The following is a compiled review for the second exam according to the study guide.

2 Groups

A Definitions

Exercise 2.72 (Normalizer $N(S)$)**.** *Let G be a group and let $S \subseteq G$ be nonempty. The normalizer of S in G is $N(S) = N_G(S) = \{g \in G \mid gSg^{-1} = S\}$...*

Exercise 2.73 (Commutator)**.** *Suppose G is a group and let G' be the subgroup generated by $\{g_1g_2g_1^{-1}g_2^{-1} \mid g_i \in G\}$, called the commutator subgroup of G...*

Definition 2.1 (Torsion)**.** *Let G be an abelian group and let T be the set of all elements of G with finite order; T is a subgroup called the torsion subgroup.*

Definition 2.20 (Homomorphism, Isomorphism, Automorphism)**.** *Let G and H be groups and let $\varphi : G \to H$ be a function.*

1. *If $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$, then φ is a homomorphism.*
2. *A bijective (one-to-one and onto) homomorphism is called an isomorphism. In that case, G amd H are said to be isomorphic and we write $G \cong H$.*
3. *If $G = H$, an isomorphism is also called an automorphism.*

Definition 2.22 (Conjugation Map)**.** *Let G be a group and let $g, h \in G$. The conjugation map $c_g : G \to G$ is defined by $c_g(h) = ghg^{-1}$.*

Definition 2.24 (Image and Kernel)**.** *Let $\varphi : G \to H$ be a homomorphism between groups.*

1. *The image of φ is $\operatorname{Im}\varphi = \{\varphi(g) \mid g \in G\}$.*
2. *The kernel of φ is $\ker\varphi = \{g \in G \mid \varphi(g) = e_H\}$.*

Definition 2.27 (Cosets)**.** *Let G be a group and let H be a subgroup of G. Let $g \in G$.*

1. *The left coset of g with respect to H is $gH = \{gh \mid h \in H\}$.*
2. *If C is a left coset with respect to H and $C = gH$, then g is called a representative of C.*
3. *The set of left cosets is denoted G/H and is called the quotient of G by H.*
4. *The index of H in G is $|G/H|$ and is denoted $[G : H]$.*

Definition 2.30 (Normality)**.** *Let G be a group, let H be a subgroup of G, and let $g \in G$.*

1. *The right coset of g with respect to H is $Hg = \{hg \mid h \in H\}$.*
2. *H is called normal if $gHg^{-1} \subseteq H$ for all $g \in G$ where $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$.*

Theorem 2.31 (Normality T.F.A.E.s)**.** *The following are equivalent:*

1. *H is normal.*
2. *$gHg^{-1} = H$ for all $g \in G$.*
3. *Left cosets are right cosets; i.e., $gH = Hg$ for all $g \in G$.*
4. *$gH \subseteq Hg$ for each $g \in G$.*
5. *$Hg \subseteq gH$ for each $g \in G$.*
6. *The equation $(g_1H)(g_2H) = (g_1g_2)H$ gives a well-defined binary operation on G/H where $g_1, g_2 \in G$.*
7. *$ghg^{-1} \in H$ for all $g \in G, h \in H$.*

Definition 2.32. *Let G be a group and let H be a normal subgroup of G. Under the bilinear operation $(g_1H)(g_2H) = (g_1g_2)H$ for $g_1, g_2 \in G$, G/H is a group and is called the quotient group or factor group.*

Exercise 2.151. *Let N and H be groups along with a homomorphism $\varphi : H \to \mathrm{Aut}(N)$. For $n \in N$ and $h \in H$, write $\varphi_h(n)$ for $(\varphi(h))(n)$. Define the semidirect product of N and H as*

$$N \rtimes H = \{(n, h) \mid n \in N, h \in H\}$$

with a group law given by

$$(n_1, h_1)(n_2, h_2) = (n_1\varphi_{h_1}(n_2), h_1h_2) \dots$$

B Book Proofs

Theorem 2.23. *Let G be a group and let $g \in G$. Then c_g is an automorphism.*

Proof. We must show that the conjugation map c_g is first, a homomorphism, second, an isomorphism, and third, from G to G.

1. Homomorphism: Let $h_1, h_2 \in G$. We know that

   $$c_g(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = c_g(h_1)c_g(h_2)$$

   therefore c_g is a homomorphism.

2. Isomorphism: Because $c_{g^{-1}}$ is a valid inverse of c_g, we know that c_g is a bijection and thus also an isomorphism.

3. $G \to G$: As $g, h_1, h_2 \in G$, c_g thus maps $G \to G$ and is consequently an automorphism.

□

Theorem 2.25. *Let $\varphi : G \to H$ be a homomorphism between groups and let $g \in G$.*

3. $\varphi(e_G) = e_h$.

4. $\varphi(g^{-1}) = \varphi(g)^{-1}$.

5. φ *is one-to-one if and only if* $\ker\varphi = \{e_G\}$.

Proof. For part (3), because φ is a homomorphism, we can say

$$\begin{aligned}\varphi(e_G) &= \varphi(e_G)\varphi(e_G)\\ \varphi(e_G)\varphi(e_G)^{-1} &= \varphi(e_G)\varphi(e_G)\varphi(e_G)^{-1}\\ e_H e_H &= \varphi(e_G)\\ e_H &= \varphi(e_G).\end{aligned}$$

For part (4), we can similarly say

$$\begin{aligned}e_H = \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})\\ \Rightarrow \varphi(g)^{-1} = \varphi(g^{-1}).\end{aligned}$$

For part (8), we must show that φ is one-to-one implies that $\ker\varphi = \{e_G\}$, and vice versa.

1. $\underline{\varphi \text{ is one-to-one} \Rightarrow \ker\varphi = \{e_G\}}$: If we suppose that φ is one-to-one, we can say that given an element $g \in G$ such that $\varphi(g) = e_H \in H$, we know that $g = e_G$ as $e_G \mapsto e_H$ in any one-to-one mapping.

2. $\underline{\ker\varphi = \{e_G\} \Rightarrow \varphi \text{ is one-to-one}}$: Suppose we have $g_1, g_2 \in G$ such that $\varphi(g_1) = \varphi(g_2)$. We can then say that $\varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_2 g_2^{-1}) \Rightarrow \varphi(g_1 g_2^{-1}) = e_H$ which implies $g_1 = g_2$, which forces φ to be one-to-one.

Thus "φ is one-to-one" $\Leftrightarrow \ker\varphi = \{e_G\}$. □

Lemma 2.27. *Let G be a group, let $H \leq G$, and let $g_1, g_2 \in G$. Then $g_1H = g_2H$ if an only if $g_2 = g_1h$ for some $h \in H$.*

Proof. To prove their biconditional relationship, we must prove that $g_1H = g_2H \Rightarrow g_2 = g_1h$ for some $h \in H$ and $g_2 = g_1h$ for some $h \in H \Rightarrow g_1H = g_2H$.

1. $\underline{g_1H = g_2H \Rightarrow \exists h \in H,\ g_2 = g_1h}$: If we suppose $g_1H = g_2H$, we know that $e \in H$ implies $g_2 \in g_2H$; consequently $g_2 \in g_1H$ therefore $\exists h \in H,\ g_2 = g_1h$.

2. $\underline{\exists h \in H,\ g_2 = g_1h \Rightarrow g_1H = g_2H}$: If we then suppose that $\exists h \in H,\ g_2 = g_1h$, we know that $g_2h = g_1hh$ implies $g_2H \subseteq g_1H$ as H is closed. For the reverse, we can rewrite the starting expression as $g_2h^{-1} = g_1$ which can be similarly manipulated as $g_2h^{-2} = g_1h^{-1}$ which implies $g_2H \supseteq g_1H$ when all h are taken into account. Therefore these two subsets are equal, $g_1H = g_2H$.

Thus $g_1H = g_2H \Leftrightarrow \exists h \in H,\ g_2 = g_1h$. □

Corollary 2.29. *Let G be a finite group.*

1. *If $g \in G$, then $|g|$ divides $|G|$.*

2. *In particular, $g^{|G|} = e$.*

Proof. For part (1), we know that $|g| = |\langle g \rangle|$ and that $\langle g \rangle$ is a subgroup of G; therefore $|g|$ does divides G by Lagrange's theorem as G is a finite group. For part (2), we can say that $|G| = |g|k$ for some $k \in \mathbb{Z}_{>0}$. Therefore $g^{|G|} = g^{|g|k} = (g^{|g|})^k = e^k = e$. □

Theorem 2.35 (First Isomorphism Theorem)**.** *Let $\varphi : G \to H$ be a homomorphism of groups.*

1. *$\ker \varphi$ is a normal subgroup of G.*

Proof. For part (1), suppose $k \in \ker \varphi$ and $g \in G$. By definition of the kernel:

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} = \varphi(g)e_H\varphi(g)^{-1} = e_H.$$

Therefore $g \ker \varphi g^{-1} = \ker \varphi$ and $\ker \varphi$ is normal. □

Lemma 2.39 (Cauchy's Theorem for Finite Abelian Groups)**.** *Let G be a finite abelian group and let p be a positive prime with $p \mid |G|$. Then G has an element of order p.*

Proof. We can express G as $\{g_1, \ldots, g_n\}$ with each elements order, $|g_i|$, represented by d_i. We can define a subgroup H as a direct product of n number of $\mathbb{Z}_{d_i}$, expressed as $\prod_{i=1}^{n} \mathbb{Z}_{d_i}$. We can then define a map $\varphi : H \to G$ by $\varphi(k_1, \ldots, k_n) = g^{k_1} \ldots g^{k_n}$; this is a well-defined, surjective homomorphism as G is abelian. Therefore, by the First Isomorphism Theorem, $|H| = |\ker \varphi||G|$. If p divides $|G|$, p must also then divide $|H|$ and consequently $\prod_{i=1}^{n} d_i$. Therefore p must divide at least one d_i and $g = g_i^{d_i/p}$ which is only true if $d_i = p$; thus p is the order of at least one element g_i. □

C Homework Exercises

Exercise 2.53. *Show the following subsets are groups:*

(b) $\{5^a \mid a \in \mathbb{Q}\} \subseteq \mathbb{R}^\times$.

(c) $k\mathbb{Z}_n = \{k[m] \mid [m] \in \mathbb{Z}_n\} \subseteq \mathbb{Z}_n$ *where* $k \in \mathbb{Z}$ *and* $n \in \mathbb{N}$.

(g) $SL(n, \mathbb{R}) \subseteq GL(n, \mathbb{R})$.

In order to demonstrate the given subsets are groups, we need to show that their operation is closed, that all elements are associative, that there exists an identity, and that each element has an inverse.

(b) The subset from part (b) is a group as it:

(i) is closed, as $(5^a) \cdot (5^n) = 5^{a+n}$, $a + n \in \mathbb{Q}$ $\forall n \in \mathbb{Q}$;
(ii) is associative, as $(5^a 5^b)5^c = 5^{a+b+c} = 5^a(5^b 5^c)$ $\forall b, c \in \mathbb{Q}$;
(iii) contains an identity, 5^0, as $5^a 5^0 = 5^{a+0} = 5^a$, and;
(iv) has an inverse for every element, as $5^a 5^{-a} = 5^{a-a} = 5^0$.

(c) The subset from part (c) is a group as it:

(i) is closed, as $k[i] + k[j] = k[i + j] \in k\mathbb{Z}_n$;
(ii) is associative, as $k[i] + (k[j] + k[l]) = (k[i] + k[j]) + k[l] = k[i + j + l]$;
(iii) contains an identity, as $k[0] \equiv 0 \pmod{n}$, and;
(iv) has an inverse for every element, as $k[i] + k[-i] = k[0] \equiv 0 \pmod{n}$.

(g) The subset from part (g) is a group as it:
(i) is closed, as two $n \times n$ invertible matrices with $\det = 1$ will produce an invertible matrix with $\det = 1$;
(ii) is associative, as all matrices in the general linear group are associative;
(iii) contains an identity, the identity matrix with $\det(I_n) = 1$, and;
(iv) has an inverse for every element, as $\det(A) = 1 \Rightarrow \det(A^{-1}) = \frac{1}{\det(A)} = 1^{-1} = 1$.

Exercise 2.57. *Evaluate the following:*

(a) $([3]_7, [5]_6) \cdot ([2]_7, [5]_6) \in U_7 \times U_6$.

(b) $([2]_4, [3]_5, [6]_7) + ([3]_4, [2]_5, [1]_7) \in \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7$.

For part (a), we perform component-wise multiplication:

$$[3]_7 \cdot [2]_7 = [6]_7, \ [5]_6 \cdot [5]_6 = [1]_6.$$

Therefore the answer in $U_7 \times U_6$ is $([6]_7, [1]_6)$. For part (b) we perform component-wise addition:

$$[2]_4 + [3]_4 = [1]_4, \ [3]_5 + [2]_5 = [0]_5, \ [6]_7 + [1]_7 = [0]_7.$$

Therefore the answer in $\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ is $([1]_4, [0]_5, [0]_7)$.

Exercise 2.63 (Subgroups of $\mathbb{Z}$ and $\mathbb{Z}_n$)**.** *Complete the following:*

(f) Find all subgroups of $\mathbb{Z}_{15}$.

The set of subgroups of $\mathbb{Z}_n$ is $\{\langle [k] \rangle \mid k \in \mathbb{N} \text{ and } k \mid n\}$. Therefore the set of all subgroups of $\mathbb{Z}_{15}$ is $\{\langle [0] \rangle, \langle [1] \rangle, \langle [3] \rangle, \langle [5] \rangle\}$.

Exercise 2.96. *Show the following groups are not isomorphic.*

(a) $\mathbb{Z}_4 \ncong \mathbb{Z}_5$.

(b) $S_3 \ncong \mathbb{Z}_6$.

(c) $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(d) $\mathbb{R}^\times \ncong \mathbb{R}$.

(e) $\mathbb{Z} \ncong \mathbb{Q}$.

D Homework Proofs

E New Exercises