Pf: For each n, $x +_n 1 = x$, $x +_n x^{-1} = 1$, so $x + 1 = x$, $x + x^{-1} = 1$.

For assoc. law: let $x, y, z \in G$, $n \geq 1$. There is $u \in G_{n+1}$ such that $x + y = (x +_n y) u$ so

$$(x+y) + z \equiv (x +_n y) + z \pmod{G_{n+1}}$$
$$\equiv (x +_n y) +_n z$$

Similarly $x + (y + z) \equiv x +_n (y +_n z) \pmod{G_{n+1}}$.

and $+_n$ is assoc.; so assoc. follows.

Similarly, for commut.

Lemma 4.13 (i) If $xy = yx$, then $x + y = xy$

(ii) For $m \in \mathbb{Z}$ $\quad mx = x^m$

(iii) For $n \geq 1$, $\quad p^{n-1} G = G_n$.

(iv) For $x, y \in G_n$ we have $x + y \equiv xy \pmod{G_{n+1}}$.

Pf: (i) by def. of $+$

(ii) for $m \geq 1$, this follows from (i)

for $m \leq -1$, this follows from $-x = x^{-1}$ and (i)

(iii) follows from 2.12

(iv) Recall that $G_n / G_{n+1} \xrightarrow{\simeq} G_{2n} / G_{2n+1}$, $x \longmapsto x^p$.

Therefore for $x, y \in G_n$ we have

$$(xy)^{p^n} \equiv x^{p^n} y^{p^n} \pmod{G_{2n+1}}$$

Extracting p^nth roots and using 4.10 we have

$$xy \equiv x +_n y \pmod{G_{n+1}} \equiv x + y \pmod{G_{n+1}}$$

and the $+$ is commut. by Remark 4.12.

Cor 4.15 For $n \in \mathbb{N}$, G_n is an add. subgp of G. The add. and mult. cosets of G_n in G coincide. Then id: $(G_n/G_{n+1}, +) \to (G_n/G_{n+1}, \cdot)$ is an isom.

Pf: By 4.13 (iii) $G_n = p^{n-1}G$ is an add. subgp of $(G,+)$. For $a \in G$, $u \in G_n$ we have

$$a+u = a+1\cdot u \equiv a+1 = a \pmod{G_n} \text{ by Rem 4.12}$$

So $a+u \in aG_n$, i.e. $a+G_n \subseteq aG_n$.

Since $au - a = au + (-a) \equiv a(-a) = 0 \pmod{G_n}$

we have $au - a \in G_n$, i.e. $au \in aG_n$,

so $aG_n \subseteq a+G_n$.

By 4.13 (iv), $\mathrm{id}|_{G_n}$ is an isom.

Prop 4.16 With the original top. of G, $(G,+)$ is a unif. powerful pro-p gp of dim $d = d(G)$ and any set of top. generat. for $(G,\cdot)$ gen. $(G,+)$.

Pf: G is cp Hausd, $x \mapsto -x = x^{-1}$ is cont. and $(x,y) \mapsto x+y$ is cont. by Rem. 4.12, so $(G,+)$ is a top. gp wrt. orig. top. $\{G_n\}$ is a nbhd basis for $0=1$ in $(G,\cdot)$ and in $(G,+)$ and since $|G:G_n|$ are p^{th}-powers, $(G,+)$ is pro-p. Since $(G,+)$ is ab., its autom. powerful and $p^{n-1}G = G_n = pG^{p^{n-1}}$

Its unif. powerful because $(G,\cdot)$ is.

If $\langle \overline{X} \rangle = (G,\cdot)$, then $G/G_2 = \langle X \rangle G_2/G_2$ as mult. gp, but by 4.13 (iv) $(G/G_2,\cdot) \cong (G/G_2,+)$, so consider. the add. Frattini, $\langle X \rangle = (G,+)$.

We want to make $(G,+)$ into $\mathbb{Z}_p$-module:

Lemma 4.16 Let G be pro-p, $g \in G$, $(a_i),(b_i) \subseteq \mathbb{Z}_p$ s.th $\varprojlim a_i = \varprojlim b_i \in \mathbb{Z}_p$. Then $(g^{a_i}),(g^{b_i})$ converge and $\lim_{i\to\infty} g^{a_i} = \lim_{i\to\infty} g^{b_i}$.

Pf: Let $N \trianglelefteq_o G$, $|G/N| = p^i$ some i; for suff. large $j,k \in \mathbb{N}$, have $a_j \equiv a_k \pmod{p^i}$ and then $g^{a_j} \equiv g^{a_k} \pmod N$. So (g^{a_i}) conv., $g_1 := \varprojlim g^{a_i}$, $g_2 := \lim g^{b_i}$. For suff. large k we also have $b_k \equiv a_k \bmod p^i$, $g^{b_k} \equiv g_2$, $g^{a_k} \equiv g_1 \pmod N$.

Thus $g_1 g_2^{-1} \equiv g^{a_k - b_k} \equiv 1 \bmod N$.

Since N was arbitr., $g_1 = g_2$.

Def 4.17 Let G be pro-p, $g \in G$, $\lambda \in \mathbb{Z}_p$. Then put

$$g^\lambda = \lim_{n\to\infty} g^{a_n} \quad \text{where } \lim a_n = \lambda.$$

This is well-def. by 4.16.

Prop 4.18 Let G be pro-p, $g,h \in G$, $\lambda,\mu \in \mathbb{Z}_p$.

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

(ii) If $gh = hg$, then $(gh)^\lambda = g^\lambda h^\lambda$

(iii) $\varphi_g : \mathbb{Z}_p \to G$, $\lambda \mapsto g^\lambda$ is contin and $\operatorname{im}\varphi_g = g^{\mathbb{Z}_p} = \overline{\langle g\rangle}$

Pf (i) and (ii) hold mod N for $N \trianglelefteq_o G$, so they hold in G. By (i) φ_g is gp homom, which is contin. because $\mathbb{Z}_p$ is fin. gen. (by Serre's result). So $\operatorname{im}\varphi_g$ is cp, hence closed. Now $g^{\mathbb{Z}_p} \supseteq \langle g\rangle$ and each $h \in g^{\mathbb{Z}_p}$ is limit of seq. in $\langle g\rangle$, so $g^{\mathbb{Z}_p} \subseteq \overline{\langle g\rangle}$, hence "$=$".

Thm 4.21 G powerf. fin. gen pro-p.
Then G is unif. powerful iff G is tors. free

Pf: Let G be fin. gen powerful pro-p, $G_i = P_i(G)$.

"$\Rightarrow$" Suppose G not tors. free. Then there is $x \in G$ of ord. p.
Say $x \in G_i \setminus G_{i+1}$. Then $1 \neq xG_{i+1} \in G_i/G_{i+1}$ and
$1 = x^p G_{i+2} \in G_i/G_{i+2}$, so f_i not isom., so G not uniform.

"$\Leftarrow$" Suppose G not unif. Then there is some i s.th.
$f_i : G_i/G_{i+1} \to G_{i+1}/G_{i+2}$ is epi, not isom.
Thus there ex $x \in G_i \setminus G_{i+1}$ s.th. $x^p \in G_{i+2}$.
Put $x_2 = x$ and suppose for some $n \geq 2$ we have
$x_2, \dots x_n$ s.th. $x_j^p \in G_{i+j}$, $x_j \equiv x_{j-1} \pmod{G_{i+j-2}}$
for $2 \leq j \leq n$.
There ex $z \in G_{i+n-1}$ s.th. $z^p = x_n^p$. Put $x_{n+1} = z^{-1}x_n$.
Then $x_{n+1} \equiv x_n \pmod{G_{i+n-1}}$ and $x_{n+1}^p \in G_{i+n+1}$.
For $p \neq 2$ $x_{n+1}^p = (z^{-1}x_n)^p \equiv z^{-p}x_n^p [x_n, z^{-1}]^{p(p-1)/2} \equiv 1 \pmod{G_{i+n+1}}$
since $[G_{i+n-1}, G, G][G_{i+n-1}, G]^p \leq G_{i+n+1}$
For $p = 2$ $x_{n+1}^p = z^{-2}[z^{-1}, x_n^{-1}]x_n^2 \equiv z^{-2}x_n^2 = 1 \pmod{G_{i+n+1}}$
since $[G_{i+n-1}, G] \leq G_{i+n-1}^4 = G_{i+n+1}$.

Thus $x_2, x_3, \dots, x_n, \dots$ converges to some $x_\infty \in G$
Then $x_\infty \equiv x \not\equiv 1 \pmod{G_{i+1}}$ and $x_\infty^p \equiv x_n^p \equiv 1 \pmod{G_{n+i+1}}$
So $x_\infty^p = 1$ and G is not tors. free