Profinite Groups, Exercise Sheet 3 — Lent 2021

*[Key questions are marked with an obelus †. Expansion questions are marked with a star *.]*

1. Properties of finite p-groups. Let P be a non-trivial finite group of order a power of the prime p.

†(i) By considering the action of P on itself by conjugation, prove that P has non-trivial centre.

†(ii) Prove that P admits a surjective map to $\mathbb{F}_p$.

(iii) Prove that P has a *chief series*: a sequence of normal subgroups $P_i \lhd P$,

$$\{1\} = P_0 \subseteq P_1 \subseteq P_2 \subseteq \cdots \subseteq P_N = P$$

such that every quotient group P_k/P_{k+1} has order p.

2. (i) Prove by induction that $\gamma_n(G)$ is a *fully characteristic* subgroup of G in the sense that, for any group homomorphism $f\colon G \to H$, we have $f(\gamma_n(G)) \subseteq \gamma_n(H)$. Deduce that any subgroup of a nilpotent group is nilpotent.

(ii) Prove that any quotient of a nilpotent group is nilpotent.

(iii) Let A be an abelian central subgroup of G, and assume that G/A is nilpotent of class c. Show that G is nilpotent of class at most $c+1$.

(iv) Deduce that a finite p-group is nilpotent. Show that the lower central p-series of a finite p-group terminates, i.e. $\gamma_n^{(p)}(G) = 1$ for some p.

(v) Find an example to show that the conclusion of part (ii) need not hold if A is only assumed to be an abelian *normal* subgroup.

3. Many of the properties or inductive arguments we have used with p-groups simply rely on the existence of non-trivial centres. As we have seen, nilpotent groups also have non-trivial centre, so one could ask why we are studying p-groups and pro-p groups rather than nilpotent groups and pro-(finite nilpotent) groups. This exercise shows why: finite nilpotent groups are simply products of p-groups.

(i) Let (G_n) be the lower central series of G. Show that G_{n-1}/G_n is central in G/G_n. In particular if G is nilpotent then $Z(G) \neq \{1\}$. Show that if G is nilpotent then the process of repeatedly factoring out centres eventually terminates in the trivial group.

(ii) Let G be a group and let H be a proper subgroup of G. Show that

$$N_G(H) = \{g \in G : g^{-1}Hg = H\}$$

is a subgroup of G which contains H. If G is nilpotent show that $H \neq N_G(H)$.

(iii) Let G be a finite group and let P be a p-Sylow subgroup of G. Show that $N_G(N_G(P)) = N_G(P)$. Deduce that if G is nilpotent then P is a normal subgroup of G.

(iv) Show that a finite nilpotent group is the direct product of its p-Sylow subgroups.

***4. An infinitely generated pro-p group with a finite index subgroup which is not open.** The pro-p group we will consider is a very simple one: the group $(\mathbb{Z}/2)^{\mathbb{N}} = \{(g_n)_{n\in\mathbb{N}} \mid g_n \in \mathbb{Z}/2\}$ with the product topology. This is a pro-2 group which is the inverse limit $\varprojlim(\mathbb{Z}/2)^n$, where the maps $(\mathbb{Z}/2)^{\mathbb{N}} \to (\mathbb{Z}/2)^n$ are the projection maps.

Let $\mathcal{F}$ be a family of subsets of $\mathbb{N}$ with the following properties.

(a) $\emptyset \notin \mathcal{F}$

(b) For $A, B \subseteq \mathbb{N}$, if $A \in \mathcal{F}$ and $B \in \mathcal{F}$ then $A \cap B \in \mathcal{F}$.

(c) For $A, B \subseteq \mathbb{N}$, if $A \in \mathcal{F}$ and $A \subseteq B$ then $B \in \mathcal{F}$

(d) For $A \subseteq \mathbb{N}$, either $A \in \mathcal{F}$ or $(\mathbb{N} \setminus A) \in \mathcal{F}$.

(e) If $\mathbb{N} \setminus A$ is finite then $A \in \mathcal{F}$.

A family $\mathcal{F}$ with properties (a)–(d) is called an *ultrafilter*. The existence of an $\mathcal{F}$ with all the properties (a)–(e) follows from the Axiom of Choice, and may be assumed for this question.

Let H be the set of elements $(g_n)_{n\in\mathbb{N}} \in (\mathbb{Z}/2)^{\mathbb{N}}$ such that $\{n : g_n = 0\} \in \mathcal{F}$.

(i) Prove that H is a subgroup of $(\mathbb{Z}/2)^{\mathbb{N}}$.

(ii) Let $\underline{1}$ be the element of $(\mathbb{Z}/2)^{\mathbb{N}}$ which is the constant sequence $\underline{1} = (1)_{n\in\mathbb{N}}$. Prove that for any $g \in (\mathbb{Z}/2)^{\mathbb{N}}$ either $g \in H$ or $\underline{1} + g \in H$, so that H has index 2 in $(\mathbb{Z}/2)^{\mathbb{N}}$.

(iii) Show that H is dense in $(\mathbb{Z}/2)^{\mathbb{N}}$, and deduce that it is not open.

5. For each pair (n, p^k) below find square roots of n modulo p^k.

(i) $n = 14$ modulo $p^k = 121 = 11^2$

(ii) $n = 44$ modulo $p^k = 343 = 7^2$

(iii) $n = 31$ modulo $p^k = 625 = 5^4$

†6. Find all solutions of $f(x) = x^2 - 2x + 2$ modulo 125.

†7. Let $p \neq 2$. Prove that if $a \in \mathbb{Z}_p$ is not congruent to 0 modulo p then there exist at most two square roots of any $a \in \mathbb{Z}/p^k\mathbb{Z}$ for any k. Show that any $a \in \mathbb{Z}_p$ has at most two square roots in $\mathbb{Z}_p$. Show that 1 has four square roots in $\mathbb{Z}/15\mathbb{Z}$. Show that p^2 has $2p$ distinct roots in $\mathbb{Z}/p^3\mathbb{Z}$.

8. The assumption that an element is a *non-zero* square modulo p in the square roots version of Hensel's Lemma is unnecessarily restrictive. Characterise exactly which elements of $\mathbb{Z}_p$ have square roots (for $p \neq 2$).

9. (Square roots when $p = 2$.)

(a) Show that if $\lambda \in \mathbb{Z}_2$ is a non-zero square then $\lambda = 2^{2r}(1 + 8a)$ for some $r \in \mathbb{Z}$ and $a \in \mathbb{Z}_2$.

(b) Let $\lambda = 1 + 8a$. Show that $x^2 = \lambda$ if and only if $y = (1 + x)/2$ satisfies the equation $y^2 - y - 2a = 0$.

(c) Deduce that $\lambda \in \mathbb{Z}_2 \setminus \{0\}$ is a square number if and only if $\lambda = 2^{2r}(1+8a)$ for some $r \in \mathbb{Z}$ and $a \in \mathbb{Z}_2$.

†10. Invertible elements of $\mathbb{Z}_p$. The ring $\mathbb{Z}$ has only two invertible elements, ± 1. We have seen already that $\mathbb{Z}_p$ has many more. In this exercise we will show the exact structure of the group of invertible elements $\mathbb{Z}_p^\times$. Let $p \neq 2$ be prime.

(i) Let $f(x)$ be a non-zero polynomial of degree $\leq d$ over a field $\mathbb{F}$. Show that $f(x)$ has at most d roots in f.

(ii) By considering solutions of the equation $x^q = 1$ in $\mathbb{F}_p$ for primes $q|(p-1)$, use the classification of abelian groups to deduce that the abelian group $\mathbb{F}_p^\times$ is cyclic.

(iii) Show that there exists $\sigma \in \mathbb{Z}_p^\times$ such that $\sigma^{p-1} = 1$ but $\sigma^n \neq 1$ for $0 < n < p-1$.

(iv) Show that $(1+p)^{(p-1)p^k} \equiv 1 + (p-1)p^{k+1}$ modulo p^{k+2}.

(v) Let $\tau = 1+p \in \mathbb{Z}_p^\times$. Show that the reduction modulo p^n of $\sigma\tau$ has order $(p-1)p^{n-1}$ in the group $\mathbb{Z}/p^n\mathbb{Z}$. Deduce that $\sigma\tau$ generates $\mathbb{Z}/p^n\mathbb{Z}$, and hence that $\sigma\tau$ topologically generates $\mathbb{Z}_p^\times$.

(vi) Show that $\mathbb{Z}_p^\times \cong C_{p-1} \times \mathbb{Z}_p$, where C_{p-1} is a cyclic group of order $p-1$.

*(vii) Show that $\mathbb{Z}_2^\times \cong C_2 \times \mathbb{Z}_2 = \langle -1 \rangle \times \langle 1+4 \rangle$.

11. Show, for a 2×2 matrix A over a commutative ring with determinant 1, that

$$A^3 = ((\operatorname{tr} A)^2 - 1)A - (\operatorname{tr} A)I$$

Deduce that the matrix

$$\begin{pmatrix} 82 & 9 \\ 9 & 1 \end{pmatrix} = 1 + 9 \begin{pmatrix} 9 & 1 \\ 1 & 0 \end{pmatrix}$$

has no cube root in $\mathrm{SL}_2(\mathbb{Z})$. Show that the equation

$$83 = x^3 - 3x$$

does have a solution in $\mathbb{Z}_3$.

12. Let $a_1, \ldots, a_{N^2}$ be a generating set of $\mathrm{GL}_N^{(1)}(\mathbb{Z}_p)$. Show that

$$\mathrm{GL}_N^{(1)}(\mathbb{Z}_p) = \overline{\langle a_1 \rangle} \cdot \overline{\langle a_2 \rangle} \cdots \overline{\langle a_{N^2} \rangle}$$

That is, for any $g \in \mathrm{GL}_N^{(1)}(\mathbb{Z}_p)$ there exist $\lambda_1, \ldots, \lambda_{N^2} \in \mathbb{Z}_p$ such that

$$g = a_1^{\lambda_1} \cdots a_{N^2}^{\lambda_{N^2}}.$$