Homework 10

Due Friday, April 24th

Recall the definition of the semidirect product.

Definition 1. *Let H, K be groups, and $\varphi : K \to \mathrm{Aut}(H)$ a group homomorphism. Denote the induced action of K on H by:*

$$k \cdot h = \varphi(k)(h).$$

The semidirect product of H and K with respect to φ is the set $H \rtimes K = \{(h, k) : h \in H, k \in K\}$, where multiplication is defined by the rule:

$$(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1k_2).$$

1. Let's make sure that $H \rtimes K$ is a group.

   (a) Show that $(1, 1) \in H \rtimes K$ is the identity. (Remember you have to check both sides).

   Proof. Fix $h \in H$ and $k \in H$. Then we check,

   $$(1, 1)(h, k) = (1(1 \cdot h), 1k) = (h, k).$$

   On the other hand:

   $$(h, k)(1, 1) = (h(k \cdot 1), k1) = (h, k),$$

   where we remark that $k \cdot 1 = 1$ because K acts *by automorphisms* (i.e. $x \mapsto k \cdot x$ is not merely a bijection, but also a homomorphism which in particular sends 1 to 1). □

   (b) Show that $(h, k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1})$. (As above, you have to check both sides).

   Proof. We check both directly:

   $$\begin{aligned}(h, k)(k^{-1} \cdot h^{-1}, k^{-1}) &= (h(k \cdot (k^{-1} \cdot h^{-1})), kk^{-1}) \\ &= (h(kk^{-1} \cdot h^{-1})), 1) \\ &= (h(1 \cdot h^{-1}), 1) \\ &= (hh^{-1}, 1) \\ &= (1, 1).\end{aligned}$$

   For the other hand, we remark that because K acts by automorphisms, we have that for each $\ell \in K$, we have $(\ell \cdot x)(\ell \cdot y) = \ell \cdot (xy)$ (because $x \mapsto \ell \cdot x$ is a homomorphism). In particular

   $$\begin{aligned}(k^{-1} \cdot h^{-1}, k^{-1})(h, k) &= ((k^{-1} \cdot h^{-1})(k^{-1} \cdot h), k^{-1}k) \\ &= (k^{-1} \cdot (h^{-1}h), 1) \\ &= (k^{-1} \cdot 1, 1) \\ &= (1, 1).\end{aligned}$$

   □

   (c) Prove that multiplication is associative.

Proof. We consider $h_1, h_2, h_3 \in H$ and $k_1, k_2, k_3 \in K$. We passing from line 2 to 3 that K acts by automorphism. Then:

$$\begin{aligned}
((h_1, k_1)(h_2, k_2))\,(h_3, k_3) &= (h_1(k_1 \cdot h_2), k_1k_2)(h_3, k_3) \\
&= (h_1(k_1 \cdot h_2)(k_1k_2 \cdot h_3), k_1k_2k_3) \\
&= (h_1(k_1 \cdot (h_2(k_2 \cdot h_3)), k_1k_2k_3) \\
&= (h_1, k_1)(h_2(k_2 \cdot h_3), k_2k_3) \\
&= (h_1, k_1)\,((h_2, k_2)(h_3, k_3))\,.
\end{aligned}$$

□

2. Let $G_1, G_2, \cdots, G_n$ be groups. Show that:

$$Z(G_1 \times G_2 \times \cdots \times G_n) = Z(G_1) \times Z(G_2) \times \cdot \times Z(G_n).$$

Conclude that a product of groups is abelian if and only if the factors are.

Proof. If $x = (x_1, \cdots, x_n) \in Z(G_1) \times \cdots Z(G_n)$, so that each $x_i \in Z(G_i)$, then:

$$\begin{aligned}
xy &= (x_1, \cdots, x_n)(y_1, \cdots, y_n) \\
&= (x_1y_1, \cdots, x_ny_n) \\
&= (y_1x_1, \cdots, y_nx_n) \\
&= (y_1, \cdots, y_n)(x_1, \cdots, x_n) \\
&= yx.
\end{aligned}$$

This shows the right side is a subset of the left one. On the other hand, if $x = (x_1, \cdots, x_n) \in Z(G_1 \times \cdots \times G_n)$. Notice that the projection maps $\pi : G_1 \times \cdots \times G_n \to G_i$ is surjective for each i. In particular, each element of $y_i \in G_i$ is $\pi(y)$ for some y in the product group. Notice that:

$$\pi(x)y_i = \pi(x)\pi(y) = \pi(xy) = \pi(yx) = \pi(y)\pi(x) = y_i\pi(x).$$

Thus $\pi(x) = x_i \in Z(G_i)$. Since each coordinate of x is in the center of its respective group, we have $x \in Z(G_1) \times \cdots \times Z(G_n)$, proving the left side includes in the right one, completing the proof.

Now notice that if every G_i is abeelian, then:

$$Z(G_1 \times \cdots \times G_n) = Z(G_1) \times \cdots \times Z(G_n) = G_1 \times \cdots \times G_n,$$

so that the product group is abelian. Conversely, if the product group is abelian, fix some $g_i \in G_i$, then $(1, \cdots, g_i, \cdots, 1)$ is in the center of the product group (everything is!), so g_i is in the center of G_i. Since g_i was arbitrary, G_i is abelian. □

3. Let's classify some abelian groups! List all *abelian* groups of the following orders, in elementary divisor and invariant factor forms.

   (a) 100

Proof. $100 = 4 \cdot 25 = 2^2 \cdot 5^2$. Then $G = P \times Q$ where P is a group of order 4 and Q of order 25. In each case these are classified by the partitions of 2 (which are $1+1$ and 2), The possibilities for P are therefore $Z_2 \times Z_2$ and Z_4, and the possibilities for Q are $Z_5 \times Z_5$ and Z_{25}. Thus the group (in elementary divisor form) are:

$$\begin{aligned} G_1 &= Z_2 \times Z_2 \times Z_5 \times Z_5 & G_2 &= Z_4 \times Z_5 \times Z_5 \\ G_3 &= Z_2 \times Z_2 \times Z_{25} & G_4 &= Z_4 \times Z_{25}. \end{aligned}$$

Let's put these into invariant factor form following the method described in class.

$$\begin{array}{c|c|c||c|c|c} G_1 & 2 & 5 & G_2 & 2 & 5 \\ \hline & 2 & 5 & & 4 & 5 \\ & 2 & 5 & & 1 & 5 \end{array}$$

$$\begin{array}{c|c|c||c|c|c} G_3 & 2 & 5 & G_4 & 2 & 5 \\ \hline & 2 & 25 & & 4 & 25 \\ & 2 & 1 & & & \end{array}$$

Multiplying horizontally gives:

$$\begin{aligned} G_1 &= Z_{10} \times Z_{10} & G_2 &= Z_{20} \times Z_5 \\ G_3 &= Z_{50} \times Z_2 & G_4 &= Z_{100}. \end{aligned}$$

□

(b) 243

Proof. $243 = 3^5$. So groups are classified by partitions of 5, which are

$$5, 4+1, 3+2, 3+1+1, 2+2+1, 2+1+1+1, 1+1+1+1+1.$$

These correspond to:

$$Z_{243}$$
$$Z_{81} \times Z_3$$
$$Z_{27} \times Z_9$$
$$Z_{27} \times Z_3 \times Z_3$$
$$Z_9 \times Z_9 \times Z_3$$
$$Z_9 \times Z_3 \times Z_3 \times Z_3$$
$$Z_3 \times Z_3 \times Z_3 \times Z_3 \times Z_3.$$

This is already in invariant factor form. □

(c) 9801

Proof. $9801 = 3^4 * 11^2$. So $G = P \times Q$ where $|P| = 81$ and $|Q| = 121$. The options for p are classified by partitions of 4, of which there are 5:

$$4, 3+1, 2+2, 2+1+1, 1+1+1+1,$$

and the options for Q are partitions of 2 (2 and $1+1$). This gives us $5 * 2 = 10$ options:

$$\begin{aligned} G_1 &= Z_{81} \times Z_{11} \times Z_{11} & G_2 &= Z_{81} \times Z_{121} \\ G_2 &= Z_{27} \times Z_3 \times Z_{11} \times Z_{11} & G_4 &= Z_{27} \times Z_3 \times Z_{121} \\ G_5 &= Z_9 \times Z_9 \times Z_{11} \times Z_{11} & G_6 &= Z_9 \times Z_9 \times Z_{121} \\ G_7 &= Z_9 \times Z_3 \times Z_3 \times Z_{11} \times Z_{11} & G_8 &= Z_9 \times Z_3 \times Z_3 \times Z_{121} \\ G_9 &= Z_3 \times Z_3 \times Z_3 \times Z_3 \times Z_{11} \times Z_{11} & G_{10} &= Z_3 \times Z_3 \times Z_3 \times Z_3 \times Z_{121}. \end{aligned}$$

We put these into invariant factor form following the method described in class.

G_1	3	11	G_2	3	11
	81	11		81	121
	1	11			

G_3	3	11	G_4	3	11
	27	11		27	121
	3	11		3	1

G_5	3	11	G_6	3	11
	9	11		9	121
	9	11		9	1

G_7	3	11	G_8	3	11
	9	11		9	121
	3	11		3	1
	3	1		3	1

G_7	3	11	G_8	3	11
	3	11		3	121
	3	11		3	1
	3	1		3	1
	3	1		3	1

Multiplying horizontally gives:

$$\begin{aligned} G_1 &= Z_{891} \times Z_{11} & G_2 &= Z_{9801} \\ G_3 &= Z_{297} \times Z_{33} & G_4 &= Z_{3267} \times Z_3 \\ G_5 &= Z_{99} \times Z_{99} & G_6 &= Z_{1089} \times Z_9 \\ G_7 &= Z_{99} \times Z_{33} \times Z_3 & G_8 &= Z_{1089} \times Z_3 \times Z_3 \\ G_9 &= Z_{33} \times Z_{33} \times Z_3 \times Z_3 & G_{10} &= Z_{363} \times Z_3 \times Z_3 \times Z_3. \end{aligned}$$

$\square$

4. Which of the following groups of order 80 are isomorphic?

   (a) $Z_5 \times Z_4 \times Z_4$

   (b) $Z_{10} \times Z_8$

   (c) $Z_4 \times Z_{20}$

   (d) $Z_8 \times Z_5 \times Z_2$

   Proof. We will put each of them in elementary divisor form. Call them G_1, G_2, G_3, G_4 respectively. The first one is already there (although I usually order it with increasing primes). That is:

   $$G_1 \cong Z_4 \times Z_4 \times Z_5.$$

   For the second group we factor $10 = 2 \cdot 5$ and $8 = 2^3$. Thus the elementary divisor form has a 2, a 2^3 and a 5. We write:

   $$G_2 \cong Z_2 \times Z_8 \times Z_5.$$

   For the third, we notice $4 = 2^2$ and $20 = 2^2 \cdot 5$. Thus we have 2 4's, and a 5. That is:

   $$G_3 \cong Z_4 \times Z_4 \times Z_5.$$

   For the last, we see $8 = 2^3$ and the rest are factored. So we have a 2, an 8, and a 5. That is:

   $$G_4 \cong Z_2 \times Z_8 \times Z_5.$$

   It is now easy to see that $G_1 \cong G_3$ and $G_2 \cong G_4$. $\square$

5. Let A be an abelian group of (invariant factor) type $(n_1, n_2, \cdots, n_s)$. Show that there exists some element in A of order m if and only if $m|n_1$. Conclude that the exponenet of A is n_1.

   Proof. We write

   $$A \cong Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_t} \cong \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_t \rangle,$$

   so that the generator of the ith component is x_i with order n_i. Suppose $m|n_1$. Let $k = n_1/m$. Then $|x_1^k| = m$ as an element of Z_{n_1}, and therefore $(x_1^k, 1, \cdots, 1) \in A$ has order m as well.

   Conversely, suppose $y \in A$ with $|y| = m$. In coordinates we have $y = (y_1, y_2, \cdots, y_t)$. Then $y^{n_1} = (y_1^{n_1}, y_2^{n_1}, \cdots, y_t^{n_1})$. Each $n_i|n_1$, so call $k_i = n_1/n_i$. Then:

   $$y_i^{n_1} = (y_i^{n_i})^{k_i} = 1^{k_i} = 1,$$

   because anything in Z_{n_i} to the n_ith power is 1. Thus $y^{n_1} = 1$, so that the order of y divides n_1. This completes the proof.

   Since anything to the power n_1 is 1, we know that n_1 is less than or equal to the exponenent of A. But $(x_1, 1, \cdots, 1)$ has order n_1, so the exponenet could be no smaller that n_1. $\square$