GROUP THEORY 2024 - 25, SOLUTION SHEET 10

Exercise 1. To do yourself. Ask the assistant if something is unclear.

Exercise 2. Let G/H be the set of left co-sets of H in G. Then $|G/H| = p$ and hence there is an induced homomorphism $\varphi : G \to S_p$. Let K denote the kernel of φ and consider the following two lemmas:

Lemma 2.1: The cardinality of G/K is p.

Lemma 2.2: We have an inclusion of subgroups $K \subseteq H$.

Assuming the lemmas, since the index of both K and H in G is p and $K \subseteq H$ we can conclude that $H = K$. The fact that K is a kernel of a homomorphism yields that $H = K$ is a normal subgroup. We leave the proof of Lemma 2.2 to the reader and prove Lemma 2.1.

Proof of Lemma 2.1:
Let q be a prime factor of $|G/K|$, then since p is assumed to be the minimum prime dividing $|G|$ and $|G/K| \mid |G|$, we have that $q \geq p$. By the first isomorphism theorem applied to φ we obtain that G/K is isomorphic to a subgroup of S_p. Therefore $q \mid |G/K| \mid p!$ and hence $q \leq p$. So we obtain $q = p$. So $|G/K| = p^n$ but $|G/K| \mid p!$ also implies that $n = 1$. Hence $|G/K| = p$. □

Exercise 3. (1) By an exercise of a preceding series, a p-group of order n has normal subgroups of order p^k for all $1 \leq k \leq n$, which proves the claim.

(2) Without loss of generality suppose that $p > q$. By the Sylow theorems, the number n_p of Sylow p-subgroups of the group divides q and has residue 1 modulo p. As $p > q$, n_p has to be 1 and by an exercise of series 9 the unique Sylow p-subgroup is be normal.

(3) If $q < p$, then the index of a Sylow p-subgroup P is equal to q, the smallest prime that divides the order of the group. By exercise 2, P is normal in G. Now suppose that $p < q$. It cannot be that case that p has residue 1 modulo q, so the number of Sylow q-subgroups, which we denote by n_q should obey $n_q = 1$ or $n_q = p^2$. If $n_q = 1$, then the unique Sylow q-subgroup is normal and G is not simple, so we assume that $n_q = p^2$. Since a Sylow q-subgroup has order q and two distinct Sylow q-subgroups intersect trivially (since $Q \cap Q'$ is a subgroup of Q, its order must divide the prime q, hence either $Q = Q'$ or $Q \cap Q' = 1$), G has $p^2(q-1)$ elements of order q. Therefore, a Sylow p-subgroup contains all of the remaining p^2 elements of G. In this case, we conclude that the Sylow p-subgroup is unique, so it is normal in G.

(4) Without loss of generality suppose that $p < q < r$. If the number n_s of Sylow s-subgroup is 1 for $s = p, q$ or r, then the (unique) Sylow s-subgroup is normal. So we suppose

now that n_p, n_q and n_r are all strictly bigger than 1. Using Sylow's theorems, we deduce that $n_p \geq q$, $n_q \geq r$ and $n_r \geq pq$. Since for $s = p, q, r$ Sylow s-subgroups are intersect trivially (as in the preceding point), we can count the elements in those Sylow s-subgroups (those elements are of order s) to find that:

$$\begin{aligned}|G| &\geq n_p(p-1) + n_q(q-1) + n_r(r-1) \\ &\geq q(p-1) + r(q-1) + pq(r-1) \\ &= qp - q + rq - r + pqr - pq = pqr + r(q-1) - q \\ &\geq |G| + q(q-2) \\ &> |G|\end{aligned}$$

a contradiction.

Exercise 4. Note that every positive integer less that 60 can be written in one of the following forms:
1. p^n for a prime p and $n \geq 0$.
2. $p^a q^b$ for distinct primes p, q and $a > 0$, $b > 0$.
3. pqr for distinct primes p, q, r.

Let G be a non-abelian group of order n such that $n < 60$. If n is of the form p^n, pqr then G is not simple by exercise 3. If n is of the form $p^a q^b$, then G is solvable by Burnside's Theorem. But then solvability of G implies that $H := [G, G]$ is a normal subgroup of G with $G \neq H$. Since G is not abelian we also have that H is not trivial. Hence G is not simple.

Exercise 5. By the Sylow theorems, the number of Sylow 2-subgroups must be either 1 or 3. In the former case, this subgroup is normal and we are done. In the latter case, we have a group homomorphism $G \to S_3$ given by the action of G on the set of Sylow 2-subgroups. If G is simple, this must be injective, which means that G has at most 6 elements, which contradicts the hypothesis $n \geq 2$.

Exercise 6. (1) Let $\sigma \in \mathrm{Aut}(K)$ such that $\sigma\varphi_1(L)\sigma^{-1} = \varphi_2(L)$. Let $x \in L$ be a generator of the cyclic group L. Then there exists $a \in \mathbb{N}$ such that $\sigma \circ \varphi_1(x) \circ \sigma^{-1} = \varphi_2(x^a) = \varphi_2(x)^a$. Now for every $l \in L$ there exists $b \in \mathbb{N}$ such that $l = x^b$, which implies that

$$\begin{aligned}\sigma \circ \varphi_1(l) \circ \sigma^{-1} &= \sigma \circ \varphi_1(x^b) \circ \sigma^{-1} \\ &= (\sigma \circ \varphi_1(x) \circ \sigma^{-1})^b \\ &= (\varphi_2(x)^a)^b \\ &= \varphi_2(x^b)^a \\ &= \varphi_2(l)^a \qquad (1)\end{aligned}$$

as suggested by the hint. We now define

$$\psi : K \rtimes_{\varphi_1} L \to K \rtimes_{\varphi_2} L$$

by $\psi(k,l) = (\sigma(k), l^a)$. We let the reader verify that ψ is a group homomorphism. To construct an inverse $\phi : K \rtimes_{\varphi_2} L \to K \rtimes_{\varphi_1} L$ of ψ, we just change the role of φ_1 and φ_2 above. By the same argument, there exists an integer b such that

(2) $$\sigma^{-1} \circ \varphi_2(l) \circ \sigma = \varphi_1(l)^b.$$

Hence we know that $\phi : (k,l) \mapsto (\sigma^{-1}(k), l^b)$ is a group homomorphism. Combining the two equations (1) and (2) we obtain that $\varphi_2(l^{ab}) = \varphi_2(l)$ and $\varphi_1(l^{ab}) = \varphi_1(l)$. It is now straightforward to check that ϕ and ψ are inverses of each other.

(2) Let $\varphi_1, \varphi_2 : L = \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z})$ be non trivial group homomorphisms. By the hint we know that $\mathrm{Aut}(\mathbb{Z}/p^2\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$ for some integer m. Since the two homomorphisms are non trivial, their kernel must be trivial and φ_1 and φ_2 are thus injective. It follows that $\varphi_1(L)$ and $\varphi_2(L)$ are subgroups of order p in $\mathbb{Z}/m\mathbb{Z}$. But cyclic groups have *unique* subgroups of each order, hence $\varphi_1(L) = \varphi_2(L)$. In particular they are conjugate, and we conclude by using the first part of the exercise.

(3) Let $\varphi_1, \varphi_2 : L = \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} = K)$ be non trivial group homomorphisms. To identify the codomain, we note that every automorphism $f : K \to K$ is a L-vector space linear automorphism. This is because for $\alpha \in L$ we have that $f(\alpha \cdot (a,b)) = \alpha \cdot f(a,b)$. It follows that L-automorphisms are in bijections with invertible matrices with coefficients in L, and therefore

$$|\mathrm{Aut}(K)| = |GL_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p) = p(p^3-p^2-p-1) = p \cdot r$$

for some even number $r \in \mathbb{N}$. It follows that Sylow p-subgroups are of order p, and hence all subgroups of order p are conjugate (by Sylow's theorem). As in the previous point the groups $\varphi_1(L)$ and $\varphi_2(L)$ are subgroups of $\mathrm{Aut}(K)$ of order p, and hence are conjugate. We conclude by the first point.

Exercise 7. (1) By the classification theorem for finitely generated abelian groups, we know that G is isomorphic to one of the following abelian groups:

$$\mathbb{Z}/p^3\mathbb{Z}, \qquad \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, \qquad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

(2) Let $x \in G$ be an element of order p^2 and K be its generating subgroup: $K = \langle x \rangle \cong \mathbb{Z}/p^2\mathbb{Z}$. Since K has index p in G, we know that K is normal in G by exercise 2 and therefore $G/K \cong \mathbb{Z}/p\mathbb{Z}$. A generator $[\alpha]$ of G/K can be represented by any element $\alpha \in G \backslash K$, which is of order p or p^2 in G. If α has order p there is a split short exact sequence

$$1 \to \mathbb{Z}/p^2\mathbb{Z} \to G \to \mathbb{Z}/p\mathbb{Z} \to 1$$

where $s(1) = \alpha$ is a splitting. If every $\alpha \in G \backslash H$ is of order p^2, Archi will write a contradiction. It follows that G is a semi direct product, which is non trivial since G is not abelian. The uniqueness part of the statement follows from the previous exercise.

(3) By exercise 5 of last week, there exists a subgroup $K \leq G$ of order p^2. Since G has no element of order p^2, we know by exercise 2 of sheet 4 that $L \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. As in the previous point K is normal in G and we have a short exact sequence

$$1 \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G \to \mathbb{Z}/p\mathbb{Z} \to 1.$$

Now if $[\alpha] \in \mathbb{Z}/p\mathbb{Z} = G/K$ is a generator represented by $\alpha \in G$, we know that α has order p in G as there is no element of order p^2. Hence $s : G/K \to G$ defined by $s([\alpha]) = \alpha$

is a splitting. It follows that $G \cong (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$, and this semi direct product is uniquely determined by exercise 6.3 as G is non abelian.

(4) Combining the previous points, we know that any group G of order p^3 is isomorphic to one of the following groups:

$$\mathbb{Z}/p^3\mathbb{Z}, \qquad \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}, \qquad \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z},$$
$$\mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}, \qquad (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$$

where the semi direct products are non-trivial, hence uniquely determined by the last exercise.

(5) We left to the reader the verification that G is a group of order p^3. We note that

$$\begin{pmatrix} p+1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

do not commute. More over the later matrix is of order p^2, which proves the claim by the second point of this exercise.

(6) We left to the reader the verification that G is a non abelian group of order p^3. We note that every $A \in G$ can be written as $A = I_3 + J$ where J is nilpotent ($N^3 = 0$). Then by the binomial coefficient theorem,

$$A^p = I_3 + \binom{p}{1} J + \binom{p}{2} J^2 = I_3$$

which shows that every element has order p. We conclude by the third point of this exercise.