Assignment 12, due April 29

Corrections: April 26: Exercise 4 corrected to replace aut$G$ (which is impossible) with aut(N). Exercise 7 made the notation clearer, replacing $\rho(f)$ with $\rho(f^j)$. April 27: Part (a) of Exercise 8 fixed a typo (actually, an editing fail) to replace N by H in one place.

This assignment describes the *semi-direct product* of groups. This is a foundation for a future discussion of induced representation of semi-direct products, which comes next week (hopefully). It is an opportunity to weave together several different parts of algebra from this semester and last semester.

1. Let G be a group, $H \subset G$ a subgroup, and $N \subset G$ a normal subgroup. Assume that $NH = G$, which means that every $g \in G$ may be written as $g = nh$ for some $n \in N$ and $h \in H$. Assume that $N \cap H = \{\text{id}\}$.
   (a) Show that if $g = nh$ with $n \in N$ and $h \in H$, then n and h are unique.
   (b) Show that $(n_1h_1)(n_2h_2) = (n_1n_2')(h_1h_2)$ with $n_2' = h_1n_2h_1^{-1}$.
2. The automorphism group of G is the group of isomorphisms of G, under composition. That is, $\rho \in \text{aut}(G)$ means that $\rho\colon G \to G$ is a group isomorphism on G. The group operation in aut(G) is composition, which means $\rho_1\rho_2 = \rho_1 \circ \rho_2$. On the left is the product in the group aut(G). On the right is composition of isomorphisms of G. Show that aut(G) defined like this is a group (associativity, inverses).
3. Describe the group aut(C_p), where C_p is the cyclic group of order p and p is prime.
4. Suppose that $N \subset G$ is a normal subgroup and $H \subset G$ is another subgroup, which need not be normal. Consider a map $\rho\colon H \to \text{aut}(N)$ defined in the following way. For $h \in H$, let $\rho(h)$ be the automorphism
$$n \xrightarrow{\rho(h)} hnh^{-1} .$$
   Show that $\rho(h) \in \text{aut}(N)$ for any $h \in H$, and that $h \to \rho(h)$ is a homomorphism from H to aut(N).
5. Suppose N and H are groups and $\rho\colon H \to \text{aut}(G)$ is a homomorphism as above. Define the operation that takes pairs of pairs to pairs $[(n_1, h_1), (n_2, h_20] \to (n_3, h_3)$ defined by $n_3 = n_1\rho(h_1)n_2$ and $h_3 = h_1h_2$. Here n_1n_2 is group multiplication in N, and h_1h_2 is group multiplication in H, and $\rho(h)n \in N$

is the result of applying the isomorphism $\rho(h)$ to n. We write with a $*$ to look like multiplication

$$(n_1, h_1) * (n_2, h_2) = (n_1 \rho(h_1) n_2, h_1 h_2) \ .$$

Show that this $*$ is a group operation (associativity, inverses). The resulting group is the *semi-direct* product of N with H (also called *twisted product*) and written

$$N \rtimes_\rho H \ .$$

Comment: It might seem clearer to express the $*$ operation as a map

$$(N \times H) \times (N \times H) \longrightarrow N \times H \ .$$

I didn't use this notation because $N \times H$ here is not the group product of the groups N and H. It is only the set product of the sets N and H, which is $\{(n,h) \mid n \in N, \ h \in H\}$. The only groups involved in this construction are N, H, and the twisted product $N \rtimes_\rho H$.

6. With the definitions of Exercise 1 and Exercise 4, show the following is an isomorphism between $N \rtimes_\rho H$ and G:

$$\begin{aligned} N \rtimes_\rho H &\longrightarrow G \\ (n,h) &\mapsto nh \ . \end{aligned}$$

In this situation (subgroups generating G), the semi-direct product is called *inner*.

7. Show that the dihedral group D_n is the semi-direct product of $N = C_n$ with $H = C_2$. For $k \in C_n$ and $j \in C_2$, the semi-direct structure is $\rho(f^j)k = (-1)^j k \pmod{n}$. The dihedral group is defined as being generated by a rotation r with $r^n = \mathrm{id}$, and a flip $f^2 = \mathrm{id}$, and the commutation relation $frf = frf^{-1} = r^{-1}$.

8. (*This longer exercise is a review of Galois theory and gives an example of semi-direct product.*) Let K be the splitting field over $\mathbb{Q}$ of $x^p = 2$, p being an odd prime. Let $\alpha = 2^{\frac{1}{p}} \in \mathbb{R}$ be the real $p-th$ root of 2. Let $\omega \in \mathbb{C}$ be a primitive $p-th$ root of unity. Let G be the Galois group of K over $\mathbb{Q}$.

   (a) Explain the basic Galois facts about the cyclotomic extension $\mathbb{Q}[\omega]/\mathbb{Q}$. Your explanation should cover the following points in whatever order or form you find convenient.

      - The elements ω^j for $j = 0, \ldots, p-2$ are a basis of $\mathbb{Q}[\omega]$ over $\mathbb{Q}$.
      - $\mathbb{Q}[\omega]$ is a normal extension of $\mathbb{Q}$ with Galois group $H = \mathrm{gal}(\mathbb{Q}[\omega]/\mathbb{Q}$ isomorphic to C_{p-1}.
      - H is generated by an automorphism of $\mathbb{Q}[\omega]/\mathbb{Q}$ that is determined by $\omega \xrightarrow{\sigma} \omega^g$.

- The inverse of this generator is determined by $\omega \overset{\sigma^{-1}}{\to} \omega^{\gamma}$ where $\gamma g = 1 \bmod p$.
- The order of the extension $\mathbb{Q}[\omega]/\mathbb{Q}$, as determined by the dimension of $\mathbb{Q}[\omega]$ as a vector space over $\mathbb{Q}$, or as determined by the order of the Galois group, is the same.

(b) Explain the basic Galois facts about $\mathbb{Q}[\omega, \alpha]/\mathbb{Q}[\omega]$. Your discussion should cover the following points in some way and in some order.

- f splits in $\mathbb{Q}[\omega, \alpha]$.
- There are no intermediate fields between $\mathbb{Q}[\omega, \alpha]$ and $\mathbb{Q}[\omega]$.
- The elements $\omega^j \alpha^k$, for $j = 0, \ldots, p-2$ and $k = 0, \ldots, p-1$, form the basis of $\mathbb{Q}[\omega, \alpha]$ over $\mathbb{Q}$.
- The elements α^k form a basis of $\mathbb{Q}[\omega, \alpha]$ over $\mathbb{Q}[\omega]$.
- f is irreducible in $\mathbb{Q}[\omega]$.
- $N = \text{gal}(\mathbb{Q}[\omega, \alpha]/\mathbb{Q}[\omega])$ is cyclic of order p generated by an element τ determined by $\alpha \overset{\tau}{\to} \omega\alpha$.
- $N \subset G$ is a normal subgroup because its fixed field is $\mathbb{Q}[\omega]$, which is a normal extension of $\mathbb{Q}$.

You may assume that f has no roots in $\mathbb{Q}$ (Proof: if $x = \frac{a}{b}$ is a rational root in "lowest terms" (a and b relatively prime) then 2 divides a, then 2 divides b.) That doesn't necessarily imply that f is irreducible.

(c) Calculate the commutator $\sigma\tau\sigma^{-1}$ as it acts on an element $x \in \mathbb{Q}[\omega, \alpha]$ in the form

$$x = \sum_{j=0}^{p-2} \sum_{k=0}^{p-1} a_{jk} \omega^j \alpha^k$$

with rational coefficients a_{jk}. Write formulas for σx and τx, etc. Use this, together with Exercise 3 to describe the homomorphism from H (part (a)) to $\text{aut}(N)$ (of part (b)). *Hint*: It was easier for me not to write a formula for τx in the form

$$\sum_{j=0}^{p-2} \sum_{k=0}^{p-1} b_{jk} \omega^j \alpha^k \ .$$

Instead, I wrote used expressions of the form

$$x = \sum_{jk} a_{jk} \omega^{l_{jk}} \alpha^{m_{jk}} \ .$$

Applying σ and τ just changes the exponents of ω and α, but keeping the fact that the elements form a basis of $\mathbb{Q}[\omega, \alpha]$ over $\mathbb{Q}$.

(d) (*The goal of all this, besides reviewing Galois theory*) Express G as a semi-direct product of C_p with C_{p-1}.