Solutions to Assignment 4

1. Let G be a finite, abelian group written additively. Let $x = \sum_{g \in G} g$, and let G_2 be the subgroup of G defined by $G_2 = \{g \in G | 2g = 0\}$.

   (a) Show that $x = \sum_{g \in G_2} g$.

   (b) Show that $x = 0$ if $|G_2| \neq 2$. If $|G_2| = 2$, show that x is the unique non-zero element of G_2.

   (c) Show that $|G_2| = 2$, iff the 2-Sylow subgroup of G is cyclic and non-trivial.

   (d) Let p be prime. Show that $(p-1)! = -1 \mod p$ (Wilson's Theorem). (Hint. Apply part (b) to the multiplicative group (mod p) $Z_p = \{1, 2, \ldots, p-1\}$.)

   Solution:
   (a) $x = \sum_{g \in G_2} g + \sum_{g \in G \setminus G_2} g$. Now, in the second summation, every $g \in G \setminus G_2$ has period not equal to 2, and hence g is not an inverse of itself. Moreover, $g \in G \setminus G_2 \implies -g \in G \setminus G_2$. Thus, every element in the second sum can be paired of with its inverse, making the sum 0. Hence, $x = \sum_{g \in G_2} g$.

   (b) Every element other than 0 in G_2 has period 2. Thus, $|G_2|$ must be a power of 2 (say 2^m). Choose m different non-zero elements of G_2, $a_1, \ldots, a_m$. Then, $G_2 = \langle a_1 \rangle \oplus \cdots \oplus \langle a_m \rangle$ (using the theorems of direct sums). Clearly, if $m > 1$ then summing over all elements of G_2 will produce 0 (just verify component-wise). When $m = 1$, $x = a_1$ the unique non-zero element.

   (c) If $|G_2| = 2$ then the unique 2-Sylow subgroup is non-trivial (has to contain G_2) and has exactly one element x of order 2. Now, the 2-Sylow subgroup being an Abelian 2-group is isomorphic to a direct sum $Z_{2^{r_1}} \oplus \cdots \oplus Z_{2^{r_k}}$. Let, $a_1, \ldots, a_k$ be the generators of the corresponding cyclic groups. But, $2^{r_i - 1} a_i$ has period 2 and must equal x for $1 \leq i \leq k$. But, the 2-Sylow subgroup is a direct sum of the $\langle a_i \rangle$, and hence $\langle a_i \rangle \cap \langle a_j \rangle = \{0\}$ for $i \neq j$. Hence, k has to be 1 and the 2-Sylow subgroup must be cyclic.
   Conversely, if the 2-Sylow subgroup is non-trivial cyclic with generator a of order $2^r, r \geq 1$, it has exactly one element of order 2, namely $2^{r-1}a$, and hence $|G_2| = 2$.

   (d) The multiplicative group of the field F_p is Abelian. Also, the equation $x^2 - 1$ has exactly two solutions $1, -1$. Thus, applying part (b) we have that the product of all elements is equal to the unique non-identity in $G_2 = \{1, -1\}$, which is -1. (Note that, we are using multiplicative notation here and so sums are written as products, the identity is 1 etc., but since the underlying group is Abelian we can use the results of part (a) and (b).

2. G be a finite group, and $\varphi : G \longrightarrow G$ a homomorphism.

   (a) Prove that there exists a positive integer n such that for all integers $m \geq n$, we have $\operatorname{Im} \varphi^m = \operatorname{Im} \varphi^n$ and $\operatorname{Ker} \varphi^m = \operatorname{Ker} \varphi^n$.

(b) For n as above, prove that G is the semidirect product of the subgroups $\operatorname{Ker}\varphi^n$ and $\operatorname{Im}\varphi^n$.

Solution: (a) We have a sequence of subgroups, $\operatorname{Ker}\varphi \subseteq \operatorname{Ker}\varphi^2 \subseteq \operatorname{Ker}\varphi^3 \cdots$, which must stabilize since G is finite. Similarly, the sequence $\operatorname{Im}\varphi \supseteq \operatorname{Im}\varphi^2 \supseteq \operatorname{Im}\varphi^3 \cdots$ must stabilize as well.

(b) Let $x \in \operatorname{Ker}\varphi^n \cap \operatorname{Im}\varphi^n$. Then $x = \varphi^n(y)$ for some $y \in G$, and $\varphi^n(x) = \varphi^{2n}(y) = e$. But then $y \in \operatorname{Ker}\varphi^{2n} = \operatorname{Ker}\varphi^n$, and so $x = e$. This shows that $\operatorname{Ker}\varphi^n \cap \operatorname{Im}\varphi^n = \{e\}$.

Since $G/\operatorname{Ker}\varphi^n \approx \operatorname{Im}\varphi^n$, we have $|G| = |\operatorname{Ker}\varphi^n||\operatorname{Im}\varphi^n|$. Since $(\operatorname{Ker}\varphi^n)(\operatorname{Im}\varphi^n)$ is a subgroup of G of order $|G|$, it must equal G. Consequently G is a semidirect product of $\operatorname{Ker}\varphi^n$ and $\operatorname{Im}\varphi^n$.

3. Let G be a finite group, and p a prime integer dividing $|G|$ such that the map $\varphi : G \longrightarrow G$, where $\varphi(x) = x^p$, is a homomorphism.

   (a) Prove that G has a unique p-Sylow subgroup P.

   (b) Prove that there is a normal subgroup $N \lhd G$ such that $N \cap P = \{e\}$ and $G = PN$.

   (c) Show that G has a nontrivial center.

Solution: (a) By the previous problem, there exists n such that $\operatorname{Im}\varphi^m = \operatorname{Im}\varphi^n$ and $\operatorname{Ker}\varphi^m = \operatorname{Ker}\varphi^n$ for all $m \geq n$. But then $\operatorname{Ker}\varphi^n$ is the subgroup of G consisting of *all* elements of G whose order is a power of p. Consequently $P = \operatorname{Ker}\varphi^n$ is the unique p-Sylow subgroup of G.

(b) Let $N = \operatorname{Im}\varphi^n$. By the previous problem, $N \cap P = \{e\}$ and $G = PN$. Let $x^{p^n} \in N$ and $g \in G$. Then $gx^{p^n}g^{-1} = (gxg^{-1})^{p^n} \in N$, and so N is normal.

(c) Since $N \lhd G$ and $P \lhd G$, we have $[n, h] \in N \cap P$ for all elements $n \in N$ and $h \in P$. But $N \cap P = \{e\}$, so $[n, h] = e$. By the previous problem G is a semi-direct product of P and N but, since elements of N commute with those of P, we actually have $G \approx P \times N$. The p-group P has a nontrivial center which is contained in the center of G.

4. Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group, i.e., $(-1)^2 = 1$ is the identity element, $i^2 = j^2 = k^2 = -1$, and

$$ij = k = -ji, \qquad jk = i = -kj, \qquad ki = j = -ik.$$

   (a) Determine all subgroups of Q and prove that they are normal.

   (b) What is the order of $\operatorname{Aut}(Q)$?

Solution: (a) Aside from e, the group Q consists of six elements of order 4 and one element of order 2, namely -1. Consequently the only subgroups of Q are

$$Q, \quad \langle i \rangle, \quad \langle j \rangle, \quad \langle k \rangle, \quad \langle -1 \rangle, \quad \{e\}.$$

(b) Any two elements of order four, which are not powers of each other, constitute a generating set for Q. Any automorphism $\varphi \in \mathrm{Aut}(Q)$ is determined by its behavior on a generating set, and must take a generating set to a generating set. Consider the generating set $\{i, j\}$. Then

$$\varphi(i) \in \{\pm i, \pm j, \pm k\} \qquad \text{and} \qquad \varphi(j) \in \{\pm i, \pm j, \pm k\} \setminus \{\pm\varphi(i)\}.$$

Consequently $|\,\mathrm{Aut}(Q)| = 24$.

5. Let $p < q$ be prime numbers such that p divides $q - 1$. If G is a non-abelian group of order pq, show that $Z(G) = \{e\}$.

   Solution: If $Z(G)$ is nontrivial, then $|Z(G)|$ equals p or q. But then $G/Z(G)$ is cyclic, in which case G must be abelian.

6. Determine, up to isomorphism, all groups of order 63.

   Solution: Let $|G| = 63$. Since $63 = 3^2 \times 7$, by an earlier homework problem either the 3-Sylow or the 7-Sylow subgroup is normal in G.

   Suppose the 3-Sylow subgroup P is normal, then

   $$G \approx P \rtimes_\alpha \mathbb{Z}/7 \quad \text{for} \quad \alpha : \mathbb{Z}/7 \longrightarrow \mathrm{Aut}(P).$$

   If $P \approx \mathbb{Z}/9$ then $|\,\mathrm{Aut}(P)| = 8$ and α is trivial. In this case, $G \approx \mathbb{Z}/9 \times \mathbb{Z}/7 \approx \mathbb{Z}/63$.

   If $P \approx \mathbb{Z}/3 \times \mathbb{Z}/3$ then $|\,\mathrm{Aut}(P)| = 48$ and once again α must be trivial. This implies that $G \approx \mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/7 \approx \mathbb{Z}/3 \times \mathbb{Z}/21$.

   If P is not normal then the 7-Sylow subgroup $Q \approx \mathbb{Z}/7$ is normal, and so

   $$G \approx \mathbb{Z}/7 \rtimes_\beta P \quad \text{where} \quad \beta : P \longrightarrow \mathrm{Aut}(\mathbb{Z}/7)$$

   is a nontrivial homomorphism. Note that $\mathrm{Aut}(\mathbb{Z}/7) \approx \mathbb{Z}/6$, and so it has a unique subgroup of order 3, which must be the image of β. Consequently, up to isomorphism, there are exactly two other groups of order 63, namely

   $$G \approx \mathbb{Z}/7 \rtimes_\beta \mathbb{Z}/9 \quad \text{and} \quad G \approx \mathbb{Z}/7 \rtimes_\beta (\mathbb{Z}/3 \times \mathbb{Z}/3).$$

7. Recall the definitions of fibre product and fibre co-product.

   (a) Show that fibre products exist in the category of Abelian groups. If $f : X \to Z, g : Y \to Z$ are Abelian group homomorphisms, show that $X \times_Z Y$ is the set of all pairs $(x, y), x \in X, y \in Y$ such that $f(x) = g(y)$.

   (b) Prove that the pull back of a surjective homomorphism is surjective.

8. The purpose of this problem is to show that fibre coproducts exist in the category of Abelian groups.

(a) In this case the fibre coproduct of two homomorphisms, $f : Z \to X, g : Z \to Y$ is the factor group, $X \oplus_Z Y = (X \oplus Y)/W$, where W is the subgroup consisting of all elements $(f(z), -g(z)), z \in Z$.

(b) Prove that the push out of an injective homomorphism is injective.

Solution: Omitted.

9. A groups is called *finitely generated* (resp. *finitely presented*) if it admits a presentation,

$$\langle (t_i)_{i\in I}; (r_j)_{j\in J}\rangle$$

where I is a finite set (resp. where I and J are finite sets).

(a) Let G be a finitely presented group and $x = (x_\alpha)_{\alpha\in A}$ a finite generating family of G. Show that there exists a finite family s of relators of the family x such that $\langle x; s\rangle$ is a presentation of G.

Solution: Let $\langle t; r\rangle$ be a finite presentation of G, where $t = (t_i)_{i\in I}$, and $r = (r_j)_{j\in J}$ and I, J are finite sets. Let $T = (T_i)_{i\in I}$ (where T_i are new symbols) and let $r_j(T)$ denote the words with the new symbols T substituted for t. Similarly, let $X = (X_\alpha)_{\alpha\in A}$.

For any set S, let $F[S]$ denote the free group on S. Let R_t be the normal subgroup of $F[T]$ generated by $r(T)$. Then, $G \cong F[T]/R_t$.

Let $\phi : F[T] \to G$ be the homomorphism sending T_i to t_i. Clearly, R_t is the kernel of ϕ. Similarly, $\psi : F[X] \to G$, sending X_α to x_α. Let R_x be the kernel of ψ.

For each $i \in I$, let $A_i \in F[X]$, such that $t_i = \psi(A_i)$. Let $\gamma_1 : F[T] \to F[X]$ sending T_i to A_i.

Similarly, for each $\alpha \in A$, let $B_\alpha \in F[T]$ such that $x_\alpha = \phi(B_\alpha)$ and let $\gamma_2 : F[X] \to F[T]$ sending X_α to B_α.

We claim, that R_x is the normal subgroup generated by the elements $r_j(A), j \in J$ and $X_\alpha^{-1}\gamma_1(\gamma_2(X_\alpha)), \alpha \in A$. Let R'_x be the normal subgroup of $F[X]$ generated by these elements. Then, clearly $R'_x \subset R_x$. The homomorphism γ_1, after passing to the quotient gives a homomorphism $G \cong F[T]/R_t \to F[X]/R'_x$, which is inverse to the canonical homomorphism $F[X]/R'_x \to F[X]/R_x \cong G$. This shows that $R'_x = R_x$.

(b) Show that a finite group is finitely presented.
Solution: The finite set of elements of the group and the finite multiplication table gives a finite set of generators and relators respectively.

(c) Given an example of a finitely presented group with a subgroup which is not finitely generated.

Solution: Let $S = \{a, b\}$ and $G = F[S]$ the free group generated by S. Let $(w_k)_{k\geq 0}$ be any enumeration of the reduced words of G, which begin and end with powers of a. Let $B = \{b^{-k}w_kb^k | k \geq 0\}$. Let H be the subgroup of G generated by B. We claim that there is no non-trivial relations on the elements of B and hence H is free on B and is thus not finitely generated. Clearly, a word on the elements of B could reduce to identity iff it is of the form $s^{\epsilon_1} \dots s^{\epsilon_n}$ where $s = b^{-k}w_kb^k$ for some fixed k and $\epsilon_i \in \{\pm 1\}$. However, in this case it is easy to see that it must be the trivial relation.

(d) If G is a finitely presented group and H a normal subgroup of G, show the equivalence of the following properties:

i. G/H is finitely presented.

ii. There exists a finite subset X of G such that H is the normal subgroup of G generated by X.

Solution: Suppose that G/H is finitely presented. Let $x = (x_i)_{i \in I}$ and $s = (s_j)_{j \in J}$ be the generators and relators of G. Similarly, let $u = (u_\alpha H)_{\alpha \in A}$ and $r = (r_\beta)_{\beta \in B}$ be the generators and relators of G/H. Here, I, J, A, B are all finite sets.

Let $X = (X_i)_{i \in I}$ and $U = (U_\alpha)_{\alpha \in A}$.

Consider the homomorphisms,

$$F[U] \to G \to G/H,$$

where the first homomorphism is defined by $U_\alpha \mapsto u_\alpha$ and the second homomorphism is the canonical homomorphism. Clearly, the kernel of the composition is the normal subgroup of $F[U]$ generated by the elements $r_\beta(U)$. Hence, the images of these elements in G must generate H. Hence, H is generated by the finite set of elements $r_\beta(u)$.

Conversely, suppose that there exists a finite set of elements $g = (g_k)_{k \in K}$ which generate H.

For each $k \in K$, let $W_k \in F[X]$ such that $w_k = g_k$.

It is easy to see that G/H can be described by the generators $(x_iH)_{i \in I}$, and relators $(s_j)_{j \in J}$ and $(W_k)_{k \in K}$.

10. Show that the group defined by the presentation

$$\langle x, y; xy^2(y^3x)^{-1}, yx^2(x^3y)^{-1} \rangle$$

is the trivial group.

Solution: We first show that $x^2y^8x^{-2} = y^{18}$ and $x^3y^8x^{-3} = y^{27}$.

$$xy^2 = y^3x \implies xy^2x^{-1} = y^3.$$

Squaring and cubing both sides we get,

$$xy^4x^{-1} = y^6, \dots\dots\dots (i)$$

and

$$xy^6x^{-1} = y^9..........(ii)$$

Substituting (i) into (ii) we get,

$$x^2y^4x^{-2} = y^9,...........(iii)$$

and squaring,

$$x^2y^8x^{-2} = y^{18}.........(iv)$$

Multiplying (iii) and (iv) we get,

$$x^2y^{12}x^2 = y^{27}..........(v)$$

Also, squaring (i) we have that,

$$xy^8x^{-1} = y^{12}............(vi)$$

Substituting (vi) into (v) we get that,

$$x^3y^8x^{-3} = y^{27}...........(vii)$$

Now,

$$y^{27} = x^3y^8x^{-3} = (x^3y)y^8(y^{-1}x^{-3}) = yx^2y^8x^{-2}y^{-1} = yy^{18}y^{-1} = y^{18}.$$

This implies that $y^9 = e$. Now, y^2, y^3 are conjugates and hence have the same period. Hence, $y = e$ and hence $x = e$.