HOMEWORK 12

Due date: Monday of Week 13

Exercises: 8.1, 8.2, 8.6, 8.7, 8.8, 8.10, 8.12, 10.1, 10.2, 10.4, 11.4, 11.6, 11.8, 11.9, pages 72-76 of Artin's book

One important construction in group theory which is not covered in the textbook is *semidirect product*. We define it here. Given a group N, recall that $\mathrm{Aut}(N)$ denotes the *group* of all automorphisms of N. It is consisting of all $f : N \to N$ such that f is an isomorphism. For example, if $N = \mathbb{Z}^+$, the map $f : N \to N$ defined by $f(x) = -x$ is an automorphism. The group structure on $\mathrm{Aut}(N)$ is just composition.

Let H and N be two groups and let $\phi : H \to \mathrm{Aut}(N)$ be a group homomorphism. In particular, for each $h \in H$, $\phi(h) : N \to N$ is an automorphism. We now define a group $N \rtimes_\phi H$, which is called the (outer) semidirect product of N with H with respect to ϕ. As a set, $N \rtimes_\phi H$ is just the Cartesian product of N with H, namely, as a set $N \rtimes_\phi H = \{(n, h) | n \in N, h \in H\}$. The group operation $\bullet$ (product in the group) is defined by

$$(n_1, h_1) \bullet (n_2, h_2) = (n_1\phi(h_1)(n_2), h_1h_2), n_1, n_2 \in N, h_1, h_2 \in H.$$

Here recall that $\phi(h_1) : N \to N$ is an isomorphism, and thus $\phi(h_1)(n_2) \in N$. Note that if ϕ is the trivial homomorphism, namely, $\phi(h) = \mathrm{id}_N$ for every $h \in H$, then $N \rtimes_\phi H$ is just the direct product $N \times H$. Thus semi-direct product is a generalization of product.

Problem 1. (1) *Show that $N \rtimes_\phi H$ defined above is indeed a group.*

(2) *Consider the map $i_N : N \to N \rtimes_\phi H$ defined by $i_N(n) = (n, 1)$ and $i_H : H \to N \rtimes_\phi H$ defined by $i_H(h) = (1, h)$. Show that i_N, i_H are injective group homomorphisms.*

(3) *Show that $i_N(N)$ is a normal subgroup of $N \rtimes_\phi H$.*

(4) *Show that the map $\pi_H : N \rtimes_\phi H \to H$ defined by $\pi_H((n, h)) = h$ is a group homomorphism.*

One might ask how the group structure of $N \rtimes_\phi H$ depends on ϕ.

Problem 2. *Let $f : H \to H$ be an automorphism and let $\phi_1 : H \to \mathrm{Aut}(N)$ be a group homomorphism. Consider $\phi_2 = \phi_1 \circ f : H \to \mathrm{Aut}(N)$. Show that $N \rtimes_{\phi_1} H \cong N \rtimes_{\phi_2} H$.*

Hint: Consider the map $N \rtimes_{\phi_1} H \to N \rtimes_{\phi_2} H$ defined by $(n, h) \mapsto (n, f^{-1}(h))$.

Problem 3. *Let $\theta \in \mathrm{Aut}(N)$ be an automorphism of N and let $\phi_1 : H \to \mathrm{Aut}(N)$ be a group homomorphism. Consider $\phi_2 : H \to \mathrm{Aut}(N)$ defined by $\phi_2(h) = \theta \circ \phi_1(h) \circ \theta^{-1}$. Show that ϕ_2 is a group homomorphism and $N \rtimes_{\phi_1} H \cong N \rtimes_{\phi_2} H$.*

If $\phi_2(h) = \theta \circ \phi_1(h) \circ \theta^{-1}$, we say that ϕ_2 and ϕ_1 differ by an inner automorphism of N.
Hint: Consider the map $N \rtimes_{\phi_1} H \to N \rtimes_{\phi_2} H$ defined by $(n, h) \mapsto (\theta(n), h)$.
If we combine Problem 2 and Problem 3, we get the following

Proposition 0.1. *If $\phi_1, \phi_2 : H \to \mathrm{Aut}(N)$ are two group homomorphisms such that there exists an automorphism $f \in \mathrm{Aut}(H)$ and an automorphism $\theta \in \mathrm{Aut}(N)$ such that $\phi_2(h) = \theta \circ \phi_1(f(h)) \circ \theta^{-1}, \forall h \in H$. Then we have*

$$N \rtimes_{\phi_1} H \cong N \rtimes_{\phi_2} H.$$

Now a good question is: is the converse true? In other words, suppose that we are given two group homomorphisms $\phi_1, \phi_2 : H \to \mathrm{Aut}(N)$ such that $N \rtimes_{\phi_1} H \cong N \rtimes_{\phi_2} H$, do we know that there exists $f \in \mathrm{Aut}(H), \theta \in \mathrm{Aut}(N)$ such that $\phi_2(h) = \theta \circ \phi_1(f(h)) \circ \theta^{-1}$? The answer to the previous question is No. See this link.

Let n be a positive integer and let C_n denote the cyclic group of order n. We have isomorphism $C_n \cong \mathbb{Z}/n\mathbb{Z}$ with addition as the group operation. If p is a prime, we can identify C_n with $\mathbb{Z}/p\mathbb{Z}$, which is the finite field $\mathbb{F}_p$.

Problem 4. *Show that* $\mathrm{Aut}(C_n) = \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. *Here recall that*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} : \text{ there is an element } b \in \mathbb{Z}/n\mathbb{Z}, \text{ such that } ab = 1\}.$$

The group structure on $(\mathbb{Z}/n\mathbb{Z})^\times$ *is multiplication.*

If $n = 10$, this is Exercise 6.10 (a).

Problem 5. *Let* p, q *be two primes.*

1. *If there exists a non-trivial group homomorphism* $C_q \to \mathrm{Aut}(C_p)$, *show that* $q|(p-1)$;
2. *Suppose* $q|(p-1)$. *Determine all group homomorphisms* $C_q \to \mathrm{Aut}(C_p)$;
3. *Suppose* $q|(p-1)$. *Let* ϕ_1, ϕ_2 *be two different nontrivial group homomorphisms* $C_q \to \mathrm{Aut}(C_p)$. *Show that there exists an isomorphism* $f : C_q \to C_q$ *such that* $\phi_2 = \phi_1 \circ f$.
4. *Suppose* $q|(p-1)$. *Conclude that there are only two isomorphism classes* $C_p \rtimes_\phi C_q$ *using Problem 2.*

(This one might be hard. For part (3), you might need to use the following fact. The group $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group. We will prove this later.)

The following is an example regarding the dependence of the semi-direct product $H \rtimes_\phi N$ on ϕ in the sense of Problem 3.

Problem 6. *Consider the group* $N = C_3 \times C_3 = \mathbb{F}_3 \times \mathbb{F}_3$ *and* $H = C_2$. *Here we identify the cyclic group* C_3 *with the finite field* $\mathbb{F}_3$.

1. *Show that* $\mathrm{Aut}(N) \cong \mathrm{GL}_2(\mathbb{F}_3)$.
2. *Classify all group homomorphisms of* $\phi : C_2 \to \mathrm{Aut}(N)$ *up to conjugation.*
3. *Show that there are only 3 isomorphism classes of the semi-direct product* $H \rtimes_\phi N$ *using Problem 3.*

(1) is somehow a generalization of part (1) of Problem 4. Of course, it is true in a more general setting. Write $C_2 = \{1, z : z^2 = 1\}$. For (2), think about what can be the image of $\phi(z)$ up to conjugation in $\mathrm{GL}_2(\mathbb{F}_3)$. It should satisfies $\phi(y)^2 = 1$ and thus it is diagonalizable because the polynomial $x^2 - 1 \in \mathbb{F}_3[x]$ has no repeated roots. The rest should be easy.

We now consider a special case of semidirect product. Suppose that N and H are both subgroups of a group G with $N \cap H = \{1\}$. Moreover, suppose that for any $h \in H$ and $n \in N$, we have $hnh^{-1} \in N$. If this condition is satisfied, we say that H normalizes N. Then we define

$$\phi : H \to \mathrm{Aut}(N)$$

by $\phi(h)(n) = hnh^{-1}$. Then we can form the semidirect product. $N \rtimes_\phi H$. In this case, we often drop ϕ from the notation, and write it as $N \rtimes H$.

Problem 7. *Show that there is an injective homomorphism* $N \rtimes H \to G$.

Hint: the map is just $(n, h) \to nh$.

We then identify $N \rtimes H$ as a subgroup of G. This is called the inner semidirect product of N and H.

Problem 8. *Suppose that* N, H *are two subgroups of* G. *Show that* $G = N \rtimes H$ *if and only if the following conditions hold.*

1. N *is normal in* G;
2. $G = NH$;
3. $N \cap H = \{1\}$.

Compare this with Proposition 2.11.4, page 65.

Problem 9. *Show that the quaternion group H defined in (2.4.5), page 47 of Artin's book is not a semidirect product of its two proper subgroups.*

The following are some examples of semi-direct product.

0.1. $\mathrm{GL}_n(F) = \mathrm{SL}_n(F) \ltimes F^\times$**.** Let F be a field and let n be a positive integer. Consider the group $G = \mathrm{GL}_n(F)$ and its subgroup $N = \mathrm{SL}_n(F) = \{g \in \mathrm{GL}_n(F) : \det(g) = 1\}$ and

$$H = \left\{ \begin{pmatrix} a & \\ & I_{n-1} \end{pmatrix} : a \in F^\times \right\} \cong F^\times.$$

Then from Problem 6, we can check that $G = N \rtimes H$. For example, to check $G = NH$, for any $g \in G$, we consider

$$n = g \begin{bmatrix} \det(g)^{-1} & \\ & I_{n-1} \end{bmatrix} \in N, h = \begin{bmatrix} \det(g) & \\ & I_{n-1} \end{bmatrix} \in H.$$

Then $g = nh \in NH$.

0.2. $S_n = A_n \rtimes (\mathbb{Z}/2\mathbb{Z})$**.** Suppose $n \geq 2$. Let $G = S_n$ and $N = A_n$. Moreover, take $\sigma = (12) \in S_n$ and $H = \{1, \sigma\} \cong \mathbb{Z}/2\mathbb{Z}$. We can check from Problem 6 that $G = N \rtimes H$. Here we just check that $G = NH$. For any $g \in S_n$. If g is a even permutation, then $g \in A_n$. If g is an odd permutation, then $n = g\sigma \in A_n$. Thus $g = (g\sigma)(\sigma) \in NH$. For example, $S_3 = N \ltimes H$, where $N = \{1, x, x^2 : x^3 = 1\}$ and $H = \{1, y : y^2 = 1\}$.

0.3. **Groups of order** pq**.** Let p, q be two distinct prime numbers and let G be a group of order p, q. Then there exists a normal subgroup N (of order p or q) and a subgroup H (or order q or p), such that $G = N \rtimes H$. This could be proved using Sylow's theorem, which we will learn later. Thus by Problem 4, there are at most two isomorphism classes of groups of order pq. Assume $q < p$. Actually, by Problem 4, if $q \nmid (p-1)$, there is only one group of order pq, which is a direct product $C_p \times C_q \cong C_{pq}$. Hence it is cyclic. If $q|(p-1)$, there are two isomorphism classes of groups of order p, q. One is cyclic, and the other one is a non-trivial semi-direct product (non-abelian).

0.4. **Isometry group.** An isometry of $\mathbb{R}^n$ is a map $f : \mathbb{R}^n \to R^n$ such that $|f(x) - f(y)| = |x - y|$ for any $x, y \in \mathbb{R}^n$, where $|x - y|$ denotes the distance between x and y. More precisely, we have

$$|x| = \sqrt{(x|x)}.$$

Here we don't assume that f is linear. One type of non-linear isometry is translation, which is defined as follows. For any $\alpha \in \mathbb{R}^n$, define $t_\alpha : \mathbb{R}^n \to \mathbb{R}^n$ defined by $t_\alpha(x) = x + \alpha$.

Theorem 0.2 (Theorem 6.2.3 of Artin's book)**.** *Given a map $\varphi : \mathbb{R}^n \to \mathbb{R}^n$. The following are equivalent.*

(1) *φ is an isometry and $\varphi(0) = 0$.*
(2) *φ preserve the standard inner product: $(\varphi(\alpha)|\varphi(\beta)) = (\alpha|\beta)$ for all $\alpha, \beta \in \mathbb{R}^n$.*
(3) *$\varphi \in \mathrm{O}_n(\mathbb{R})$, namely, φ is an orthogonal linear operator.*

The proof is not hard. From this, one sees that, up to a translation, an isometry is just an orthogonal linear operator. More precisely, let $f : \mathbb{R}^n \to \mathbb{R}^n$ be an isometry, and suppose $\alpha = f(0)$. Consider the map $\varphi := t_{-\alpha} \circ f$. We have $\varphi(0) = t_{-\alpha}(\alpha) = 0$. Thus φ is an orthogonal linear operator. We then have $f = t_{-\alpha} \circ \varphi$.

Let M_n be the set of all isometries on $\mathbb{R}^n$. One sees easily that $(M_n, \circ)$ is a group, where $\circ$ denotes composition. Let $\mathbb{T}_n$ be the subset of M_n consisting of translations.

Problem 10. (1) *Show that the map $t : \mathbb{R}^n \to \mathbb{T}_n$ defined by $t(\alpha) = t_\alpha$ is a group isomorphism. Here $\mathbb{R}^n$ is viewed as an abelian group under the addition.*
(2) *Show that $\mathbb{T}_n$ is a normal subgroup of M_n.*
(3) *Show that there is an isomorphism $M_n \cong \mathbb{R}^n \rtimes_\phi \mathrm{O}_n(\mathbb{R})$, where $\phi : \mathrm{O}_n(\mathbb{R}) \to \mathrm{Aut}(\mathbb{R}^n)$ is the natural map $T \mapsto \phi(T)$ for $T \in \mathrm{O}_n(\mathbb{R})$, where $\phi(T) : \mathbb{R}^n \to \mathbb{R}^n$ is defined by $\phi(T)(\alpha) = T(\alpha)$. Here $T \in \mathrm{O}_n(\mathbb{R})$ is viewed as a linear orthogonal operator $\mathbb{R}^n \to \mathbb{R}^n$.*
(4) *Show that the above semi-direct product is not a direct product.*