GROUP THEORY 2024 - 25, SOLUTION SHEET 4

Exercise 1. *To always do in every course!*
Review the lecture and understand/fill in the gaps in the proofs.

Exercise 2. Suppose that G is not cyclic.

(1) Let $G \curvearrowright G$ be the action by conjugation, defined by $g \cdot x = gxg^{-1}$. The set $X = G$ is partitioned by its orbits, which are conjugacy classes of elements. Note that $x \in Z(G)$ if and only if its orbit is trivial since $gxg^{-1} = x$ for all $g \in G$, i.e.
$$x \in Z(G) \iff Orb(x) = x.$$
Hence elements of the center defines their own conjugagy classes, and so
$$|G| = |Z(G)| + \sum_{\text{non trivial orbits}} |Orb(x)|.$$
By the orbit stabilizer theorem $|Stab_G(x)| = p^2/|Orb(x)|$ which implies that $|Orb(x)| \in \{p, p^2\}$ for all non trivial orbits. Therefore, taking the above equation mod p we find that $|Z(G)| = 0 \bmod p$, henceforth implying that $Z(G)$ is non trivial, as desired.

(2) By the last point, since the order of a subgroup must divide p^2 and $Z(G)$ is non trivial, $|Z(G)| \in \{p, p^2\}$. If it is p^2 then G is abelian and we are done. So suppose that $|Z(G)|$ $|G/Z(G)| = p$ and so the quotient must be cyclic, generated by any non trivial element. Let $a \in G \backslash Z(G)$, which is such that $aZ(G)$ generates $G/Z(G)$ as explained, and take any two elements $x_1, x_2 \in G$. There must exist $z_1, z_2 \in Z(G)$ such that $x_1 = a^{k_1} z_1$ and $x_2 = a^{k_2} z_2$. Hence we find that
$$x_1 x_2 = a^{k_1} z_1 a^{k_2} z_2 = a^{k_2} z_2 a^{k_1} z_1 = x_2 x_1$$
since all these elements commute with each other. Hence G is abelian.

(3) Let $x \in G$ be non trivial. Since G is not cyclic, it generates a cyclic subgroup $\langle x \rangle \cong \mathbb{Z}/p\mathbb{Z}$ of order p. Pick any $y \in G \backslash \langle x \rangle$, which also generates a cyclic subgroup $\langle y \rangle \cong \mathbb{Z}/p\mathbb{Z}$ of order p such that $\langle x \rangle \cap \langle y \rangle = \{0\}$ since otherwise their intersection (which is a subgroup) would be of order p as well, contradicting the fact that $y \notin \langle x \rangle$. We construct a homomorphism
$$f : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G$$
$$([n], [m]) \mapsto x^n y^m$$
It is clear that this function is well defined since x and y are of order p. Moreover you can easily show that it is a homomorphism using the second point. Lastly it is injective since if $x^n y^m = 0$, then $x^n \in \langle y \rangle$ and so $x^n = 0$ since $\langle x \rangle \cap \langle y \rangle = \{0\}$. This implies that $n = 0 \bmod p$, which in turn implies that $m = 0 \bmod p$ as well. Therefore f is an injective homomorphism between two groups of order p^2, hence is an isomorphism.

Exercise 3. It is straightforward to see that $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$ is trivial, so the only such homomorphism φ must also be the trivial one. Hence, the only semi-direct product is in fact isomorphic to the direct product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. However, we know that this group and $\mathbb{Z}/4\mathbb{Z}$ are not isomorphic, because the latter has an element of order 4, while the first does not.

Exercise 4. *Internal semi-direct product*

(1) Consider the map
$$\alpha : K \rtimes_\varphi L \to G,\ (k,l) \mapsto kl.$$
We show that α is an isomorphism of groups. Note that for all $(k_1,l_1),(k_2,l_2) \in K \rtimes_\varphi L$ we have that:
$$\alpha((k_1,l_1)\cdot(k_2,l_2)) = \alpha(k_1l_1k_2l_1^{-1}, l_1l_2) = k_1l_1k_2l_2 = \alpha((k_1,l_1))\alpha((k_2,l_2)).$$
This shows that α is a group homomorphism. It follows from the assumption $KL = G$ that α is surjective. Now suppose $\alpha((k,l)) = kl = 1$, then $k = l^{-1}$ therefore the assumption $K \cap L = \{1\}$ forces $k = l = 1$. Hence α is also injective and therefore an isomorphism.

(2) Consider the element $g = klk^{-1}l^{-1} \in G$ for some $k \in K$ and $l \in L$. Since L is normal, we have that $klk^{-1} \in L$ and hence $g \in L$. Similarly, normality of K yields that $g \in K$. Since $K \cap L$ is trivial, we obtain that $g = 1$ and hence $kl = lk$. It follows straightaway that φ is the trivial homomorphism.
Note that if $\varphi : L \to Aut(K)$ is the trivial homomorphism then $(k_1,l_1)\cdot(k_2,l_2) = (l_1l_2, k_1k_2)$ for all $(k_1,l_1),(k_2,l_2) \in K \rtimes_\varphi L$. This implies that the set theoretic bijection $K \times L \to K \rtimes_\varphi L$, $(k,l) \mapsto (k,l)$ is also a group homomorphism and hence an isomorphism.

Exercise 5. One checks that $K \rtimes_\psi L \to L$, $(k,l) \mapsto l$ is a group homomorphism with kernel $K \times \{1\}$. Since Kernels of homomorphisms are normal subgroups we have that $K \times \{1\}$ is normal. It is also clear that $(K \times \{1\}) \cap (\{1\} \times L)$ is the identity element of G and that $(K \times \{1\}) \cdot (\{1\} \times L) = G$. Hence $K \rtimes_\psi L$ is the internal semi-direct product of $K \times \{1\}$ with $\{1\} \times L$.

Using the group law on $G = K \rtimes_\psi L$, we have that:
$$(1,l)(k,1)(1,l)^{-1} = (1\cdot\psi_l(k), l)(1,l)^{-1} = (\psi_l(k), l)(1, l^{-1}) = (\psi_l(k)\cdot\psi_l(1), 1) = (\psi_l(k), 1).$$

This identity implies that the set theoretic bijection
$$K \rtimes_\psi L \to (K \times \{1\}) \rtimes_\varphi (\{1\} \times L),\ (k,l) \mapsto ((k,1),(1,l))$$
is a group homomorphism and hence an isomorphism.

Exercise 6. Apply exercise 2.(1) with $K =< (123) > \trianglelefteq S_3$ and $L =< (12) >$ (check that all the conditions are satified!).

Exercise 7. (1) Let us first find $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$: we know that these correspond to choices of elements of order 4 in the codomain, so $|\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})| = 2$ and thus $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. Now, the homomorphisms $\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ correspond to choices of elements of 2-torsion in the codomain, and there are exactly 2 of these: the identity and the zero morphism.

(2) As we have seen, the zero morphism gives us the direct product $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The "identity" morphism from point (1) is explicitely given by

$$\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$$
$$1 \mapsto \cdot 3$$

where $\cdot 3 : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ is the multiplication by 3. Hence, the group structure of $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ is given by $(a, 0) \cdot (c, d) = (a + c, d)$ and $(a, 1) \cdot (c, d) = (a + 3c, 1 + d)$.

(3) The latter, $\mathbb{Z}/4\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, is indeed isomorphic to D_8. See (4).

(4) Recall exercise 2, point (1). Define $K =< \sigma >$, where σ is the rotation of the regular n-gon, and $L =< \tau >$, where τ is the reflection. By the fact that it has index 2, we know that K is normal in D_{2n} (see sheet 3). Moreover, $K \bigcap L = \{id\}$ and $KL = D_{2n}$ (check this!). We infer that $D_{2n} \cong K \rtimes_\varphi L$. Observe that K is cyclic of order n, so $K \cong \mathbb{Z}/n\mathbb{Z}$, while L is of order 2, so $L \cong \mathbb{Z}/2\mathbb{Z}$. By analyzing the way the groups are identified via these isomorphisms, we can see that $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ corresponds to $1 \mapsto \cdot(-1)$, where $\cdot(-1) : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is the multiplication with (-1). We have thus found our desired φ.

Exercise 8. Consider

$$\phi : F^\times \to GL_n(F),\ a \mapsto M_a = \begin{pmatrix} a & 0 & 0 & ... \\ 0 & 1 & 0 & ... \\ 0 & 0 & 1 & ... \\ ... & ... & ... & ... \end{pmatrix}.$$

That is $M_a = \mathrm{Diag}(a, 1, 1, 1....)$. One verifies readily that ϕ is a group homomorphism and that $det \circ \phi = Id_{F^\times}$. Hence the following short exact sequence splits on the right:

$$1 \to SL_n(F) \xrightarrow{i} GL_n(F) \xrightarrow{\det} F^\times \to 1.$$

Using Proposition 10 of lecture 4, this shows that:

$$GL_n(F) \cong SL_n(F) \rtimes_\varphi F^\times.$$

Where $\varphi : F^\times \to Aut(SL_n(F))$ is given by the action :

$$a \cdot M = M_a M M_a^{-1}.$$