$, use induction on $|G|$. Let $x \in G^p$. By (7.11), $x = y^p z$, some $y \in G$, $z \in G^{p^2}$.
Let $H = \langle y \rangle G^p$. Since G^p p.e. G (7.7), $\Rightarrow$ H powerful ((7.1)(iv)).
Also $x \in H^p$, since $z \in G^{p^2} = (G^p)^p \leq H^p$. If $H \lneq G$, use induction hypothesis: $x \in H^{\{p^i\}} \leq G^{\{p^i\}}$.
Or if $H = G$, then $G = \langle y \rangle \Phi(G) \Rightarrow G = \langle y \rangle$. So true. Then use induction on α.

Now we concentrate on generators of subgroups.

Theorem 7.13: Let $G = \langle a_1, \dots, a_d \rangle$ be a powerful p-group, then $G^{p^\alpha} = \langle a_1^{p^\alpha}, \dots, a_d^{p^\alpha} \rangle$.

Proof: Use induction on α. By (7.11), $\theta : G/G^p \to G^p/G^{p^2}$ is a surjective homomorphism.
So $G^p = \langle a_1^p, \dots, a_d^p \rangle G^{p^2} = \langle a_1^p, \dots, a_d^p \rangle \Phi(G^p)$, by (7.10)(iii). So, $G^p = \langle a_1^p, \dots, a_d^p \rangle$.
Assume result holds for $\alpha - 1$, let $H = G^{p^{\alpha-1}}$ -powerful. Then $H = \langle a_1^{p^{\alpha-1}}, \dots, a_d^{p^{\alpha-1}} \rangle$
$\Rightarrow$ $G^{p^\alpha} = H^p = \langle a_1^{p^\alpha}, \dots, a_d^{p^\alpha} \rangle$.

Corollary 7.14: $G = \langle a_1, \dots, a_d \rangle$, powerful p-group. Then $G = \langle a_1 \rangle \dots \langle a_d \rangle$. (ie, every element of G can be expressed in the form $a_1^{n_1} \dots a_d^{n_d}$, $n_i \in \mathbb{Z}$.)

Proof: Let $\alpha \in \mathbb{Z}$ be s.t. $G^{p^\alpha} > G^{p^{\alpha+1}} = \langle 1 \rangle$ - use induction on α. If $\alpha = 0$, G elementary abelian.
Assume $\alpha > 0$ and that the result holds for smaller α. By induction hypothesis,
$G = \langle a_1 \rangle \dots \langle a_d \rangle G^{p^\alpha}$. By (7.13), $G^{p^\alpha} = \langle a_1^{p^\alpha}, \dots, a_d^{p^\alpha} \rangle$ and $[G^{p^\alpha}, G] \leq G^{p^{\alpha+1}} = \langle 1 \rangle$.
Hence, G^{p^α} central and each element of G can be expressed as an element of $\langle a_1 \rangle \dots \langle a_d \rangle$.

Remark: • S_n, symmetric group of degree n, $d(S_n) = 2$. But $H = \langle (1,2), (3,4), (5,6) \rangle \leq S_n$, but $d(H) = 3$.
• $J = \langle f : tf = t(t^2) \rangle$ - Nottingham group, $J_n = \langle f : tf = t(t^{n+1}) \rangle \lhd J$: $d(J) = 2$, $d(J_n) = n+1$

Theorem 7.15: G a powerful p-group, $H \leq G$, then $d(H) \leq d(G)$.

Proof: (7.10)(iii) $\Rightarrow$ $G^p = \Phi(G)$, $G^{p^2} = \Phi(G^p)$. Let $K = H \cap G^p$, then $K \cap G^{p^2} = K \cap \Phi(G) \geq \Phi(K)$.
Let $d = d(G)$, $m = d(G^p)$, $k = d(K)$. Use induction on $|G|$. If $|G| = p$, nothing to prove.
So assume $|G| > p$ and that the result holds for smaller groups. By (7.8), G^p p.e. G, so G^p powerful and $|G^p| < |G|$. Hence by induction hypothesis, $k \leq m$.
Now, HG^p/G^p is a subspace of G/G^p. Let $h_1 G^p, \dots, h_e G^p$ be a basis, $e \leq d$.
Let $L = \langle h_1^p, \dots, h_e^p \rangle \leq K$. In vector space $K/\Phi(K)$, $L\Phi(K)/\Phi(K)$ is a subspace, dimension $r \leq e$.
Hence, there is a basis for $K/\Phi(K)$ consisting of r of $h_1^p \Phi(K), \dots, h_e^p \Phi(K)$ together with $y_{r+1}\Phi(K), \dots, y_k \Phi(K)$, some $y_{r+1}, \dots, y_k \in K$.
$K = H \cap G^p \Rightarrow H = \langle h_1, \dots, h_e, y_{r+1}, \dots, y_k \rangle \Rightarrow d(H) \leq e + k - r$.
From (7.11), $\theta : G/G^p \to G^p/G^{p^2}$, a surjective homomorphism, defines a linear map between the two vector spaces $\Rightarrow \dim(\ker\theta) = \dim(G/G^p) - \dim(G^p/G^{p^2}) = d - m$. Take restriction of θ to $HG^p/G^p \Rightarrow \dim(\theta(HG^p/G^p)) \geq e - (d-m) = m + e - d$.
Also, $\theta(HG^p/G^p) = LG^{p^2}/G^{p^2} \cong L/L \cap G^{p^2}$, a quotient of $L/L \cap \Phi(K) \cong L\Phi(K)/\Phi(K)$.
$\Rightarrow$ $r \geq m + e - d \geq k + e - d$. $\Rightarrow$ $d(H) \leq e + k - r \leq d$.

The next results are concerned with finding powerful subgroups of finite p-groups.

Definition: For a finite p-group G, let $V(G,r)$ denote the intersection of all kernels of homomorphisms from G to $GL_r(\mathbb{F}_p)$.

Lemma 7.16: (i) $N \trianglelefteq G$ then $V(G,r)/N \leq V(G/N, r)$

(ii) $V(G,r)$ is a characteristic subgroup of G.

(iii) $V(G,r)$ is the intersection of the kernels of all homomorphisms from G to U, where U is the Sylow p-subgroup of $GL_r(\mathbb{F}_p)$ consisting of all lower unitriangular matrices.

(iv) $M, N \trianglelefteq G$ and $\Phi(N) \leq M \leq N$ and $d(N) \leq r$, then $[N, V(G,r)] \leq M$

Proof: (i) $\pi: G \to G/N$, $\vartheta: G/N \to GL_r(\mathbb{F}_p)$. Then $\vartheta\pi: G \to GL_r(\mathbb{F}_p) \Rightarrow V(G,r) \leq \ker \vartheta\pi$
$\Rightarrow V(G,r)N/N = \pi V(G,r) \leq \ker \vartheta$.

(ii) $\alpha \in \mathrm{Aut}(G)$, $\vartheta: G \to GL_r(\mathbb{F}_p)$. Then $\vartheta\alpha: G \to GL_r(\mathbb{F}_p)$.

(iii) $\vartheta: G \to GL_r(\mathbb{F}_p)$. ϑG is a finite p-group of $GL_r(\mathbb{F}_p) \Rightarrow (\vartheta G)^g \leq U$, some $g \in GL_r(\mathbb{F}_p)$.
$\ker\vartheta$ is also the kernel of the composition of ϑ followed by conjugation by g which maps G to U.

(iv) N/M is elementary abelian, so regard it as a vector space over $\mathbb{F}_p$, $\dim = s \leq r$.
Let $v_1, \dots, v_s$ be a basis. Given $x \in G$, define $\alpha_x: N/M \to N/M$, $Mn \mapsto Mn^x$.
Let A_x be the matrix of α_x wrt $v_1, \dots, v_s$. Define $\vartheta: G \to GL_s(\mathbb{F}_p) \hookrightarrow GL_r(\mathbb{F}_p)$ by $x \mapsto A_x$. Then ϑ is a homomorphism, so $V(G,r) \leq \ker\vartheta$.
Now, $x \in \ker\vartheta$ iff $M_n = M_{n^x}$ $\forall n \in N$, and so $[n,x] \in M$ $\forall n \in N$.

Theorem 7.17: G a finite p-group, $r \in \mathbb{Z}^+$, $N \trianglelefteq G$, $d(N) \leq r$.

(i) $p \neq 2$. If $N \leq V(G,r)$, then N p.e. $V(G,r)$

(ii) $p = 2$. If $N \leq V(G,r)^2$, then N p.e. $V(G,r)^2$.

Corollary 7.18: (i) $p \neq 2$. If $d(V(G,r)) \leq r \Rightarrow V(G,r)$ powerful.

(ii) $p = 2$. If $d(V(G,r)^2) \leq r \Rightarrow V(G,r)^2$ powerful.

Proof of 7.17: Let $V = V(G,r)$ and use induction on $|N|$. ($|N| = 1$ is fine.)
Assume result holds for smaller orders and $N \leq V$, N not p.e. V. So, $[N,V] \not\leq [N,V,V]N^p$.
$\exists$ $L, M \trianglelefteq G$ s.t. $[N,V,V]N^p \leq L \leq [N,V]N^p \leq M \leq N$, with $|N:M| = p$, $|[N,V]N^p : L| = p$.
$N/[N,V]N^p$ is elementary abelian, so a vector space over $\mathbb{F}_p$ of dimension $\leq r$.
$M/[N,N]N^p$ is a proper subspace, so dimension $< r$. Also, $|[N,V]N^p/L| = p \Rightarrow d(M/L) \leq r$.
But $|M/L| < |N|$ and $M/L \leq V/L \leq V(G/L, r)$ by (7.16)(i). Hence by induction, M/L p.e. V/L.
$\Rightarrow [M,V] \leq M^pL = L$. So M/L central in V/L and so in N/L, and M/N is cyclic.
$\Rightarrow N/L$ abelian $\Rightarrow [N,N] \leq L$.
Now, $\Phi(N) = [N,N]N^p \leq L \leq N$, and $d(N) \leq r$. So (7.16)(iv) $\Rightarrow [N,V] \leq L \Rightarrow [N,V]N^p \leq L$ #

Theorem 7.19: G a finite p-group, $r = \max\{d(N) : N \trianglelefteq G\}$. Then G has a powerful characteristic subgroup of index $\leq p^{r\lambda(r)}$, for $p \neq 2$, $(\leq 2^{r+\lambda(r)}$, for $p=2)$, where $\lambda(r)$ is the smallest integer s.t. $\lambda(r) \geq 1$, $r \leq 2^{\lambda(r)}$.

Proof: p odd. $V = V(G,r)$ is a powerful, characteristic subgroup of G, by (7.18), (7.16) (iii).
Let $\theta_1, \ldots, \theta_k$ be all distinct homomorphisms from $G \to U$ (unitriangular matrices in $GL_r(\mathbb{F}_p)$.).
Then, by (7.16), $V = \bigcap_{i=1}^{k} \ker\theta_i$. Define $\theta: G \to \underbrace{U \times \cdots \times U}_{k}$, $x \mapsto (\theta_1 x, \ldots, \theta_k x)$.
Then $x \in \ker\theta$ iff $x \in V$. Hence $G/V \cong \theta G \leq$ subgroup of $U \times \cdots \times U$.
Let $U_m \leq U$, $U_m = (a_{ij})$, $a_{ij} = 0$, $j+1 \leq i \leq j+m$. Ie: $\{m\text{-}1\text{'s}\} = U_m \trianglelefteq U$. $(U_1 = U)$.
$U = U_1 > U_2 > U_4 \cdots > U_{2^{\lambda(r)}} = \langle 1 \rangle$ and U_i/U_{i+1} elementary abelian (see handout).
$\Rightarrow \exists$ series of normal subgroups $G = G_1 > G_2 > \cdots > G_s = V$, G_i/G_{i+1} elementary abelian, $s \leq 2^{\lambda(r)}$.
Also, $G_{i+1} \geq \Phi(G_i)$ and $d(G_i) \leq r$. $\Rightarrow |G_i/G_{i+1}| = p^r \Rightarrow |G:V| \leq p^{r\lambda(r)}$

8 Pro-p groups of finite rank

Definition: G a pro-p group.
(i) G is powerful if $[G,G] \leq \overline{G^p}$ for p odd, $[G,G] \leq \overline{G^4}$ for $p=2$.
(iii) $N \leq_o G$, N powerfully embedded (p.e.) in G if $[N,G] \leq \overline{N^p}$ for p odd, $[N,G] \leq \overline{N^4}$ for $p=2$.

Remark: N p.e. $G \Rightarrow N \trianglelefteq_o G$ and N powerful.

Proposition 8.1: G a pro-p group, $N \leq_o G$. Then N p.e. G iff N^K/K p.e. G/K $\forall$ $K \trianglelefteq_o G$.

Proof: $(\Rightarrow)$ ✓
$(\Leftarrow)$ $[N,G] \leq N^p K$ $\forall$ $K \trianglelefteq_o G$, but $\bigcap_{K \trianglelefteq_o G} N^p K = \overline{N^p}$.

Corollary 8.2: A topological group G is a powerful pro-p group iff G is the inverse limit of an inverse system of powerful finite p-groups in which all maps are surjective.

Proof: $(\Rightarrow)$ $G \cong \varprojlim_{N \trianglelefteq_o G} G/N$ and G/N powerful.
$(\Leftarrow)$ Suppose $G \cong \varprojlim G_\lambda$, G_λ powerful finite p-groups and $G_\mu \to G_\lambda$ surjective, $\mu \geq \lambda$.
Then G is a pro-p group and if $K \trianglelefteq_o G$, by (3.1) G/K is a quotient of some G_λ, so powerful $\Rightarrow$ G powerful by (8.1)

So we can translate results of the previous chapter to f.g. pro-p groups - need the lower p-series to consist of open subgroups.

Lemma 8.3: G a powerful, f.g., pro-p group. Then $G^p = G^{\{p\}}$ and $G^p = \Phi(G)$ is open in G.
If $p=2$, G^4 is open in G.

Proof: Let $g \in \overline{G^p}$. Then $gN \in (G/N)^p$ for each $N \trianglelefteq_o G$. (7.12) $\Rightarrow gN$ is a pth power in G/N, each N.
$\Rightarrow g$ is a pth power in G (exercise). So, $\overline{G^p} \leq G^{\{p\}}$, ie $\overline{G^p} = G^{\{p\}}$.
Since $[G,G] \leq \overline{G^p}$ $\Rightarrow G^p = \Phi(G) = P_2(G)$, open, by (5.7).
For $p=2$, $G^4 = \overline{G^4} \geq P_3(G)$, open.

Corollary 8.4: G a powerful, f.g. pro-p group. Then $G^{p^i} = (G^{p^{i-1}})^p = G^{\{p^i\}}$ p.e. $G^{p^{i-1}}$.

Proof: $\overline{G^p}$ p.e. G, (8.1) & (7.7), use induction.

Theorem 8.5: Let $G = \overline{\langle a_1, \dots, a_d \rangle}$, f.g., powerful pro-$p$ group, let $G_i = P_i(G)$.

(i) G_i p.e. G

(ii) $G_{i+k} = P_{k+1}(G_i) = G_i^{p^k}$, $k \geq 0$, so $G_{in} = \Phi(G_i)$.

(iii) $G_i = G^{p^{i-1}} = G^{\{p^{i-1}\}} = \overline{\langle a_1^{p^{i-1}}, \dots, a_d^{p^{i-1}} \rangle}$.

(iv) $G_i/G_{i+1} \to G_{i+k}/G_{i+k+1}$, $xG_{i+1} \mapsto x^{p^k} G_{i+k+1}$ is a surjective homomorphism $\forall\, i,k$.

Proof: Apply results about finite p-groups to $G/\overline{G^{p^n}}$ – since $\overline{G^{p^n}}$ open and form a base of nbhds of 1, and (8.4) (iii)

Proposition 8.6: If $G = \overline{\langle a_1, \dots, a_d \rangle}$ is a powerful pro-p group then $G = \overline{\langle a_1 \rangle} \cdots \overline{\langle a_d \rangle}$, a product of procyclic subgroups.

Proof: Let $A = \overline{\langle a_1 \rangle} \cdots \overline{\langle a_d \rangle}$, $\overline{\langle a_i \rangle}$ closed, so compact $\Rightarrow$ A closed. So $A = \bigcap_{N \trianglelefteq_o G} AN$.
(7.14) $\Rightarrow$ $AN/N = G/N$ $\forall\, N \trianglelefteq_o G$, (5.1) $\Rightarrow$ $A = G$.

Theorem 8.7: G a powerful, f.g., pro-p group, H a closed subgroup. Then $d(H) \leq d(G)$.

Proof: Use (5.1) & (7.15)

Definition: G a f.g. pro-p group. Let $V(G,r)$ denote the intersections of all homomorphisms from G to $GL_r(\mathbb{F}_p)$.

Remark: G f.g., $GL_r(\mathbb{F}_p)$ finite $\Rightarrow$ homomorphisms continuous (5.10). So if $G = \overline{\langle g_1, \dots, g_d \rangle}$ then $\theta(G)$ is determined by $\theta(g_1), \dots, \theta(g_d)$, by (5.1) $\Rightarrow$ finitely many θ.
Clearly $\ker \theta \trianglelefteq_o G \Rightarrow V(G,r)$ open and characteristic.
For $p=2$, $V(G,r)^2$ is open, since: $V(G,r)$ open $\overset{(5.2)}{\Rightarrow}$ $V(G,r)$ f.g $\overset{(5.6)}{\Rightarrow}$ $\Phi(V)$ open $\overset{(5.9)}{\Rightarrow}$ V^2 open.

Proposition 8.8: G a f.g. pro-p group, $r \in \mathbb{Z}^+$, $V = V(G,r)$. Let $N \trianglelefteq_o G$, $d(N) \leq r$.
$p \neq 2$: $N \leq V \Rightarrow N$ p.e. V, $p=2$: $N \leq V^2 \Rightarrow N$ p.e. V^2.

Proof: (7.17) & (8.1)

Theorem 8.9: G a f.g. pro-p group. Suppose $r = \sup_{N \trianglelefteq_o G} d(N)$ is finite. Then G has a powerful open subgroup of index $\leq p^{r\lambda(r)}$, p odd. ($\leq 2^{r+\lambda(r)}$, $p=2$).

Proof: As in finite case.

Recall, if G is finite, then the rank is $rk(G) = \sup\{d(H) : H \leq G\}$. So what is the definition of rank for profinite G?

Proposition 8.10: G a profinite group,
$r_1 = \sup\{d(H) : H \leq_c G\}$
$r_2 = \sup\{d(H) : H \leq_c G, d(H) < \infty\}$.
$r_3 = \sup\{d(H) : H \leq_o G\}$
$r_4 = \sup\{rk(G/N) : N \trianglelefteq_o G\}$.

Then $r_1 = r_2 = r_3 = r_4$.

Proof: Clearly, $r_2 \leq r_1$, $r_3 \leq r_1$ (H open $\Rightarrow$ H closed, by (1.1)(c).)
$r_4 \leq r_3$: If $N \trianglelefteq_o G$ and $M/N \leq G/N$, then $d(M/N) \leq d(M) \leq r_3$, $\forall (M \leq_o G)$.
$r_4 \leq r_2$: Again, $N \trianglelefteq_o G$, $M/N \leq G/N$, then $M = NX$, where X finite subsets of G.
Let $H = \overline{\langle X \rangle}$, then $d(M/N) = d(HN/N) \leq d(H) \leq r_2$.
$r_1 \leq r_4$: $H \leq_c G$. Then $d(H) = \sup\{ d(HN/N) : N \trianglelefteq_o G \}$, by (5.1)(b).

Definition: G a profinite group. Then the **rank** is $rk(G)$, the common value of $r_1, \ldots, r_4$.

Remark: (i) G finite rank $\Rightarrow$ G f.g.
(ii) G a f.g., powerful, pro-p group $\Rightarrow$ G has finite rank. (8.7).
(iii) G profinite, $N \trianglelefteq_c G$, then $\max\{ rk(N), rk(G/N) \} \leq rk(G) \leq rk(N) + rk(G/N)$. (Exercise.)
Deduce that if $H \leq_o G$ and $rk(H)$ finite, then $rk(G)$ finite.
Thus G f.g. and $H \leq_o G$, H powerful $\Rightarrow$ G has finite rank.

Theorem 8.11: G a pro-p group. G has finite rank iff G f.g. and G has an open powerful subgroup (in which case G has a powerful open characteristic subgroup).
Proof: ($\Rightarrow$) (8.9)
($\Leftarrow$) Remark above.

So, G has finite rank iff G is virtually powerful. The following theorem (which we won't prove) gives an algebraic condition for being p-adic analytic.

Theorem: A topological group G is p-adic analytic iff G has an open subgroup which is a pro-p group of finite rank.

9. Uniform pro-p groups.

Definition: A pro-p group G is **uniformly powerful** (or just **uniform**) if
(i) G f.g.
(ii) G powerful
(iii) $\forall i$, $|P_i(G) : P_{i+1}(G)| = |G : P_2(G)|$, $\forall i \geq 1$.

Remark: Theorem (8.5) tells us that the map $f_i : P_i(G)/P_{i+1}(G) \to P_{i+1}(G)/P_{i+2}(G)$, $xP_{i+1}(G) \mapsto x^p P_{i+2}(G)$, is a surjective homomorphism for f.g. powerful pro-p group G. Condition (iii) above is equivalent to saying that the f_i are isomorphisms.

Theorem 9.1: G a f.g. powerful pro-p group. Then $P_k(G)$ is uniform for all sufficiently large k.
Proof: Let $|P_i(G) : P_{i+1}(G)| = p^{d_i}$. As in remark, $d_1 \geq d_2 \geq \cdots \geq d_i \geq \cdots$, so $\exists\, m$ s.t. $d_k = d_m$ $\forall\, k \geq m$.
Let $G_k = P_k(G)$. (8.5) $\Rightarrow$ $P_i(G_k) = G_{k+i-1}$ and G_k powerful.
So G_k is a uniform subgroup, as required.

Corollary 9.2: A pro-p group of finite rank, G, has a characteristic open uniform subgroup.

Proof: (8.11) $\Rightarrow$ $H \leq_o G$, H characteristic and powerful.
(9.1) $\Rightarrow$ $P_k(H)$ uniform, characteristic, and open in H. $\Rightarrow$ $P_k(H)$ is the required subgroup.

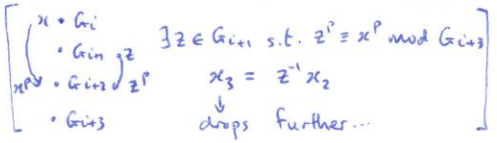
Proposition 9.3: G a f.g. powerful pro-p group. The following are equivalent.
(a) G uniform
(b) $d(P_i(G)) = d(G)$ $\forall i \geq 1$
(c) $d(H) = d(G)$ for every powerful open subgroup H of G.

Proof: (a) $\Leftrightarrow$ (b): (8.5) $\Rightarrow$ $\Phi(P_i(G)) = P_{i+1}(G)$, $|P_i(G)/P_{i+1}(G)| = |G/P_2(G)|$
(c) $\Rightarrow$ (b): Clear.
(b) $\Rightarrow$ (c): Note that if H is a powerful open subgroup of G, then $H \geq P_i(G)$, some i, so $d(P_i(G)) \leq d(H) \leq \mathrm{rk}(G) = d$.

Theorem 9.4: A powerful f.g. pro-p group is uniform iff it is torsion-free.

Proof: ($\Rightarrow$) G powerful f.g. pro-p group, write $G_i = P_i(G)$. Suppose G is not torsion-free. Then $\exists\, x \in G$, $o(x) = p$ (exercise: elements of finite order have p-power order). Say $x \in G_i \setminus G_{i+1}$. Then $1 \neq xG_{i+1} \in G_i/G_{i+1}$, $1 = x^p G_{i+2} \in G_{i+1}/G_{i+2}$, so the map $f_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ is not injective. So G is not uniform.

($\Leftarrow$) Suppose G is not uniform. Then f_i, $xG_{i+1} \mapsto x^p G_{i+2}$, is surjective but not injective, for some i. So $\exists\, x \in G_i \setminus G_{i+1}$ s.t. $x^p \in G_{i+2}$. Put $x_2 = x$, and suppose that for some $n \geq 2$ we have $x_2, \dots, x_n$ satisfying $x_j^p \in G_{i+j}$ and $x_j \equiv x_{j-1} \bmod G_{i+j-2}$, $2 \leq j \leq n$.



So, $\exists\, z \in G_{i+n-1}$ s.t. $z^p \equiv x_n^p \bmod G_{i+n-1}$.
Put $x_{n+1} = z^{-1}x_n$, then $x_{n+1} \equiv x_n \bmod G_{i+n-1}$.
$x_{n+1}^p \equiv z^{-p}x_n^p [x_n, z^{-1}]^{p(p-1)/2} \equiv 1 \bmod G_{i+n-1}$ (p odd),
since $[G_{i+n-1}, G]^p \leq G_{i+n-1}$, $[G_{i+n-1}, G, G] \leq G_{i+n-1}$.

Thus $x_2, \dots, x_n, \dots$ is constructed recursively and is Cauchy, so has a limit, $\lim x_n = x_\infty$, say, $\in G$. And $x_\infty \equiv x \not\equiv 1 \bmod G_{i+1}$, $x_\infty^p \equiv x_n^p \equiv 1 \bmod G_{i+n-1}$ $\forall n$,
$\Rightarrow x_\infty^p \equiv 1$. Ie, G has torsion.

Lemma 9.5: $A, B \leq_o G$, a pro-p group, A, B uniform, then $d(A) = d(B)$.

Proof: $A \cap B$ is an open subgroup of A, so $A \cap B \geq P_i(A)$, some i. Ie, $P_i(A) \leq A \cap B \leq B$.
Then $d(B) = d(P_i(A)) = d(A)$.

Definition: G a pro-p group of finite rank. The dimension of G is $\dim G = d(H)$, where H is any open uniform subgroup.

Remark: $\dim G$ is the dimension of G as a p-adic analytic group.

Recall: A Lie algebra over a commutative ring R is an R-module, with a binary operation $(\cdot,\cdot) : L \times L \to L$, which is R-bilinear, and
- $(x,x) = 0$ $\forall x \in L$
- $((x,y),z) + ((y,z),x) + ((z,x),y) = 0$ $\forall x,y,z \in L$. (Jacobi identity.)

Eg, if A is an associative algebra over R, define $(a,b) = ab - ba$, eg with $A = M_n(R)$

We define an "intrinsic" Lie algebra structure on a uniform pro-p group, so we need to define addition, a Lie bracket, and multiplication by $\mathbb{Z}_p$.

§: Multiplicative Structure.

Theorem 9.6: G a uniform pro-p group, $G = \overline{\langle a_1, \dots, a_d \rangle}$, where $d = d(G)$.
Then $\theta : \overbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}^{d} \to G$, $(\lambda_1, \dots, \lambda_d) \mapsto a_1^{\lambda_1} \cdots a_d^{\lambda_d}$ is a homeomorphism.

Proof: By (8.6), $G = \overline{\langle a_1 \rangle} \cdots \overline{\langle a_d \rangle}$. So, given $a \in G$, $a = a_1^{\lambda_1} \cdots a_d^{\lambda_d}$ with $\lambda_1, \dots, \lambda_d \in \mathbb{Z}_p$ $-(*)$.
Fix k, write $G_k = P_k(G)$, consider G/G_{k+1}. Now, G is uniform, so $|G/G_{k+1}| = p^{kd}$, and $G/G_{k+1} = \langle a_1 G_{k+1} \rangle \cdots \langle a_d G_{k+1} \rangle$, by (7.14), and $|\langle a_i G_{k+1} \rangle| \leq p^k$, so $|\langle a_i G_{k+1} \rangle| = p^k$.
So each element of G/G_{k+1} can be written as $a_1^{e_1} \cdots a_d^{e_d} G_{k+1}$, with $e_1, \dots, e_d$ determined uniquely modulo p^k. So in $(*)$, $\lambda_1, \dots, \lambda_d$ determined uniquely modulo p^k $\forall k$, so $\lambda_1, \dots, \lambda_d$ are determined uniquely as p-adic integers. Thus θ is a bijective map.
Consider the restriction of θ to the ith component, so $\theta|_i : \mathbb{Z}_p \to \overline{\langle a_i \rangle}$, $\lambda_i \mapsto a_i^{\lambda_i}$, which is a group homomorphism from a f.g. pro-p group to a profinite group, so is continuous by (5.10). Also, multiplication is continuous $\Rightarrow \theta$ is continuous. Finally, $\mathbb{Z}_p^d$ and G are compact and Hausdorff $\Rightarrow \theta$ is a homeomorphism.

§: Additive Structure.

We are going to define an operation "addition" on our uniform G, $(G_i = P_i(G))$

Lemma 9.7: The map $G_k \to G_{k+n}$, $x \mapsto x^{p^n}$ $\forall n, k$, is a bijective homeomorphism, and induces a bijection $G_k/G_{k+m} \to G_{n+k}/G_{n+k+m}$, $xG_{k+m} \mapsto x^{p^n} G_{n+k+m}$, $\forall k, n, m$.

Proof: Write $f(x) = x^{p^n}$. (8.5) $\Rightarrow f(G_k) = G_{k+n}$ $(G^k = G^{\{p^{k-1}\}})$.
(8.5)(iv) $\Rightarrow$ '$x \equiv y \ (G_{k+m}) \Rightarrow f(x) \equiv f(y) \ (G_{n+k+m})$'. Thus the map $G_k/G_{k+m} \to G_{n+k}/G_{n+k+m}$ is a surjection. But G uniform, so $|G_k/G_{k+m}| = |G_{n+k}/G_{n+k+m}|$, hence the map is a bijection.
So if $x, y \in G_k$ and $f(x) = f(y)$, then $x \equiv y \bmod G_{k+m}$ $\forall m \Rightarrow f : G_k \to G_{k+n}$ injective, since $\bigcap_m G_{k+m} = 1$. Clearly f is continuous (since multiplication is), and G is compact and Hausdorff, so f is a homeomorphism.

Remark: The previous lemma shows that given $x \in G_{n+1}$, then x has a unique p^nth root, $x^{p^{-n}} \in G$. Hence the following definition makes sense.

Definition: G a uniform pro-p group. For $x, y \in G$, define $x +_n y = (x^{p^n} y^{p^n})^{p^{-n}}$

Remark: So, $(G_{n+1}, \cdot) \to (G, +_n)$, $x \mapsto x^{p^{-n}}$ is an isomorphism.

Lemma 9.8: If $n > 1$, $x, y \in G$, $u, v \in G_n$, then $xu +_n yv \equiv x +_n y \equiv x +_{n-1} y \bmod G_n$, and $\forall m > n$, $x +_m y \equiv x +_n y \bmod G_{n+1}$.

Proof: (5.7) $\Rightarrow [G_n, G_n] \leq G_{2n}$, so $x^{p^n} y^{p^n} \equiv (x^{p^{n-1}} y^{p^{n-1}})^p \bmod G_{2n} \equiv (x +_{n-1} y)^{p^n} \bmod G_{2n}$. Then take p^nth roots $\Rightarrow x +_n y = (x^{p^n} y^{p^n})^{p^{-n}} \equiv x +_{n-1} y \bmod G_n$. Also, $(xu)^{p^n} \equiv x^{p^n} \bmod G_{2n}$, yv similarly, so $x^{p^n} y^{p^n} \equiv (xu)^{p^n} (yv)^{p^n} \bmod G_{2n} \Rightarrow x +_n y = (x^{p^n} y^{p^n})^{p^{-n}} \equiv ((xu)^{p^n} (yv)^{p^n})^{p^{-n}} \equiv xu +_n yv \bmod G_n$.
Then use induction.

So $(x +_n y)$ defines a Cauchy sequence and we may make the following definition.

Definition: $x, y \in G$, uniform. Then $x+y = \lim_{n\to\infty} x +_n y$.

Remark: (i) $x+y \equiv x +_n y \pmod{G_{n+1}}$
(ii) $u, v \in G_n$ then $xu+yv \equiv x+y \pmod{G_n}$

Proposition 9.9: The set G with the operation $+$ is an abelian group, with identity 1 and inversion given by $x \mapsto x^{-1}$.

Proof:
- $x +_n 1 = (x^{p^n} \cdot 1)^{p^{-n}} = x \quad \forall n \Rightarrow x+1 = x \quad \forall x$.
- $x +_n x^{-1} = (x^{p^n}(x^{-1})^{p^n})^{p^{-n}} = 1 \quad \forall n \Rightarrow x + x^{-1} = 1 \quad \forall x$
- $x, y, z \in G$, $n \geq 1$. $x+y = (x+_n y)u$, some $u \in G_{n+1}$.
  $(x+y)+z \equiv (x+_n y)+z \pmod{G_{n+1}} \equiv (x+_n y)+_n z \pmod{G_{n+1}}$
  Similarly $x+(y+z) \equiv x +_n (y+_n z) \pmod{G_{n+1}}$.
  But $x +_n (y +_n z) = (x^{p^n}(y^{p^n} z^{p^n})^{p^{-n}})^{p^{-n}} = \cdots = (x +_n y) +_n z \quad \forall n$. So associative.
- $[x^{p^n}, y^{p^n}] \in [G_{n+1}, G_{n+1}] \leq G_{2n+2}$, so $x^{p^n} y^{p^n} \equiv y^{p^n} x^{p^n} \pmod{G_{2n+2}}$,
  so $x +_n y \equiv y +_n x \pmod{G_{2n+2}} \quad \forall n$. So abelian.

Notation: Use additive notation for $(G, +)$, write 0 for 1 and $-x$ for x^{-1}, etc.

Lemma 9.10: (i) If $xy = yx$ then $x+y = xy$
(ii) $m \in \mathbb{Z}$, then $mx = x^m$
(iii) $n \geq 1$, then $p^{n-1} G = G_n$
(iv) $x, y \in G_n$, then $xy \equiv x+y \pmod{G_{n+1}}$

Proof: (i) $xy = yx$, so $x^{p^n} y^{p^n} = (xy)^{p^n}$.
(iii) $m \geq 1$: use (i) and induction. $m = 0$: ✓ $m < 0$: note $-x = x^{-1}$.
(iii) Recall $G_n = G^{\{p^{n-1}\}}$ from (8.5)(iii). Use (ii)
(iv) Recall $G_n/G_{n+1} \to G_{2n}/G_{2n+1}$, $x G_{n+1} \mapsto x^{p^n} G_{2n+1}$ is a homomorphism.
So, $(xy)^{p^n} \equiv x^{p^n} y^{p^n} \pmod{G_{2n+1}} \Rightarrow xy \equiv x +_n y \pmod{G_{n+1}} \quad \forall n$.

Corollary 9.11: For each n, G_n is an additive subgroup of G; the additive cosets of G_n in G are the same as the multiplicative cosets of G_n in G.
Also, identity: $(G_n/G_{n+1}, +) \to (G_n/G_{n+1}, \cdot)$ is an isomorphism.
And the index of G_n in additive $(G, +)$ is equal to $|G : G_n|$

Proof: (9.10)(iii) $\Rightarrow G_n = p^{n-1} G$ - additive subgroup. For the cosets bit, if $a \in G$, $u \in G_n$, then
$a+u = a + 1.u \equiv a + 1 \equiv a \pmod{G_n} \Rightarrow a+u \in aG_n \Rightarrow a + G_n \subseteq aG_n$.
Also, $au - a = au + (-a) \equiv a + (-a) \equiv 0 \pmod{G_n} \Rightarrow au - a \in G_n \Rightarrow au \in a + G_n \Rightarrow aG_n \subseteq a + G_n$.
Hence, the notation G/G_n, as sets, is unambiguous. $|G : G_n|$ is the same for either group.
Remaining part: (9.10)(iv)

Proposition 9.12: With the original topology of G, $(G,+)$ is a uniform pro-p group of dimension $d = d(G)$. Moreover, if $G = \overline{\langle a_1, \dots, a_d \rangle}$ multiplicatively, then also $G = \overline{\langle a_1, \dots, a_d \rangle}_+$ additively.

Proof: G compact, Hausdorff, totally disconnected space. $x \mapsto -x = x^{-1}$ continuous.
Consider $G \times G \to G$, $(x,y) \mapsto x+y$. We noted that if $u, v \in G_n$ then $xu + yv \equiv x+y \pmod{G_n}$. Since G_n form a base of nbhds of $1 \Rightarrow x+y$ continuous.
So $(G,+)$ is a topological group.
Further, the index of G_n in $(G,+)$ is $|G : G_n| = p$-power, so we have a base of nbhds of 1 of p-power $\Rightarrow G$ is a pro-p group.
$(G,+)$ abelian $\Rightarrow G$ powerful. So, lower p-series of $(G,+)$ is given by p-power series, ie $P_n G = G_{n+1}$. And $|G_n : G_{n+1}| = p^d$ $\forall n$ (G uniform) $\Rightarrow (G,+)$ uniform, $\dim = d$.
Suppose $\overline{\langle X \rangle} = G$ multiplicatively. $\Rightarrow G/G_2 = \langle x \rangle G_2 / G_2$. But (9.11) $\Rightarrow (G,+)/G_2 = \langle x \rangle_+ + G_2/G_2$, $\langle x \rangle_+$ additive group generated by X. But $G_2 = pG = \Phi(G,+) \Rightarrow (G,+)$ generated topologically by $\langle x \rangle_+$.

Remark: $(G,+)$ is a pro-p group, so admits a natural action by $\mathbb{Z}_p$, ie g^λ, $\lambda \in \mathbb{Z}_p$.
Also, since $(G,+)$ is abelian, $(gh)^\lambda = g^\lambda h^\lambda$ (see 6.3). So $(G,+)$ is a $\mathbb{Z}_p$-module.

Theorem 9.13: G a uniform pro-p group of dimension d, and $G = \overline{\langle a_1, \dots, a_d \rangle}$. Then $(G,+)$ is a free $\mathbb{Z}_p$-module on the basis $\{a_1, \dots, a_d\}$.

Proof: (9.12) $\Rightarrow$ $d(G,+) = d$ and $\{a_1, \dots, a_d\}$ generates $(G,+)$ topologically.
(9.6) applied to $(G,+)$ shows that $a \in (G,+)$ can be written uniquely as $a = \lambda_1 a_1 + \cdots + \lambda_d a_d$, $\lambda_i \in \mathbb{Z}_p$, which is what we want.
(Note: $\mu_i \in \mathbb{Z}$, $\mu_i \to \mu \in \mathbb{Z}_p$, $\mu a = \lim \mu_i a = \lim a^{\mu_i} = a^\mu$. See (9.10) (iii).)

Corollary 9.14: G a uniform pro-p group, $\dim(G) = d$. Then the action of $\mathrm{Aut}(G)$ on G is $\mathbb{Z}_p$-linear w.r.t the $\mathbb{Z}_p$-module structure of $(G,+)$. Hence $\mathrm{Aut}(G) \leq GL_d(\mathbb{Z}_p)$.

Proof: Let $\alpha \in \mathrm{Aut}(G)$. Then α is continuous (use (5.10)).
Let $x \in G^{p^n}$, then $x = z^{p^n}$, some $z \in G$ (8.5), so $\alpha(x^{p^{-n}}) = \alpha((z^{p^n})^{p^{-n}}) = \alpha(z) = \alpha(z^{p^n})^{p^{-n}} = \alpha(x)^{p^{-n}}$
ie, α respects taking p^nth roots. $\Rightarrow \alpha$ respects $+_n$ $\Rightarrow \alpha$ respects $+$ by continuity.
(ie $\alpha(x+y) = \alpha(x) + \alpha(y)$.) Also, since $\lambda g = g^\lambda = g^{\lim a_i}$, $a_i \in \mathbb{Z}$, α continuous $\Rightarrow$ α respects multiplication by $\mathbb{Z}_p$. So α is an automorphism of $(G,+)$ and the result follows.

Corollary 9.15: G a pro-p group of finite rank, dimension d. Then $\exists$ an exact sequence $1 \to \mathbb{Z}_p^e \to G \to GL_d(\mathbb{Z}_p) \times F$ for some $e \leq d$, and some finite p-group F.

Notation: $G' \xrightarrow{f} G \xrightarrow{g} G''$, G, G', G'' groups, f, g homomorphisms. It is *exact* if $\mathrm{im} f = \ker g$.
For example, if $H \trianglelefteq G$, have $1 \to H \to G \to G/H \to 1$.
(inclusion; canonical surjection.)

Proof of 9.15: $\exists H \trianglelefteq_o G$, H uniform (8.15). Let $A = Z(H)$, then A is closed in H (by sheet 1, qn 4). $\Rightarrow A$ is torsion-free, abelian pro-p group of $\mathrm{rk} A \leq \mathrm{rk} H = d$.
$\Rightarrow A \cong \mathbb{Z}_p^e$, some $e \leq d$. (eg 9.6)
For $g \in G$, let $g^* \in \mathrm{Aut}\, H$ s.t. $g^*(h) = g^{-1}hg$. Then $\theta : G \to \mathrm{Aut}\, H \times G/H$, $g \mapsto (g^*, gH)$ is a homomorphism, with $\ker \theta = A$. Finally, $\mathrm{Aut}\, H \leq GL_d(\mathbb{Z}_p)$, by 9.14.

§ Lie Algebra Structure

Note, all free $\mathbb{Z}_p$-modules of given rank are isomorphic, so we've lost a lot of information about our uniform pro-p group G when we moved to the $\mathbb{Z}_p$-module $(G,+)$. We can regain this information by defining a Lie bracket.

Definition: $x, y \in G$, uniform, $n \in \mathbb{N}$. Let $(x,y)_n = [x^{p^n}, y^{p^n}]^{p^{-2n}}$.

Remark: $[x^{p^n} y^{p^n}] \in [G_{n+1}, G_{n+1}] \leq G_{2n+2}$.

Lemma 9.16: If $n \geq 1$, $x, y \in G$, $u, v \in G_n$, then $(xu, yv)_n \equiv (x,y)_n \equiv (x,y)_{n-1} \pmod{G_{n+1}}$, and $\forall\, m > n$, $(x,y)_m \equiv (x,y)_n \pmod{G_{n+2}}$

Proof: $(xu)^{p^n} \equiv x^{p^n} \pmod{G_{2n}}$, $(yv)^{p^n} \equiv y^{p^n} \pmod{G_{2n}}$.
Using $[ab,c] = [a,c]^b [b,c]$ and that $[G_{2n}, G_{n+1}] \leq G_{3n+1} \Rightarrow (xu, yv)_n \equiv (x,y)_n \pmod{G_{n+1}}$.
Again, using commutator identities, if $a \in G_i$, $b \in G_j$, then $[a^p, b] \equiv [a,b]^p \pmod{G_{2i+j}}$, and $[a, b^p] \equiv [a,b]^p \pmod{G_{i+2j}}$. Taking $a = x^{p^n} \in G_{n+1}$, $b = y^{p^{n-1}} \in G_n$, we get $[x^{p^n}, y^{p^n}] \equiv [x^{p^n}, y^{p^{n-1}}]^p \pmod{G_{3n+1}}$. Taking $a = x^{p^{n-1}} \in G_{n+1}$, $b = y^{p^{n-1}} \in G_n$, we get $[x^{p^n}, y^{p^{n-1}}] \equiv [x^{p^{n-1}}, y^{p^{n-1}}]^p \pmod{G_{3n}}$.
Thus $[x^{p^n}, y^{p^n}] \equiv [x^{p^{n-1}}, y^{p^{n-1}}]^{p^2} \pmod{G_{3n+1}} \equiv (x,y)_{n-1}^{p^{2n}} \pmod{G_{3n+1}}$
Extracting p^{2n}th roots, $(x,y)_n \equiv (x,y)_{n-1} \pmod{G_{n+1}}$.
Finally, use induction on $m-n$.

Thus, for $x, y \in G$, $(x,y)_n$ defines a Cauchy sequence.

Definition: $x, y \in G$ uniform, let $(x,y) = \lim_{n \to \infty} (x,y)_n$.

Theorem 9.17: With the operation $(,)$, the $\mathbb{Z}_p$-module $(G,+)$ becomes a Lie algebra over $\mathbb{Z}_p$.

To prove this, we need that $(,)$ is a Lie bracket, and that it's bilinear wrt the $\mathbb{Z}_p$-module structure on $(G,+)$. We use the following lemmas.

Lemma 9.18: (i) $(x,y) = -(y,x)$
(ii) $(x,y) \in G^{p^\varepsilon}$ ($\varepsilon = 1$ for $p \neq 2$, $\varepsilon = 2$ for $p = 2$)

Proof: (i) Note $[x,y] = [y,x]^{-1}$.
(ii) $p \neq 2$ ✓. If $p = 2$, need G a powerful 2-group, $[G_i, G_j] \leq G_{i+j+1}$.

Remark: Part (ii) tells us that the Lie algebra we're constructing is powerful. Ie, $\simeq \mathbb{Z}_p^d$ and satisfies $(L,L) \leq p^\varepsilon L$.

Lemma 9.19: $\lambda \in \mathbb{Z}_p$, $\lambda \equiv a \ (p^n)$ where $a \in \mathbb{Z}$. Then $(\lambda x, y) \equiv (ax, y) \pmod{G_{n+1}}$.
Proof: Recall $\lambda x = x^\lambda = x^a x^b$, where $p^n \mid b$. $\Rightarrow \lambda x = x^a u$, some $u \in G_{n+1}$.
$\Rightarrow (\lambda x, y) \equiv (x^a, y) \equiv (ax, y) \pmod{G_{n+1}}$, by (9.16).

Lemma 9.20: $\forall n$, $(x,z)_n +_n (y,z)_n \equiv (x +_n y, z)_n \pmod{G_{n+3}} \Rightarrow (x,z) + (y,z) = (x+y, z)$.
Proof: Note that $[x^{p^n}, z^{p^n}]^{p^{-n}} [y^{p^n}, z^{p^n}]^{p^{-n}} = ((x,z)_n +_n (y,z)_n)^{p^n}$, and $[x^{p^n} y^{p^n}, z^{p^n}]^{p^{-n}} = (x +_n y, z)_n^{p^n}$.
Also, if we let $a = [x^{p^n}, z^{p^n}]^{p^{-n}}$ and $b = [y^{p^n}, z^{p^n}]^{p^{-n}}$, and recall that $(ab)^{p^n} \equiv a^{p^n} b^{p^n} \pmod{G_{n+3}}$, we get $[x^{p^n} y^{p^n}, z^{p^n}]^{p^{-n}} \equiv [x^{p^n}, z^{p^n}]^{p^{-n}} [y^{p^n}, z^{p^n}]^{p^{-n}} \pmod{G_{2n+3}}$.
These three equalities give us $(x,z)_n +_n (y,z)_n \equiv (x +_n y, z)_n \pmod{G_{n+3}}$, and the second result follows.

These three lemmas give us bilinearity of $(,)$ over $\mathbb{Z}_p$, and we must check that it actually is a Lie bracket. (Exercise.)

Proposition 9.21: H a uniform closed subgroup of G, uniform. Let $N \trianglelefteq_c G$ s.t. G/N uniform.
(i) The inclusion map $H \hookrightarrow G$ is a monomorphism of Lie algebras $(H, +, (,)) \to (G, +, (,))$.
(ii) N is uniform.
(iii) N is an ideal in $(G, +, (,))$; the additive cosets of N in G are the same as the multiplicative cosets, so $(G/N, +, (,)) = (G, +, (,))/(N, +, (,))$.
Moreover, the natural homomorphism $*: G \to G/N$ is a Lie algebra epimorphism.
Proof: (i) follows since H inherits subspace topology.
(ii) G/N is torsion-free, by (9.4). So if $x^{p^n} \in N \Rightarrow x \in N$. Also, $G^p = G^{(p)}$, so $G^p \cap N = N^p$. So $N/N^p = N/G^p \cap N \cong NG^p/G^p$, abelian.
$\Rightarrow N$ powerful ($p \neq 2$) and torsion-free, so N uniform (9.4). (Similarly for $p = 2$.)
(iii) Consider $*: G \to G/N$. Let $a, b \in G$, let $c_n = a +_n b$. Then $(c_n^*)^{p^n} = (c_n^{p^n})^*$
$= (a^{p^n} b^{p^n})^* = (a^*)^{p^n} (b^*)^{p^n} \Rightarrow c_n^* = a^* +_n b^*$. Continuity of $*$ (5.10) $\Rightarrow$
$a^* + b^* = \lim c_n^* = (\lim c_n)^* = (a+b)^*$. Similarly, $*$ respects Lie bracket and multiplication by $\mathbb{Z}_p$, so is a Lie algebra homomorphism.
$\ker * = N$, an ideal. $aN = bN \Leftrightarrow a - b \in N \Leftrightarrow (a-b)^* = 0 \Leftrightarrow a^* = b^* \Leftrightarrow aN = bN$.
Ie $(G,+)/(N,+) = (G/N, +)$, as sets.

10. Normed Algebras.

R, a ring with identity $1_R \neq 0$.

Definition: A norm on a ring R is a function $\|\cdot\| : R \to \mathbb{R}$, s.t. $\forall a, b \in R$,
(N1) $\|a\| \geq 0$, with $=$ iff $a = 0$.
(N2) $\|1_R\| = 1$ and $\|ab\| \leq \|a\| \cdot \|b\|$.
(N3) $\|a \pm b\| \leq \max\{\|a\|, \|b\|\}$.
Then $(R, \|\cdot\|)$ is called a normed ring.

Remark: (i). (N3) is called an "ultrametric inequality". This kind of norm is called "non-Archimedean".

(ii) (N3) $\Rightarrow \|a_1+\cdots+a_n\| \leq \max_i\{\|a_i\|\}$; $\|a \pm b\| = \max\{\|a\|, \|b\|\}$ if $\|a\| \neq \|b\|$.

(iii)

Given $(R, \|\cdot\|)$, a normed ring, we can define a distance function, $d(x,y) = \|x-y\|$, so we have a metric space.

Definition: (i) $(R, \|\cdot\|)$ is complete if every Cauchy sequence converges to an element of R.

(ii) $(\hat{R}, \|\cdot\|)$ is a completion of R if

(a) R is dense in $\hat{R}$ and the norm on $\hat{R}$ extends that on R.

(b) $\hat{R}$ is complete.

Proposition 10.1: If $(R, \|\cdot\|)$ is a normed ring, then $\exists$ a completion $\hat{R}$ of R, which is unique up to isomorphism.

Recall: Example, $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$, s.t. $|0|_p = 0$, $|a|_p = p^{-k}$ where $a = p^k \cdot \frac{m}{n}$, $p \nmid mn$. This defines a norm on $\mathbb{Q}$, and the completion of $(\mathbb{Q}, |\cdot|_p)$ is the p-adic field, $\mathbb{Q}_p$. Ostrowski $\Rightarrow$ p-adic norms are the only non-trivial norms on $\mathbb{Q}$. (Note that the usual metric is not a norm here.)

The following generalises the construction of the p-adic norm on $\mathbb{Z}$.

Lemma 10.2: R a ring and $R = R_0 \supseteq R_1 \supseteq \cdots \supseteq R_i \supseteq R_{i+1} \supseteq \cdots$, a chain of ideals s.t.

(a) $\bigcap_{i \in \mathbb{N}} R_i = 0$

(b) $\forall\, i,j$, $R_i R_j \subseteq R_{i+j}$.

Fix $c \in \mathbb{R}$, $c > 1$, $\|\cdot\| : R \to \mathbb{R}$, s.t. $\|0\| = 0$, $\|a\| = c^{-k}$ where $a \in R_k \setminus R_{k+1}$.

Then $(R, \|\cdot\|)$ is a normed ring.

Remark: We can extend our norm to $\varprojlim (R/R_i)$ in the natural way, ie, if $\alpha \in \varprojlim (R/R_i)$, $\alpha = (a_i)$, then $\|\alpha\| = \lim \|a_i\|$.

It can then be shown that $(\hat{R}, \|\cdot\|) \cong (\varprojlim (R/R_i), \|\cdot\|)$.

Definition: A, a $\mathbb{Q}_p$-algebra. Then $(A, \|\cdot\|)$ is a normed $\mathbb{Q}_p$-algebra if $(A, \|\cdot\|)$ is a ring, and

(N4) $\|\lambda a\| = |\lambda|_p \|a\|$, $\forall\, a \in A$, $\lambda \in \mathbb{Q}_p$.

Example: Define a norm on $M_n(\mathbb{Q}_p)$ by $\|(a_{ij})\| = \max\{|a_{ij}|_p, i,j\}$.

§ Sequences & Series.

Let $(R, \|\cdot\|)$ be a complete normed ring. The following results illustrate how non-Archimedean analysis is different from Archimedean.

Definition: T a countably infinite, a map $T \to R$, $n \to a_n$, we say

(i) the family $(a_n)_{n\in T}$ converges to a, written $\lim_{n\in T} a_n = a$, if for each $\varepsilon > 0$ $\exists$ a finite subset $T' \subset T$ s.t. $\|a - a_n\| < \varepsilon$ $\forall\, n \in T \setminus T'$.

(ii) $\sum a_n$ converges to s, written $\sum_{n\in T} a_n = s$, if for each $\varepsilon > 0$ $\exists$ finite subset $T' \subset T$ s.t. $\forall$ finite subsets T'' with $T' \subseteq T'' \subset T$ we have $\| s - \sum_{n\in T''} a_n \| < \varepsilon$.

Proposition 10.3: T a countably infinite set, $T \to R$, $n \mapsto a_n$. Let $i \mapsto n(i)$ be a bijection from $\mathbb{N}$ onto T.

(i) $\lim_{n\in T} a_n = a$ iff $\lim_{i\to\infty} a_{n(i)} = a$.

(ii) $\sum_{n\in T} a_n = s$ iff $\lim_{n\in T} a_n = 0$.

(iii) $\sum_{n\in T} a_n = s$ iff $\sum_{i\in\mathbb{N}} a_{n(i)} = s$.

(iv) $\sum_{n\in T} a_n = s$, then $\|s\| \le \sup\{\|a_n\| : n \in T\}$

(v) If $\sum_{n\in T} a_n = s$ and for some $m \in T$, $\|a_m\| > \|a_n\|$ $\forall\, n \in T \setminus \{m\}$, then $\|s\| = \|a_m\|$.

Proof: (iv) Let $\sigma = \sup\{\|a_n\| : n \in T\}$. If $\sigma = 0$, then $s = 0$ and we're done. So suppose $\sigma > 0$.
By convergence, $\exists$ finite subset $T' \subset T$ s.t. $\| s - \sum_{n\in T'} a_n \| < \sigma$.
So, $\|s\| \le \max\{\| s - \sum_{n\in T'} a_n \|, \|a_n\| : n \in T'\} \le \sigma$.

(v) Let $\sigma = \|a_m\| > \|a_n\|$ $(n \ne m)$. (ii) $\Rightarrow$ $\|a_n\| < \frac{\sigma}{2}$ $\forall$ but finitely many $n \in T$.
Hence, $\sup\{\|a_n\| : n \in T \setminus \{m\}\} < \sigma$. By (iv), $\|s - a_m\| = \| \sum_{T\setminus\{m\}} a_n \| \le \sup\{\|a_n\| : n \in T\setminus\{m\}\} < \|a_m\|$.
So $\|s\| = \max\{\|s - a_m\|, \|a_m\|\} = \|a_m\|$.

The following result says that if two power series are equal on a nbhd of 0, then they are identical

Proposition 10.4: Let A be a complete $\mathbb{Q}_p$-normed algebra and $a_n \in A$. Suppose $\exists$ a nbhd V of 0 in $\mathbb{Q}_p$ s.t. $\sum_{n\in\mathbb{N}} \lambda^n a_n = 0$ $\forall\, \lambda \in V$. Then $a_n = 0$ $\forall\, n \in \mathbb{N}$.

Proof: Suppose not all $a_\lambda = 0$ and choose m minimal s.t. $a_m \ne 0$. Let $0 \ne \lambda_0 \in V$, set $r = |\lambda_0|_p$.
$\sum \lambda_0^n a_n$ converges $\Rightarrow$ $\exists\, C > 0$ s.t. $r^n \|a_n\| = \|\lambda_0^n a_n\| < C$ $\forall\, n \in \mathbb{N}$.
Choose $\lambda \in V$ s.t. $0 < |\lambda| < r \cdot \min\{C^{-1} r^m \|a_m\|, 1\}$. Let $n > m$, then
$\|\lambda^n a_n\| = |\lambda|_p^n \|a_n\| \le r^{n-m-1} \|a_n\| \, |\lambda|_p^{m+1}$ (since $|\lambda|_p \le |r|$), $< \frac{C}{r^{m+1}} \cdot |\lambda| \cdot |\lambda|^m$ (defn of C)
$< \|a_m\| \cdot |\lambda|^m$ (since $\|a_m\| > \frac{|\lambda| C}{r^{m+1}}$) $= \|\lambda^m a_m\|$.
Since $a_n = 0$ $\forall\, n < m$, (10.3) (v) $\Rightarrow$ $\| \sum \lambda^n a_n \| = \|\lambda^m a_m\| \ne 0$ #.

11. Another Lie Algebra of a Uniform Pro-p Group.

Let G be a uniform pro-p group. $A = \mathbb{Q}_p[G]$, the group algebra. (This has elements of the form $\sum_{g\in G} a_g g$, $a_g \in \mathbb{Q}_p$, s.t. all but finitely many are zero. Addition is: $\sum a_g g + \sum b_g g = \sum (a_g + b_g) g$, multiplication by $\mathbb{Q}_p$ is: $\lambda \sum a_g g = \sum \lambda a_g g$; group multiplication is: $(\sum a_g g)(\sum b_g g) = \sum c_g g$, where $c_g = \sum_{x\in G} a_x b_{x^{-1}g}$.)

We want to define a norm on A which is compatible with the topology on G, (Note, $G \hookrightarrow \mathbb{Q}_p[G]$.), so that A is a normed $\mathbb{Q}_p$-algebra. First we define a norm on $R = \mathbb{Z}_p[G]$.

Definition: Let $I_k = \ker\left(\mathbb{Z}_p[G] \to \mathbb{Z}_p[G/G_k]\right)$, where the map is $\sum a_g g \mapsto \sum a_g g\, G_k$.
Then $I_k = \langle (x-1) : x \in G_k \rangle$, the generalised augmentation ideal, since $\sum a_g g\, G_k = 0$ for fixed $g \Rightarrow \sum_{x \in G_k} a_{gx} = 0 \Rightarrow \sum_{x \in G_{k+1}} a_{gx} = -a_{g\bullet}$, so $\sum_{x \in G_k} a_{gx} \cdot gx = \sum_{x \in G_{k+1}} a_{gx}\, g(x-1)$.

Let $J_0 = R = \mathbb{Z}_p[G]$, $J = pR + I_1$, $J_k = J^k + I_k$, $k \geq 1$.

Lemma II.1: (i) $\forall\ l \geq k \geq 1$, $J_k = J^k + I_l$.
(ii) $\forall\ k, l \geq 0$, $J_k J_l \leq J_{k+l}$.
(iii) $\bigcap_{k \in \mathbb{N}} J_k = 0$.

Hence we can define a norm on $\mathbb{Z}_p[G] = R$ as follows: $\|0\| = 0$, $\|c\| = p^{-k}$ for $c \in J_k \setminus J_{k+1}$.
This norm is compatible with the norms on $\mathbb{Z}_p$ and G, since $\|\lambda c\| \leq |\lambda|_p \|c\|$, and $\|x - 1\| \leq p^{-k}$ for $x \in G_k$, $k \geq 1$. (Recall, G_k defines a basis of nbhds of 1)
Furthermore, this norm satisfies $\|\lambda c\| = |\lambda|_p \|c\|$ for $\lambda \in \mathbb{Z}_p$, $c \in \mathbb{Z}_p[G]$. This is dependent on G being uniform. We can therefore make the following definition.

Definition: If $a \in A = \mathbb{Q}_p[G]$, then $a = \lambda c$, some $\lambda \in \mathbb{Q}_p$, $c \in \mathbb{Z}_p[G]$.
Define $\|a\| = |\lambda|_p \|c\|$.

So $(A, \|\cdot\|)$ is a normed $\mathbb{Q}_p$-algebra. We call the completion $(\hat{A}, \|\cdot\|)$ of it the completed group algebra of uniform G.

§ Log & Exp.

To define log and exp on our completed group algebra $\widehat{\mathbb{Q}_p[G]}$, we need to consider formal power series in non-commuting variables (since G is not abelian).
So, $\mathbb{Q}_p \langle\langle X_1, \ldots, X_n \rangle\rangle$ will denote formal power series in non-commuting $X_1, \ldots, X_n$.

Definition: We define two formal power series in $\mathbb{Q}_p\langle\langle X \rangle\rangle$ as:
$$E(X) = \sum_{n=0}^{\infty} \frac{1}{n!} X^n \quad , \quad L(X) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} X^n .$$

We need to see where these power series converge

Lemma II.2: $n \in \mathbb{N}$, $v(n!) \leq \frac{n-1}{p-1}$, where $|x|_p = p^{-v(x)}$ (ie, $x = p^k \frac{m}{n}$, $p \nmid mn \Rightarrow k = v(x)$).
Proof: $v(n!) = \sum_{i=1}^{n} v(i)$. Now, $|\{i : v(i) \geq j \text{ and } 1 \leq i \leq n\}| = [n/p^j]$
$\therefore\ v(n!) \leq \sum_{j=1}^{n} n/p^j = \frac{n(1-p^{-k})}{p-1} \leq \frac{n-1}{p-1}$, where $p^k \leq n < p^{k+1}$.

Let $(B, \|\cdot\|)$ be a complete normed $\mathbb{Q}_p$-algebra.

Definition: For p odd, let $B_0 = \{x \in B : \|x\| \leq p^{-1}\}$.

Remark: Everything we do can be modified for $p = 2$, but from now on we shall concentrate on p odd.

Lemma 11.3: For each $x \in B_0$,

(i) $\sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n$ converges to an element in B_0.

(ii) $\sum_{n=0}^{\infty} \frac{1}{n!} x^n$ converges to an element in $1 + B_0$.

Proof: By (11.2), $|n|_p \geq |n!|_p \geq p^{-(n-1)/(p-1)}$. So if $\|x\| = p^{-r}$, for $n \geq 1$, $\left\| \frac{(-1)^{n+1}}{n} x^n \right\| \leq \left\| \frac{x^n}{n!} \right\| \leq p^{-nr + \frac{n-1}{p-1}}$.

For $r \geq \frac{1}{p-1}$, $\lim_{n \to \infty} p^{-nr + \frac{n-1}{p-1}} = 0$. Ie series converges for $x \in B_0$, by (10.3) (ii).

Also, if $n \geq 1$ and $x \in B_0$, then $\frac{(-1)^{n+1} x^n}{n} \in B_0$ and $\frac{x^n}{n!} \in B_0$, so we get the lemma.

Definition: For $x \in B_0$, we define $\underline{\log(1+x)} = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$, $\underline{\exp(x)} = \sum_{n=0}^{\infty} \frac{x^n}{n!}$.

After defining composition of formal power series, we can check that the following usual identities for log and exp hold.

Theorem 11.4: $x \in B_0$. Then

(i) $\log(\exp(x)) = x$

(ii) $\exp(\log(1+x)) = 1+x$

(iii) $\log((1+x)^n) = n \log(1+x)$, $n \in \mathbb{Z}$.

(iv) $\exp(nx) = (\exp(x))^n$, $n \in \mathbb{Z}$.

§ Campbell - Hausdorff Formula (CHF).

(Also known as the Baker - Campbell - Hausdorff Formula.)

This formula allows us to connect exp and log for non-commuting x and y.

Definition: Let $P(X,Y) = \mathcal{E}(X)\mathcal{E}(Y) - 1 \in \mathbb{Q}_p \langle\langle X, Y \rangle\rangle$

$C(X,Y) = \mathcal{E}(-X)\mathcal{E}(-Y)\mathcal{E}(X)\mathcal{E}(Y) - 1 \in \mathbb{Q}_p \langle\langle X, Y \rangle\rangle$.

The Campbell - Hausdorff series $\Phi(X,Y) = (\mathcal{I} \circ P)(X,Y)$,

the commutator Campbell - Hausdorff series $\Psi(X,Y) = (\mathcal{I} \circ C)(X,Y)$.

Proposition 11.5: Let $x, y \in B_0$. Then both Φ and Ψ can be evaluated at (x,y) and

$\Phi(x,y) = \log(\exp x \cdot \exp y)$

$\Psi(x,y) = \log(\exp(-x) \cdot \exp(-y) \cdot \exp x \cdot \exp y)$

Remark: $\exp \Phi(x,y) = \exp x \cdot \exp y$, by (11.4).

The interesting feature of the CHF is that it can be expressed as an infinite sum of Lie elements. $\mathbb{Q}_p \langle\langle X, Y \rangle\rangle$ is an associative algebra, so has a natural Lie bracket: $(u_1, u_2) = u_1 u_2 - u_2 u_1$.

Notation: Use left-normed convention: $(u_1, u_2, \ldots, u_r) = ((u_1, \ldots, u_{r-1}), u_r)$, and for a vector $\underset{\sim}{e} = (e_1, \ldots, e_n)$, $e_i \in \mathbb{N}$, write $(X,Y)_{\underset{\sim}{e}} = (X, \underbrace{Y, \ldots, Y}_{e_1}, \underbrace{X, \ldots, X}_{e_2}, \ldots)$, and write $\langle \underset{\sim}{e} \rangle = e_1 + \cdots + e_n$.

Theorem 11.6 = Campbell - Hausdorff Formula.

Let $\varphi(X,Y) = \sum_{n\in\mathbb{N}} u_n(X,Y)$, u_n a sum of terms of degree n.
Then $u_0(X,Y) = 0$, $u_1(X,Y) = X+Y$, $u_2(X,Y) = \frac{1}{2}(XY-YX) = \frac{1}{2}(X,Y)$, and for each $n\geq 3$, $u_n(X,Y) = \sum_{\underline{e}:=n-1} q_{\underline{e}}(X,Y)_{\underline{e}}$, where $q_{\underline{e}} \in \mathbb{Q}$ and satisfies $p^{n-1} q_{\underline{e}} \in p\mathbb{Z}_p$ (p odd).
Moreover, $\lim_{\langle \underline{e}\rangle \to \infty} |p^{\langle \underline{e}\rangle} \cdot q_{\underline{e}}|_p = 0$.

This result allows us to define an operation on a powerful Lie algebra - later. Recall:

Definition: A Lie algebra L over $\mathbb{Z}_p$ is called powerful if $L \cong \mathbb{Z}_p^d$ and $(L,L) \subseteq \begin{cases} pL & (p\neq 2) \\ 4L & (p=2). \end{cases}$

Corollary 11.7: L a powerful Lie algebra, $x,y\in L$, $n\in\mathbb{N}$, and define u_n as in (11.6), $\in \mathbb{Q}_p L$.
Then (i) $u_n(x,y) \in L \ \forall n\in\mathbb{N}$
(ii) the series $\varphi(x,y) = \sum_{n\in\mathbb{N}} u_n(x,y)$ converges in L.
(iii) $\varphi(x,y) - (x+y) \in pL$ (p odd).

Proof: (i) p odd. Since L powerful, $(x,y)_{\underline{e}} \in p^{n-1}L$. And, $p^{n-1} q_{\underline{e}} \in \mathbb{Z}_p$ (11.6) $\Rightarrow p^{n-1} q_{\underline{e}} (x,y)_{\underline{e}} \in p^{n-1}L$
$\therefore q_{\underline{e}}(x,y)_{\underline{e}} \in L \Rightarrow$ (i).
(ii) We think of L as an additive pro-p group and show that the partial sums form a Cauchy sequence. Let $N\in\mathbb{N}$, Then for sufficiently large n, $p^{n-1} q_{\underline{e}} \in p^N \mathbb{Z}_p$.
As before, $\Rightarrow p^{n-1} q_{\underline{e}} (x,y)_{\underline{e}} \in p^{N+(n-1)}L \Rightarrow u_n(x,y) \in p^N L \ \forall$ sufficiently large.
(iii) Note the above argument shows $u_n(x,y) \in p^2 L$ for $n\geq 3$, since $p^{n-1} q_{\underline{e}} \in p\mathbb{Z}_p$.
Also $\frac{1}{2} \in \mathbb{Z}_p$ (for p odd). So (iii) follows since pL closed.

§ The Lie Algebras of Uniform G.

Let G be uniform. We have defined a norm on the group algebra $A = \mathbb{Q}_p[G]$, so that A is a $\mathbb{Q}_p$-algebra. We then took $\hat{A}$ to be the completion of A and defined $\hat{A}_0 = \{x\in\hat{A} : \|x\| \leq p^{-1}\}$, p odd. The topology on G was induced from the topology on $\hat{A}$, and $G-1 \subseteq \hat{A}_0$.
We have defined a mapping which takes: $\log : 1+\hat{A}_0 \to \hat{A}_0$.
Let $\Lambda = \log G \subseteq \hat{A}_0$. $\hat{A}_0$ is an associative algebra and so has a natural Lie algebra structure: $(x,y) = xy-yx$. We have also defined an intrinsic Lie algebra structure on G (ch.9). Call these operations $(,)_G$, $+_G$. The following lemma links these two structures.

Lemma 11.8: $g,h\in G$, uniform, $\lambda\in\mathbb{Z}_p$. Then
(i) $\log g + \log h = \log(g +_G h)$.
(ii) $\lambda \log g = \log g^\lambda$.
(iii) $(\log g, \log h)_G = \log(g,h)_G$.

Proof: Let $\gamma = \log g$, $\eta = \log h$
(i) We use the CHF, $\varphi(X,Y) = X+Y+\sum_{n\geq 2} u_n(X,Y)$. By (11.4), $\log g^{p^i} = p^i\gamma$, $\log h^{p^i} = p^i\eta$.
(11.5) $\Rightarrow \log(g^{p^i}h^{p^i}) = \log(\exp(\log g^{p^i}).\exp(\log h^{p^i})) = \varphi(\log g^{p^i}, \log h^{p^i}) = \varphi(p^i\gamma, p^i\eta)$
$= p^i\gamma + p^i\eta + \sum_{n\geq 2} u_n(p^i\gamma, p^i\eta) = p^i(\gamma+\eta) + \sum_{n\geq 2} p^{ni} u_n(\gamma,\eta)$.
Thus $\log(g^{p^i}h^{p^i})^{p^{-i}} = p^{-i}\log(g^{p^i}h^{p^i}) = \gamma+\eta + p^i \sum_{n\geq 2} p^{(n-2)i} u_n(\gamma,\eta)$.(*)
Now, $\log$ cts $\Rightarrow \lim_{i\to\infty} \log(g^{p^i}\times h^{p^i})^{p^{-i}} = \log \lim_{i\to\infty} (g^{p^i}h^{p^i})^{p^{-i}} = \log(g +_G h)$ - using same topologies.
Now, $\sum u_n$ converges, so $\sum_{n\geq 2} p^{(n-2)i} u_n(\gamma,\eta)$ bounded $\Rightarrow \lim_{i\to\infty} p^i(\ldots) = 0$. So limit of (*) $\Rightarrow \log g + \log h = \log(g+_G h)$

(ii) $\lambda \in \mathbb{Z}_p$, $\lambda = \lim_{i\to\infty} a_i$, $a_i \in \mathbb{N}$. Since $\|\cdot\|$ on $\widehat{\mathbb{Q}_p[G]}$ induces the usual norm on G, we have $g^\lambda = \lim g^{a_i} \in G \subseteq \hat{A}$. Log continuous, so (11.4)(ii) $\Rightarrow \lambda \log g = \lim_{i\to\infty} a_i \log g$
$= \lim_{i\to\infty} \log g^{a_i} = \log \lim_{i\to\infty} g^{a_i} = \log g^\lambda$.

(iii) Commutator CHF: $\Psi(X,Y) = XY - YX + \sum_{n\geq 3} v_n(X,Y)$.
$\log [g^{p^i}, h^{p^i}]^{p^{-2i}} = p^{-2i} \log [\exp(\log g^{p^i}), \exp(\log h^{p^i})] = p^{-2i} \log [g^{p^i}, h^{p^i}]$
$= \gamma\eta - \eta\gamma + p^i \sum_{n\geq 3} p^{(n-3)i} v_n(\gamma, \eta)$
Continuity of log: $\lim_{i\to\infty} \log [g^{p^i}, h^{p^i}]^{p^{-2i}} = \log \lim_{i\to\infty} [g^{p^i}, h^{p^i}]^{p^{-2i}} = \log (g,h)_G$.
Also, $\lim_{i\to\infty} p^i \sum p^{(n-3)i} v_n(\gamma,\eta) = 0 \Rightarrow \log (g,h)_G = \gamma\eta - \eta\gamma = (\log g, \log h]$

Recall, $\Lambda = \log G$.

Theorem 11.9: $(\Lambda, +, (,))$ is a $\mathbb{Z}_p$-Lie-subalgebra of the Lie algebra $(\hat{A}, +, (,))$, and it's a free $\mathbb{Z}_p$-module, of rank d.

Proof: We need that $(\Lambda, +, (,))$ is closed under these operations. This follows from the previous result since G is closed under $+_G$, $(,)_G$. For the last part, recall (9.13) - $(G, +_G)$ is a free $\mathbb{Z}_p$-module of rank d.

Arguing in the reverse direction - recall (11.4).

Corollary 11.10: $(G, +_G, (,)_G)$ is a Lie algebra over $\mathbb{Z}_p$ and $\log : (G, +_G, (,)_G] \to (\Lambda, +, (,))$ is a $\mathbb{Z}_p$-Lie algebra isomorphism.

Remark: So bilinearity and Jacobi identity for $(,)_G$ hold since they hold in $(\Lambda, +, (,))$.

12. Linearity of Uniform Pro-p Groups.

We prove this by going via the Lie algebra. We use the following classic result.

Ado's Theorem: L, a finite dimensional Lie algebra over a field k of characteristic 0. Then L admits a faithful finite dimensional linear representation $\varphi : L \to M_n(k)$.

Proof: See, eg, Jacobson, chapter VI

We have $\Lambda = \log G$, G uniform - a $\mathbb{Z}_p$ Lie algebra.

Definition: Let $\mathbb{Q}_p\Lambda$ be the $\mathbb{Q}_p$-vector subspace of $\hat{A} = \widehat{\mathbb{Q}_p[G]}$ spanned by Λ. So $\mathbb{Q}_p\Lambda$ is a finite dimensional Lie algebra over $\mathbb{Q}_p$.

So Ado's Theorem $\Rightarrow \varphi : \mathbb{Q}_p\Lambda \to M_n(\mathbb{Q}_p) = \mathcal{B}$, a normed $\mathbb{Q}_p$-algebra, $\|(a_{ij})\| = \max\{|a_{ij}|_p\}$.
Let $B_0 = M_n(p\mathbb{Z}_p) = \{x \in \mathcal{B} : \|x\| \leq p^{-1}\}$, ($p$ odd), $B_0 = M_n(4\mathbb{Z}_2)$, ($p=2$).
So exp is defined on B_0: $\exp B_0 \subseteq 1 + B_0 \subseteq GL_n(\mathbb{Z}_p)$

Definition: Let $\Lambda_0 = \varphi^{-1}(\varphi(\Lambda) \cap B_0) \leq \Lambda = \log G$. So $\exp \Lambda_0 \leq G$.

Lemma 12.1: $\exists\ m \geq 1$ s.t. $G_m \leq \exp \Lambda_0$

Proof: Λ is f.g. as a $\mathbb{Z}_p$-module. So $\varphi\Lambda = \langle \varphi(a_1), .., \varphi(a_d) \rangle$, say.
$\exists\ i \in \mathbb{N}$ s.t. $p^i \varphi(a_j) \in M_n(\mathbb{Z}_p)\ \forall j$. Ie, $p^i \varphi(\Lambda) \leq M_n(\mathbb{Z}_p)$.
Let $m = i+2$ (p odd). (9.10) $\Rightarrow G_m = p^{m-1}(G, +_G)$, so $G_m = p^{i+1}(G, +_G)$.
(11.10) $\Rightarrow \log(G_m) \leq p^{i+1}\Lambda$. So, $\varphi(\log G_m) \leq \varphi(p^{i+1}\Lambda) \leq p M_n(\mathbb{Z}_p) = B_0$.
Clearly $\log(G_m) \leq \Lambda$. So, $\varphi(\log G_m) \cap B_0 = \varphi(\log G_m) \Rightarrow \log G_m = \varphi^{-1}(\varphi(\log G_m)) \subseteq \Lambda_0$.
Ie, $G_m \leq \exp \Lambda_0$.

Definition: Let $\Psi = \exp \cdot \varphi \cdot \log : G_m \to M_n(\mathbb{Q}_p)$, where $m \in \mathbb{N}$ s.t. $G_m \leq \exp \Lambda_0$.

So $\Psi(G_m) = \exp \cdot \varphi \cdot \log(G_m) \leq \exp \cdot \varphi(\Lambda_0) \leq \exp(B_0) \leq GL_n(\mathbb{Z}_p)$.

Proposition 12.2: This map $G_m \to GL_n(\mathbb{Z}_p)$ is a faithful linear representation of G_m.

Proof: Ψ is clearly injective. Need to show Ψ is a group homomorphism, ie $\Psi(gh) = \Psi(g)\Psi(h)$.
$G_m \leq \exp \Lambda_0$, if $g, h \in G_m$, let $g = \exp x$, $h = \exp y$, some $x, y \in \Lambda_0$.
Recall CHF: $F(x,y) = \sum_{n \in \mathbb{N}} u_n(x,y)$. So $\log(\exp x \cdot \exp y) = F(x,y) = \sum u_n(x,y)$.
The u_n are lie elements, so $u_n(x,y) \in \mathbb{Q}_p\Lambda$, $\Lambda = \log G$. So, $\varphi(u_n(x,y))$ is defined.
And since φ is a lie algebra homomorphism, $\varphi(u_n(x,y)) = u_n(\varphi(x), \varphi(y))$.
Also, $\varphi: \mathbb{Q}_p\Lambda \to M_n(\mathbb{Q}_p)$ is continuous (see exercise sheet 3).
So $\varphi(\log(g|h)) = \varphi(\sum u_n(x,y)) = \sum \varphi(u_n(x,y)) = \sum u_n(\varphi(x), \varphi(y))$.
Now $\varphi(x), \varphi(y) \in B_0$, so applying CHF to $\mathbb{Q}_p$-algebra $B = M_n(\mathbb{Q}_p)$ gives
$\sum u_n(\varphi(x), \varphi(y)) = \log(\exp \varphi(x) \cdot \exp \varphi(y)) = \log(\exp \varphi(\log g) \cdot \exp \varphi(\log h)) = \log(\Psi(g), \Psi(h))$
$\Rightarrow \Psi(g)\Psi(h) = \Psi(gh)$, as required.

Recall, pro-p groups of finite rank are virtually uniform.

Theorem 12.3: Pro-p groups of finite rank are linear over $\mathbb{Z}_p$.

Remark: Also, p-adic analytic pro-p groups have finite rank so are linear

13. Powerful Lie algebras

Recall, Lie algebra L is powerful if $L \cong \mathbb{Z}_p^d$ and $(L,L) \leq \begin{cases} pL, & p \text{ odd} \\ 4L & p = 2. \end{cases}$
In (11.7), we showed that the CHF defines a binary operation on powerful L, by $x * y = F(x,y)$.

Theorem 13.1: L a powerful lie algebra. Then $*$ makes L into a uniform pro-p group.
If $\{a_1, .., a_d\}$ is a basis for L over $\mathbb{Z}_p$, then $\{a_1, .., a_d\}$ generate $(L, *)$ topologically and $\dim(L, *) = d$.

Proof: Recall, $F(X,Y) = X+Y+\sum u_n(X,Y)$. So $x*0 = x = 0*x$, $x*(-x) = 0$.
Associativity - technical, but true. Thus $(L,*)$ is a group.
If $(x,y) = 0$, then $u_n(x,y) = 0$, so $x*y = x+y$.
So (using multiplicative notation for $*$), $x^m = mx$, $m \in \mathbb{N}$. But $x^{-1} = -x$, so $x^m = mx$ $\forall m \in \mathbb{Z}$.
So $\{x^{p^t} : x \in L\} = p^tL$, a powerful Lie algebra, so $(p^tL, *) \underset{(\text{sbgp})}{\leq} (L,*)$.
So $\{x^{p^t} : x \in L\} = \langle x^{p^t} : x \in L\rangle = L^{p^t}$, which is closed since p^tL is.
Note L^{p^t} gives a ppower series - normal subgroups.
Now, to show the multiplicative cosets of p^tL in L are the same as the additive cosets. Suppose $x - y \in p^tL$, so $x - y = p^t z$, some $z \in L$. Now, $\langle e\rangle \geq 1$, so
$(x, -y)_e = (x, x-y, \dots) = p^t(x, z, \dots) \in p^{t+\langle e\rangle}L$.
In the CHF, $u_n(x,y) = \sum q_{\underline{e}}(x,y)\underline{e}$, where $p^{\langle \underline{e}\rangle} q_{\underline{e}} \in p\mathbb{Z}_p$ and $|p^{\langle \underline{e}\rangle} q_{\underline{e}}| \to 0$ as $\langle \underline{e}\rangle \to \infty$.
$\Rightarrow u_n(x,-y) \in p^tL$, each $n \geq 2$.
$\Rightarrow xy^{-1} = x*(-y) = x + (-y) + \sum u_n(x,-y) \in p^tL$.
Similarly, if $xy^{-1} = v \in p^tL \Rightarrow x - y = v*y - y \in p^tL$.
Therefore, for $t \geq 1$, $|(L,*) : (L^{p^t}, *)| = |L : p^tL| = p^{td}$.
The additive cosets, $x + p^tL$, form a base for the open sets in the p-adic topology on L, and $x + p^tL = xL^{p^t}$. So we have a base for the nbhds of 1 of $(L,*)$ given by normal subgroups of p-power index. Compactness, etc - inherited. $\Rightarrow (L,*)$ is a pro-p group.
Now to show $(L,*)$ powerful.
(11.7) (iii) $\Rightarrow \varphi(x,y) - (x+y) \in pL$. So $x*y - (x+y) \in pL$, and $y*x - (y+x) \in pL$.
But $x + y = y + x \Rightarrow (x*y)L^p = (y*x)L^p$. Ie $(L,*)/(L^p,*)$ abelian $\Rightarrow (L,*)$ powerful.
Now, $|L : L^{p^t}| = p^{td} \Rightarrow (L,*)$ uniform.
Finally, $(x*y) - (x+y) \in pL \Rightarrow \mathrm{id} : L/pL \to L/L^p$ is an isomorphism between additive and multiplicative structures. So $(L,*) = \langle a_1, \dots, a_d\rangle L^p$, but $L^p = \Phi(L)$, Frattini subgroup.

So, given a powerful Lie algebra, we can construct a uniform pro-p group. But we have already shown (ch.9) that given a uniform pro-p group, we can construct an 'intrinsic' $\mathbb{Z}_p$ Lie algebra $L_G = (G, +_G, (,)_G)$.
Recall $(x,y)_G = \lim_{n\to\infty} [x^{p^n}, y^{p^n}]^{p^{-2n}}$, $[x^{p^n}, y^{p^n}] \in [G^{p^n}, G^{p^n}] \leq G^{p^{2n+1}}$. So L_G powerful.

Theorem 13.2: The maps $G \to L_G$ and $L \to (L,*)$ are mutually inverse isomorphisms between the category of uniform pro-p groups and the category of power Lie algebras over $\mathbb{Z}_p$.

Remarks: So, L_G captures all information about G.

Proof of 13.2: Note that since we are talking about categories, we also have to say what happens to our 'morphisms'; we map each morphism to itself as a map of the underlying sets. So, let G, H be uniform pro-p groups, and $f : G \to H$ a group homomorphism.
Then $f : L_G \to L_H$ is a Lie algebra homomorphism. This follows from the definitions of $+_G, +_H, (,)_G, (,)_H$ and that f is continuous (by 5.10), so respects limits.
Conversely, if L, M are powerful Lie algebras, and $f : L \to M$ a Lie algebra homomorphism, Then $f : (L,*) \to (M,*)$ is a group homomorphism. Since f is s.t. $f(u_n(x,y)) = u_n(f(x), f(y))$, and f is continuous $\Rightarrow f(x*y) = f(x)*f(y)$.

We must show:

(a) L a powerful Lie algebra $\Rightarrow L_{(L,*)} = L$

(b) G a uniform pro-p group $\Rightarrow (L_G, *) = G$.

Recall, topology is preserved as we move from $L \to (L,*)$ and $G \to L_G$.

Also, recall that for $m \in \mathbb{N}$, $x \in L$, $\overbrace{x * \cdots * x}^{m \text{ } x^m} x = mx$, and for $x \in G$, $\overbrace{x +_G \cdots +_G x}^{m \text{ } mx} = x^m$.

Ie, x^m is the same in $(L_G, *)$ as it in G, and by continuity, the operation of $\mathbb{Z}_p$ on $L_{(L,*)}$ is the same as that on L.

To prove (a), we need for $a, b \in L$:

$(*)$ $\lim_{n\to\infty} p^{-n}((p^n a) * (p^n b)) = a + b$.

$(**)$ $\lim_{n\to\infty} p^{-2n} \left| (-((p^n b) * (p^n a)) * ((p^n a) * (p^n b)) \right| = (a,b)$

Now, $p^{-n}((p^n a) * (p^n b)) = p^{-n}\left(p^n a + p^n b + \sum_{m\geq 2} p^{mn} u_m(a,b)\right)$

$= a + b + p^{-n} c_n$, where $c_n = \sum_{m\geq 2} p^{(m-1)n} u_m(a,b) \to 0$ as $n \to \infty$.

Similarly, $-((p^n b) * (p^n a)) = -p^n b - p^n a - \frac{p^{2n}}{2}(b,a) - p^{3n} r^n$, $r^n \in L$.

and $(p^n a) * (p^n b) = p^n a + p^n b + \frac{p^{2n}}{2}(a,b) + p^{3n} s^n$, $s^n \in L$.

$\Rightarrow p^{2n}(\text{LHS of } (**)) = p^{2n}(a,b) + p^{3n} t_n$, $t_n \in L$.

So, LHS of $(**) = (a,b) + p^n t_n \to (a,b)$ as $n \to \infty$.

To prove (b), we need $x * y = xy$ for $x, y \in G$.

Recall, $\log: G \to \Lambda = \log G \leq \hat{A}_0$, $\hat{A} = \widehat{\mathbb{Q}_p[G]}$.

Put $u = \log x$, $v = \log y$. $\log$ is continuous, so

$\log(x * y) = \log \Phi(x,y) = \Phi(\log x, \log y) = \Phi(u,v) = \log(\exp u \cdot \exp v) = \log(xy)$.

Ie, $x * y = xy$.