THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2023-24
Homework 2 Answer

Compulsory Part

1. When $A = \{a\}$ is a singleton, show that the free group $F(A)$ is isomorphic to the infinite cyclic group $\mathbb{Z}$.

   Proof. Any word in $F(A)$ must be of the form $a^k,\ k \in \mathbb{Z}$, and for each $k \neq 0$, $a^k \neq 1$. Hence $F(A) \simeq \mathbb{Z}$.

   Another Proof (Categorical approach): We verify that $\mathbb{Z}$ possesses the desired universal property: Let $\phi : \{a\} \to \mathbb{Z}$ be such that $\phi(a) = 1$. Then we need to show that for any group G, and for any map $\psi : \{a\} \to G$, there exists a unique group homomorphism $f : \mathbb{Z} \to G$ such that $f \circ \phi = \psi$. Given such a pair (G, ψ), $f \circ \phi = \psi \iff f(1) = \psi(a)$. There do exists a unique homomorphism $f : \mathbb{Z} \to G$ such that $f(1) = \psi(a)$: It is the f such that $f(n) = \psi(a)^n$ for any $n \in \mathbb{Z}$. $\square$

2. Verify that $\mathbb{Z}^{\oplus A} := \{f : A \to \mathbb{Z} : f(a) \neq 0$ for only finitely many $a \in A\}$ is indeed an abelian group, for any given set A.

   Proof. For $f \in \mathbb{Z}^{\oplus A}$, let Supp$(f) := \{a \in A \mid f(a) \neq 0\}$. Then $|\text{Supp}(f)| < \infty$ for any $f \in \mathbb{Z}^{\oplus A}$. Note that Supp$(f + g) \subseteq$ Supp$(f) \cup$ Supp(g). Therefore, Supp$(f + g)$ is also finite, thus $\mathbb{Z}^{\oplus A}$ is closed under the operation $+$.

   Next, as integer-valued functions, $(f + g) + h = f + (g + h)$ and $f + g = g + f$ for any $f, g, h \in \mathbb{Z}^{\oplus A}$. The 0 function $0(a) = 0$ for any $a \in A$ serves as the identity in $\mathbb{Z}^{\oplus A}$, and the inverse of f is $-f$ with $(-f)(a) = -(f(a))$, where both 0 and $-f$ lie in $\mathbb{Z}^{\oplus A}$ because Supp$(0) = \varnothing$, and Supp$(-f) =$ Supp(f). Thus, we have verified that $(\mathbb{Z}^{\oplus A}, +)$ is an abelian group. $\square$

3. Show that a finitely generated abelian group can be presented as a quotient of $\mathbb{Z}^{\oplus n}$ for some positive integer n.

   Proof. By the structure theorem of finitely generated abelian group, the group is isomorphic to $\mathbb{Z}^{\oplus m} \oplus (\bigoplus_{i=1}^{n} \mathbb{Z}_{p_i^{r_i}})$.

   Hence it can be represented by the quotient $\mathbb{Z}^{m+n}/(0 \oplus (\bigoplus_{i=1}^{n} p_i^{r_i}\mathbb{Z}))$. $\square$

4. Prove that $(\mathbb{Q}_{>0}, \cdot)$ is a free abelian group, meaning that it is isomorphic to $\mathbb{Z}^{\oplus A}$ for some set A.

   [*Hint*: Use the fundamental theorem of arithemetic, i.e., every positive integer can be uniquely factorized as a product of primes.]

Proof. Consider the set $\mathbb{P}$ of all prime numbers. We claim that $\mathbb{Q}_{>0}$ is free on the basis $\mathbb{P}$ with respect to multiplication.

To show this, we first note that every positive rational number q can be uniquely expressed in the form $q = \prod_{p\in\mathbb{P}} p^{n_p}$, where $n_p \in \mathbb{Z}$ and all but finitely many n_p are zero. This is a direct consequence of the Fundamental Theorem of Arithmetic, as each n_p represents the power of the prime p in the prime factorization of q (positive for factors in the numerator and negative for factors in the denominator).

In other words, each element of $\mathbb{Q}_{>0}$ can be uniquely expressed as a finite product of elements of $\mathbb{P}$ raised to integer powers. This means that the set $\mathbb{P}$ forms a basis for $\mathbb{Q}_{>0}$ with respect to multiplication, and that $\mathbb{Q}_{>0}$ is free on $\mathbb{P}$.

This basis has the same cardinality as $\mathbb{Z}^{\oplus A}$ for $A = \mathbb{P}$, so $(\mathbb{Q}_{>0}, \cdot)$ is isomorphic to $\mathbb{Z}^{\oplus A}$, as required. □

5. Let G be a group. For any $g \in G$, the map $i_g : G \to G$ defined by $i_g(a) = gag^{-1}$ for any $a \in G$ is an automorphism of G, which is called an **inner automorphism** of G. Prove that the set $\mathrm{Inn}(G)$ of inner automorphisms of G is a normal subgroup of the automorphism group $\mathrm{Aut}(G)$ of G.

   [*Warning:* Be sure to show that the inner automorphisms do form a subgroup.]

   Proof. Let G be a group. Define the map $\phi : G \to \mathrm{Aut}(G)$ by $g \mapsto i_g$, where $i_g(x) = gxg^{-1}$ is the conjugation by g. We show that ϕ is a homomorphism. Let $g, h \in G$. Then $i_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = g(i_h(x))g^{-1} = i_g(i_h(x))$. Note that $\mathrm{Inn}(G) = \phi(G)$. Therefore, $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$.

   Let $\phi \in \mathrm{Aut}(G), g \in G$. Then

$$\begin{aligned}
&\phi i_g \phi^{-1}(x)\\
&= \phi(g\phi^{-1}(x)g^{-1})\\
&= \phi(g)\phi(\phi^{-1}(x))\phi(g^{-1})\\
&= \phi(g)x(\phi(g))^{-1}\\
&= i_{\phi(g)}(x).
\end{aligned}$$

   Therefore, $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

   □

6. Show that an intersection of normal subgroups of a group G is again a normal subgroup of G.

   Proof. Let $\{N_\alpha\}_{\alpha\in I}$ be a family of normal subgroups of G. Then $e_G \in N_\alpha$ for each α, so $e_G \in \bigcap N_\alpha$. Let $a, b \in \bigcap N_\alpha$. Then for any $\alpha \in I$, $a, b \in N_\alpha$, so $ab^{-1} \in N_\alpha$ as $N_\alpha \leq G$. Therefore, $ab^{-1} \in \bigcap N_\alpha$. It follows that $\bigcap N_\alpha < G$.

   For any $g \in G$, $a \in \bigcap N_\alpha$, $gag^{-1} \in N_\alpha$ for each N_α, because each $N_\alpha \lhd G$. Therefore, $gag^{-1} \in \bigcap N_\alpha$. Thus, $\bigcap N_\alpha \lhd G$. □

7. Let G be a group containing at least one subgroup of a fixed finite order s. Show that the intersection of all subgroups of G of order s is a normal subgroup of G.

   [*Hint:* Use the fact that if H has order s, then so does $x^{-1}Hx$ for all $x \in G$.]

   Proof. Let $K = \bigcap_{H<G,|H|=s} H$. We show that $K \lhd G$. First, K is a subgroup of G as it is the intersection of a family of subgroups of G. Let $a \in G$. Then $aKa^{-1} = \bigcap_{H<G,|H|=s} aHa^{-1}$. Clearly, for each $H < G$ with $|H| = s$, aHa^{-1} also satisfies $aHa^{-1} < G$ and $|aHa^{-1}| = s$. Therefore, $aKa^{-1} = \bigcap_{H<G,|H|=s} aHa^{-1} \subseteq \bigcap_{H<G,|H|=s} H = K$. It follows that $K \lhd G$.

   $\square$

Optional Part

1. Let G be a finite group with $|G|$ odd. Show that the equation $x^2 = a$, where x is the indeterminate and a is any element in G, always has a solution. (In other words, every element in G is a square.)

   Proof. For any $a \in G$, suppose the order of a is n. Then n is odd since $|G|$ is odd. Let $b = a^{\frac{n+1}{2}}$, we have $b^2 = a^{n+1} = a$. $\square$

2. Generalizing the above question: If G is a finite group of order n and k is an integer relatively prime to n, show that the map $G \to G, a \mapsto a^k$ is surjective.

   Proof. $\forall a \in G$, suppose the order of a is m where $m|n$. There exists some t such that $kt = 1 \; mod \; n$ since n and k are relatively prime. Define $b = a^t$, then $b^t = a^{kt} = a$. $\square$

3. Prove that every finite group is finitely presented.

   Proof. Let $X = \{g_1, ..., g_n\}$ be the set of all elements of G, then we can define the surjective homomorphism $\phi : F(X) \to G$ which maps all words to the corresponding words in G. Therefore, G is finitely generated. The relations of G are finitely generated. It suffices to use all the $g_i g_j g_{\phi(i,j)}^{-1} = e$ kind of relation, where $\phi(i,j)$ is such that $g_i g_j = g_{\phi(i,j)}$. The number of generating relations used is n^2. $\square$

4. We have learnt that a presentation of the dihedral group D_n is given by $(a, b \mid a^2, b^n)$.

   Let a, b be distinct elements of order 2 in a group G. Suppose that ab has finite order $n \geq 3$. Prove that the subgroup $\langle a, b \rangle$ generated by a and b is isomorphic to the dihedral group D_n (which has $2n$ elements).

   Proof. The subgroup $\langle a, b \rangle = \langle a, ab \rangle$ satisifies the relation: $a^2 = e, (ab)^n = e, b^2 = (a^{-1}ab)^2 = e$. Hence we have a surjective group homomorphism $\phi : D_n = \langle r, s \mid r^n = s^2 = rsrs = 1 \rangle \to \langle a, b \rangle$ with $\phi(s) = a, \phi(r) = ab$.

   Note that $\langle ab \rangle < \langle a, ab \rangle$. Because $\operatorname{ord}(ab) \geq 3$, $ab \neq (ab)^{-1}$. Then $ab \neq ba$, so $\langle a, b \rangle$ is not abelian. Therefore, $[\langle a, b \rangle : \langle ab \rangle] \geq 2$. Then $|\langle a, b \rangle| \geq 2n$. Since $\phi : D_n \to \langle a, ab \rangle$ is surjective, it must be that $|\langle a, b \rangle| = 2n$, and that ϕ is bijective. Therefore, $\langle a, b \rangle \simeq D_n$. $\square$

5. Let $G = \mathbb{Z}^{\oplus \mathbb{N}}$. Prove that $G \times G \cong G$ (as abelian groups).

   Proof. Define a homomorphism:

   $$\mathbb{Z}^{\mathbb{N}} \times \mathbb{Z}^{\mathbb{N}} \longrightarrow \mathbb{Z}^{2\mathbb{N}+1} \times \mathbb{Z}^{2\mathbb{N}} \cong \mathbb{Z}^{\mathbb{N}}$$

   Clearly it is a bijective, hence isomorphism. $\square$

6. Prove that $(\mathbb{Q}, +)$ is not a free abelian group.

Proof. Suppose, for contradiction, that $(\mathbb{Q}, +)$ is a free abelian group with basis B.

First, note that for any $a \in \mathbb{Q}$, $Za \neq \mathbb{Q}$, where Za represents the set of all integer multiples of a. This means that no single element can generate the whole group, implying that B must contain at least two distinct elements.

Let a and b be two distinct elements in B. We can represent a and b as m/n and p/q respectively, for some integers m, n, p, q with $n, q \neq 0$.

Now, consider the relation $mqb = npa$. Since at least one of a, b in nonzero, we have $m \neq 0$ or $p \neq 0$. This relation implies that a and b are not independent over $\mathbb{Z}$, which contradicts our assumption that B is a basis.

Therefore, we have a contradiction, so $(\mathbb{Q}, +)$ cannot be a free abelian group. $\square$

7. Show that if a finite group G has exactly one subgroup H of a given order, then H is a normal subgroup of G.

   Proof. Let $a \in G$. Then aHa^{-1} is a subgroup of G (it is the image of H under the inner automorphism $x \mapsto axa^{-1}$) and has the same order as H. By the assumption, aHa^{-1} must be equal to H. Therefore, H is normal. $\square$

8. Show that the set of all $g \in G$ such that the inner automorphism $i_g : G \to G$ is the identity inner automorphism i_e is a normal subgroup of a group G.

   Proof. Let G be a group. Define the map $\phi : G \to \text{Aut}(G)$ by $g \mapsto i_g$. We show that ϕ is a homomorphism. Let $g, h \in G$. Then $i_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = g(i_h(x))g^{-1} = i_g(i_h(x))$. Now the set of all $g \in G$ such that i_g is the identity inner automorphism is the kernel of ϕ. It follows that this set is a normal subgroup of G. $\square$