Contributions to Projective Group Theory

Francois Koch van Niekerk

Thesis presented in partial fulfillment of the requirements for the degree of Master of Science in Mathematics in the Faculty of Science at Stellenbosch University.

Supervised by Professor Zurab Janelidze
December 2017

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: December 2017

Abstract

Projective Group Theory (PGT for short) provides a self-dual axiomatic context that allows one to establish homomorphism theorems for (non-abelian) group-like structures. The present thesis has two broad aims. The first is to introduce a "norm function" in PGT as a way to capture the notion of an order of a (finite) group in PGT, extend some elementary results on finite groups to PGT, propose a definition of a (finite) cyclic group in PGT, and make an attempt to recapture the Second Sylow Theorem. We also describe a process of building a model for *normed* PGT (i.e. PGT with a norm function), from a monoid equipped with a family of congruences, subject to suitable axioms. In the case of the multiplicative monoid of natural numbers equipped with the family of modular congruences, we recover the model of normed PGT formed by finite cyclic groups. The second aim of the thesis is to introduce and study biproducts and commutators in PGT, which generalize usual products and commutators for group-like structures. Our biproducts are not categorical products, although, as we show, they form a monoidal structure. However, our notion of a biproduct is self-dual, just like (and is in fact very similar to) the one in the context of an abelian category.

Opsomming

Projektiewe groepteorie (PGT vir kort) bied ’n selfduale konteks wat mens toelaat om homomorfisme stellings vir (nie-abelse) groepagtige strukture vas te stel. Die huidige tesis het twee breë doelwitte. Die eerste is om ’n “norm funksie” in PGT voor te stel as ’n manier om die konsep van ’n orde van ’n (eindige) groep in PGT vas te vang, sommige elementêre resultate van eindige groepe na PGT te verleng, ’n definisie van (eindige) sikliese groepe in PGT voor te stel, en om ’n poging aan te wend om die Tweede Sylow Stelling vas te vang. Ons beskryf ook ’n proses om modelle vir genormeerde PGT (d.w.s. PGT met ’n norm funksie) te bou van monoïede toegerus met ’n familie van kongruensies, onderhewig aan geskikte aksiomas. In die geval van die multiplikatiewe monoïed van natuurlike getalle toegerus met die familie van modulêre kongruensies, kry ons die model van genormeerde PGT gevorm deur eindige sikliese groepe terug. Die tweede doelwit van hierdie tesis is om biprodukte en kommutators in PGT voor te stel en te studeer, wat die gewone produkte en kommutators vir groepagtige strukture veralgemeen. Ons biprodukte is nie kategoriese produkte nie, alhoewel, soos ons wys, vorm hulle ’n monoïedale struktuur. Egter, ons konsep van biproduk is selfduaal, net soos (en is in werklikheid baie soortgelyk tot) die een in die konteks van ’n abelse kategorie.

Acknowledgements

Firstly I would like to thank my supervisor, Professor Zurab Janelidze. The door to Prof. Janelidzes office was always open whenever I ran into a trouble spot or had a question about my research or writing. He consistently allowed this paper to be my own work, but steered me in the right direction whenever I needed it.

Then I wish to thank the Harry Crossley Scholarship Fund for financial support during 2016 and 2017. It was an indispensable part of my studies.

Finally, I must express my gratitude to my parents, Pieter and Christel van Niekerk, for their support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis.

Contents

Chapter 1

Introduction

1.1 Background and Outline

Projective group theory (PGT for short) provides a self-dual approach to certain results and constructions in group theory — for example, the isomorphism theorems. On one hand, PGT unifies certain constructions and theorems in classical group theory via duality, and on the other hand, it is applicable to many other group-like structures such as rings, modules, loops, and more generally to any semi-abelian category in the sense of [7] and any Grandis exact category in the sense of [5].

The term "projective group theory" has so far only appeared in informal notes of Janelidze, who developed this theory together with his collaborators (see [4] and the references there).

The context of PGT consists of abstract "groups", "subgroup lattices", "group homomorphisms", their composition and direct and inverse images of subgroups along group homomorphisms. This structure can be presented as a functor $F\colon \mathbb{B} \to \mathbb{C}$ where $\mathbb{C}$ is the "category of groups" and fibers of F are the subgroup lattices. Duality in PGT refers to switching from F to its dual functor $F^{\mathsf{op}}\colon \mathbb{B}^{\mathsf{op}} \to \mathbb{C}^{\mathsf{op}}$ — the axioms of PGT are invariant under this process, so we refer to them as being *self-dual*. A detailed discussion of this structural background of PGT is carried out in the present Chapter 1.

The aim of Chapters 2 and 3 is to make several new contributions to PGT. Chapter 2 begins with introducing a "norm function" in PGT which assigns to each subgroup an element in a fixed multiplicative abelian group, which intuitively is the "size" of the subgroup. For classical group theory, the norm of a subgroup is simply its order. To allow for self-dual axioms on the norm function, in PGT we define the "order" of a group as the quotient of the norms of its largest and smallest subgroup. So in PGT the size of a group is no longer the same as the size of itself seen as a subgroup (note that in PGT subgroups and groups are different objects — the former are objects from the category $\mathbb{B}$ and the latter from the category $\mathbb{C}$). We establish some basic facts how the norm of subgroups and the order of groups interact with the rests of the structure of PGT. We then describe a process of building models of *normed* PGT (i.e. PGT equipped with a norm function), from an abstract monoid equipped with a family of congruences, subject to suitable axioms. In the case of the multiplicative monoid of natural numbers equipped with the family of modular congruences, we recover the model of normed PGT formed by cyclic groups. Chapter 2 concludes with an attempt to recover the Second Sylow Theorem in PGT.

In Chapter 3 we introduce and study "biproducts" in PGT, which generalize the usual cartesian products of ordinary groups. In classical group theory, restricting to only finite groups, we lose direct sums of groups, which are the categorical duals of cartesian products. However, our notion of a biproduct is such that on the one hand it is self-dual, and on the other hand, restricting to ordinary groups (finite or not) it gives precisely the notion of cartesian product of groups. This also means that in general, our biproducts are not categorical products. However, we show that they still form a monoidal structure. We also show that existence of biproducts in general PGT implies that the category of groups (the category $\mathbb{C}$ from the earlier notation) is a pointed category. We then use biproducts to introduce commutators of subgroups in PGT and study their fundamental properties. There is an existing theory of commutators for semi-abelian categories, and since PGT is in some sense a self-dual version of the theory of semi-abelian categories, one expects there to be a number of close links between our theory of commutators in PGT and the one for semi-abelian categories. However, in the present thesis we do not go in the direction of establishing these links and rather leave it for a future work. Another link to be explored in future is the link with the theory of abelian categories, but we should already now remark that our definition of a biproduct in PGT was inspired by one of characterizations of biproducts in an abelian category found in [3] (Theorem 2.42 on page 51) — this is also why we use the term "biproduct", even though our biproducts are in general not categorical products, as already mentioned above.

The final Chapter 4 is less significant than the other chapters. It contains an account of some side observations in classical group theory (which could be original or not), mainly motivated by the investigation of cyclic groups and Sylow theorems in PGT.

1.2 Noetherian Forms

Most of the material in this section comes from Goswami and Janelidze's paper [4]. The presentation given here, is the author's presentation (although all notions come from either [4] or the papers from the same series cited there). This section contains all the necessary background of projective group theory for the other chapters that build on projective group theory.

Definition 1. A *form* is a functor $F\colon \mathbb{B} \to \mathbb{C}$ which is faithful and amnestic.

Definition 2. Two forms $F\colon \mathbb{B} \to \mathbb{C}$ and $F'\colon \mathbb{B}' \to \mathbb{C}'$ are isomorphic when there exist two isomorphisms $H\colon B \to \mathbb{B}'$ and $G\colon \mathbb{C} \to \mathbb{C}'$ such that $F'H = GF$.

Example 1. Let Grp_2 be the category where objects are pairs of groups (G, X) such that $X \leq G$, and morphisms $f\colon (G, X) \to (H, Y)$ are group homomorphisms

$f\colon G \to H$ such that $fX \leq Y$, and composition is composition of group homomorphisms. Functor $F\colon \mathsf{Grp}_2 \to \mathsf{Grp}$, defined by $Ff\colon G \to H$ for $f\colon (G,X) \to (H,Y)$, is a form.

The above example of a form motivates the following definition of a "set of subgroups" from an arbitrary functor.

Definition 3. For any functor $F\colon \mathbb{B} \to \mathbb{C}$, objects of $\mathbb{C}$ will be called *groups* and for any $G \in \mathbb{C}$, the *set of subgroups* of G is defined as

$$\mathsf{sub}G = \{X \in \mathbb{B} \mid FX = G\}.$$

Element of $\mathsf{sub}G$ will be called *subgroups* of G. Moreover, there is a *subgroup inclusion* relation $\leq$ defined by

$$X \leq Y \quad \Leftrightarrow \quad \exists_{f\colon X \to Y}(Ff = 1_G).$$

Proposition 1. *If $F\colon \mathbb{B} \to \mathbb{C}$ is a form, then for any G in $\mathbb{C}$, $(\mathsf{sub}G, \leq)$ is a partially ordered set.*

Proof. Reflexive: For any $X \in \mathsf{sub}G$, we have $F1_X = 1_G$, thus $X \leq X$.

Transitive: For any $X, Y, Z \in \mathsf{sub}G$ such that $X \leq Y$ and $Y \leq Z$, there is some $f\colon X \to Y$ and $g\colon Y \to Z$ such that $Ff = 1_G$ and $Fg = 1_G$. Then the composition, $gf\colon X \to Z$, is a morphism such that $F(gf) = 1_G$. Thus $X \leq Z$.

Anti-symmetric: For any $X, Y \in \mathsf{sub}G$ such that $X \leq Y$ and $Y \leq X$, there is some $f\colon X \to Y$ and $g\colon Y \to X$ such that $Ff = 1_G$ and $Fg = 1_G$. So $F(gf) = 1_G$. Since F is faithful, $gf = 1_X$. Similarly, $fg = 1_Y$. So $f\colon X \to Y$ is an isomorphism. Since F is amnestic, $f = 1_X$. $\square$

In projective group theory, we also want the concept of "direct" and "inverse image". They are defined as follow:

Definition 4. Take any morphism $f\colon G \to H$ in $\mathbb{C}$. For any $X \in \mathsf{sub}G$, if the set

$$\{Y \in \mathsf{sub}H \mid \exists_{g\colon X \to Y}(Fg = f)\}$$

has a minimum element, the minimum element will be denoted by fX and will be called the *direct image* of X under f. Furthermore, if $\mathsf{sub}G$ has a top element 1, and $f1$ exists, then $f1$ will be called the *image* of f, denoted by $\mathsf{Im}f$. And for $Y \in \mathsf{sub}H$, if the set

$$\{Y \in \mathsf{sub}H \mid \exists_{g\colon X \to Y}(Fg = f)\}$$

has a maximum element, the maximum element will be denoted by $f^{-1}Y$ and will be called the *inverse image* of Y under f. Furthermore, if $\mathsf{sub}H$ has a bottom element 0 and $f^{-1}0$ exists, then $f^{-1}0$ will be called the *kernel* of f, denoted by $\mathsf{Ker}f$.

The following proposition might be part of a motivation of the *amnestic* part of the definition of a form.

Proposition 2. *Suppose $F\colon \mathbb{B} \to \mathbb{C}$ is a faithful functor such that for any object G in $\mathbb{C}_0$, $(\mathsf{sub}(G), \leq)$ is a poset, then F is amnestic.*

Proof. Suppose $f\colon X \to Y$ is an isomorphism in $\mathbb{B}$ such that $Ff = 1_G$. So both X and Y are in $\mathsf{sub}G$, and $X \leq Y$. Since $Ff^{-1} = 1_G$ as well, $Y \leq X$. Since $(\mathsf{sub}G, \leq)$ is a poset, $X = Y$. Since F is faithful, $f = 1_X$. Thus F is amnestic. □

For the rest of this section, we will work with a fixed form $F\colon \mathbb{B} \to \mathbb{C}$. Consider the following axioms on a form.

Axiom 1. F is surjective on objects. Furthermore, for any $f\colon G \to H$ in $\mathbb{C}$ and any $X \in \mathsf{sub}G$, the set

$$\{Y \in \mathsf{sub}H \mid \exists_{g\colon X\to Y}(Fg = f)\}$$

has a minimum element, and also for any $Y \in \mathsf{sub}H$, the set

$$\{X \in \mathsf{sub}G \mid \exists_{g\colon X\to Y}(Fg = f)\}$$

has a maximum element. That is, direct and inverse images of subgroups always exists. Also, for any two composable morphisms $f\colon G \to H$ and $g\colon H \to K$, and subgroups X of G and Y of K, we have

$$(gf)X = g(fX) \quad \text{and} \quad f^{-1}(g^{-1}Y) = (gf)^{-1}Y$$

Axiom 2. For any group G, $\mathsf{sub}G$ is a bounded lattice. Furthermore, for any $f\colon G \to H$ in $\mathbb{C}$ and any $X \in \mathsf{sub}G$, we have

$$f^{-1}fX = X \vee f^{-1}0,$$

and, also, for any $Y \in \mathsf{sub}H$, we have

$$ff^{-1}Y = Y \wedge f1.$$

Axiom 3. For any group G and any subgroup X of G, there is a morphism $l_X\colon \underline{X}/1 \to G$, called the *embedding* of X, which is universal among all morphisms into G whose image is contained in X. That is, $\mathsf{Im}l_X \leq X$ and for any morphism $f\colon H \to G$ such that $\mathsf{Im}f \leq X$, there exists a unique $h\colon H \to \underline{X}/1$ such that $l_X h = f$.

And, there is also a morphism $r_X\colon G \to G/\overline{X}$, called the *projection* of X, which is universal among all morphisms from G whose kernel contains X.

Note that, for simplicity, if X is conormal, we will sometime denote the group $\underline{X}/1$ by just X.

Definition 5. The image of l_X will be denoted by $\underline{X}$, called the *conormal interior* of X, and the kernel of r_X will be denoted by $\overline{X}$, called the *normal closure* of X.

Axiom 4. Any $f\colon G \to H$ factorizes as

$$f = l_{\mathsf{Im}f} h r_{\mathsf{Ker}f}$$

for some isomorphism h.

A subgroup which is the kernel of some morphism, is called a *normal* subgroup. Also, a subgroup which is the image of some morphism, is called a *conormal* subgroup.

Axiom 5. The meet of conormal subgroups, is conormal. And the join of normal subgroups, is normal.

Definition 6. A form that satisfies all of five axioms above, will be called a *Noetherian* form.

These axioms holds for the form in Example 1, and the resulting definitions of direct and inverse image maps coincide with the direct and inverse image maps in group theory (and therefor also the definitions of kernels and images). Also, normal subgroups here coincide with normal subgroups in group theory, and all groups are conormal in group theory.

Notice that for any two isomorphic forms $F\colon \mathbb{B} \to \mathbb{C}$ and $G\colon \mathbb{A} \to \mathbb{C}$, F is a Noetherian form if and only if G is a Noetherian form. When that is the case, all the arising structure are isomorphic as well.

In the paper [4], they start with a mathematical structure, which we derived from a form, with similar five axioms. They also have five axioms, all of which are the same, except for their first axiom, which is:

Axiom. Groups and group homomorphisms, under composition of homomorphisms, form a category (called the *category of groups*). Furthermore, for each group G, the subgroups of G together with subgroup inclusions form a poset $\mathsf{Sub}G$; for each homomorphism $f\colon X \to Y$ the direct and inverse image maps form a monotone Galois connection and this defines a functor from the category of posets and Galois connections.

Our way of starting with a Noetherian form, satisfies this axiom. It follows from the following proposition which is an immediate consequence from how we defined direct and inverse image maps.

Proposition 3. *For each morphism $f\colon G \to H$ in $\mathbb{C}$, $f\colon \mathsf{sub}G \to \mathsf{sub}H$ and $f^{-1}\colon \mathsf{sub}H \to \mathsf{sub}G$ forms a monotone Galois connection.*

Proof. For any $X \in \mathsf{sub}G$ and $Y \in \mathsf{sub}H$, we have

$$fX \leq Y \quad \Leftrightarrow \quad \exists_{g\colon X \to Y}(Fg = f) \quad \Leftrightarrow \quad X \leq f^{-1}Y.$$

□

Also, starting with the way it is done in [4], there is a Noetherian form such that all the structure defined through the form coincides with their starting structure. It is the following form: $S\colon \mathbb{C}_2 \to \mathbb{C}$, where objects of $\mathbb{C}_2$ are pairs (G, X) where G is a group and X is a subgroup of G. Morphisms $f\colon (G, X) \to (H, Y)$ are group morphisms $f\colon G \to H$ such that $fX \leq Y$. Composition is compositions of group morphisms. S is defined on objects as $S(G, X) = G$ and on morphisms as $Sf = f$.

So it doesn't matter with which way we start, we will get the same results either way.

For a Noetherian form, since all the new structure was defined using the categorical structure, they have categorical duals. The resulting duality will coincide with the duality described in [4]. Take a form $F\colon \mathbb{B} \to \mathbb{C}$. The dual functor $F^{\mathrm{op}}\colon \mathbb{B}^{\mathrm{op}} \to \mathbb{C}^{\mathrm{op}}$ is also a form. Also, G is an object of $\mathbb{C}$ if and only if G is an object of $\mathbb{C}^{\mathrm{op}}$. So 'G is a group' is a self-dual statement. Similarly, how the dual functor is defined, $FX = G$ if and only if $F^{\mathrm{op}}X = G$. So 'X is a subgroup of G' is also self-dual. For subgroups X and Y, $X \leq Y$ if and only if $\exists_{g\colon X\to Y}(Fg = 1_G)$ whose dual is $\exists_{g^{\mathrm{op}}\colon Y\to X}(Fg^{\mathrm{op}} = 1_G)$. So the dual of $X \leq Y$ is $Y \leq X$. For $f\colon G \to H$ and $X \in \mathsf{sub}G$, the dual of the minimum element of

$$\{Y \in \mathsf{sub}H \mid \exists_{g\colon X\to Y} Fg = f\}$$

is the maximum element of

$$\{Y \in \mathsf{sub}H \mid \exists_{g^{\mathrm{op}}\colon Y\to X} F^{\mathrm{op}}g^{\mathrm{op}} = f^{\mathrm{op}}\},$$

thus the dual of fX is $(f^{\mathrm{op}})^{-1}X$. So the direct image map is dual to the inverse image map. From all this we can deduce that the top element (if it exists) of $\mathsf{sub}G$ is dual to the bottom element(if it exists) of $\mathsf{sub}G$, the dual of image is kernel, the dual of X being normal is X being conormal, and the dual of f is an embedding is f is a projection. We summarize this in the following table:

Expression	**Dual Expression**
G is a group	G is a group
$f\colon X \to Y$	$f\colon Y \to X$
$h = gf$	$h = fg$
$X \in \mathsf{sub}G$	$X \in \mathsf{sub}G$
$X \leq Y$	$Y \leq X$
$Y = fX$	$Y = f^{-1}X$
$X = f^{-1}Y$	$X = fY$
X largest subgroup of G	X is smallest subgroup of G
X is normal subgroup of G	X is conormal subgroup of G
f is an embedding	f is a projection

From this we see that the axioms are self-dual, and consequently the dual of a Noetherian form is a Noetherian form.

Here are some basic useful consequences that will be used further on in the thesis, whose proofs are in [4]:

(1) the direct image and inverse image preserve inclusion of subgroups. Furthermore, direct image preserves joins and inverse image preserves meets;

(2) the direct image of the trivial subgroup is trivial, and inverse image of the top subgroup, is the top subgroup;

(3) the direct and inverse image maps of an isomorphism are the same as the inverse and direct image maps, respectively, of its inverse;

(4) join of conormal subgroups is conormal, and meet of normal subgroups is normal;

(5) any embedding is a monomorphism, and any projection is an epimorphism;

(6) any embedding is an embedding of its image, and any projection is a projection of its kernel;

(7) a morphism is an isomorphism if and only if it is both an embedding and a projection;

(8) direct images of conormal subgroups, are conormal subgroups, and inverse images of normal subgroups, are normal subgroups;

(9) inverse images of conormal subgroups along embeddings, are conormal subgroups, and direct images of normal subgroups along projections, are normal subgroups;

(10) a morphism is an embedding if and only if it has trivial kernel. And, a morphism is a projection if and only if its image is the top element;

(11) composition of embeddings is an embedding, and composition of projections is a projection;

(12) if for any composable f and g, fg is an embedding, then g is an embedding, and if fg is a projection, then f is a projection;

(13) conormal subgroups are stable under inverse images along embeddings, and normal subgroups are stable under direct images along projections;

(14) If fg is an embedding, then g is an embedding. And dually, if fg is a projection, then f is a projection;

(15) in any group, for any subgroup X, $\overline{X}$ is the smallest normal subgroup containing X, and $\underline{X}$ is the largest conormal subgroup contained in X.

As noted somewhere before, this context allows one to establish the isomorphism theorems in groups. Quotients are defined as follows:

Definition 7. For any group G and subgroups X and Y such that $X \leq Y$, Y/X will denote the codomain of $r_{l_Y^{-1}X}$.

We will only make use of the Second Isomorphism Theorem.

Theorem 4. *Consider two subgroups A and B of a group G. If B is conormal and $A \lhd A \vee B$, then $A \wedge B \lhd B$ and there is an isomorphism*

$$B/(A \wedge B) \cong (A \vee B)/A.$$

To prove this directly here is going to be too long. For an elegant see [4].

In [4], they proved a so called "restricted modular law". In their proof the author noticed, that they proved something stronger, which isn't stated in the paper.

Proposition 5. *For a morphism f and a subgroup X below the image of f and a normal subgroup N of the codomain of f, we have*

$$f^{-1}(X \vee N) = f^{-1}X \vee f^{-1}N.$$

Proof. Suppose $N = g^{-1}0$, where g is some morphism. We have

$$\begin{aligned} f^{-1}X \vee f^{-1}N =& f^{-1}X \vee f^{-1}g^{-1}0 \\ =& f^{-1}X \vee (gf)^{-1}0 \\ =& (gf)^{-1}(gf)f^{-1}X \\ =& f^{-1}g^{-1}gff^{-1}X \\ =& f^{-1}g^{-1}gX \\ =& f^{-1}(X \vee g^{-1}0) \\ =& f^{-1}(X \vee N). \end{aligned}$$

□

Here is the restricted modular law:

Lemma 6. *For any three subgroups X, Y, and Z of a group G, if Y is normal and Z is conormal, then*

$$X \leq Z \quad \Rightarrow \quad X \vee (Y \wedge Z) = (X \vee Y) \wedge Z.$$

Dually, if Y is conormal and X is normal, then

$$X \leq Z \quad \Rightarrow \quad X \vee (Y \wedge Z) = (X \vee Y) \wedge Z.$$

Proof. Assume $Y = g^{-1}0$ and $Z = f1$ for some morphisms g and f. Suppose $X \leq Z$. We have

$$\begin{aligned} X \vee (Y \wedge Z) =& X \vee (g^{-1}0 \wedge f1) \\ =& ff^{-1}X \vee ff^{-1}g^{-1}0 \\ =& f(f^{-1}X \vee f^{-1}g^{-1}0) \\ =& ff^{-1}(X \vee g^{-1}0) \\ =& (X \vee g^{-1}0) \wedge f1 \\ =& (X \vee Y) \wedge Z. \end{aligned}$$

□

We sometimes have pushouts and pullbacks.

Lemma 7. *For any projection $f\colon A \to B$ and any morphism $g\colon A \to C$, the diagram*

$$\begin{tikzcd} & B \arrow[dr, "p"] & \\ A \arrow[ur, "f"] \arrow[dr, "g"'] & & D \\ & C \arrow[ur, "q"'] & \end{tikzcd}$$

where q is the projection of $gf^{-1}0$, and p is the unique morphism making the diagram commute (since qg sends $f^{-1}0$ to 0 and f is a projection of its kernel), is a pushout of f and g.

Proof. Take any $u\colon B \to W$ and $v\colon C \to W$ such that $uf = vg$. Consider diagram

$$\begin{tikzcd} & B \arrow[dr, "p"] \arrow[drr, bend left, "u"] & & \\ A \arrow[ur, "f"] \arrow[dr, "g"'] & & D \arrow[r, dashed, "h"] & W \\ & C \arrow[ur, "q"'] \arrow[urr, bend right, "v"'] & & \end{tikzcd}$$

We have

$$v(gf^{-1}0) = uff^{-1}0 = 0.$$

Thus there is a unique morphism $h\colon D \to W$ such that $hq = v$. We also have

$$hpf = hqg = vg = uf.$$

Which implies $hp = u$, since f is a projection (thus in particular an epimorphism). And since h is unique such, the original diagram is a pushout diagram. $\square$

Chapter 2

Normed Projective Group Theory

2.1 Normed Noetherian Forms

In this section we propose a possible way to define a norm function on a form. Intuitively, if a category equipped with a Noetherian form represents groups, then adding this additional structure should represent finite groups. We will first define a norm function. Next we will show that there are equivalent ways to define the axioms. After that, deduce some basic results, and give a possible definition of a cyclic group in this context.

Throughout this section we will fix a (multiplicative) abelian group Q. Furthermore, we will also work with a fix Noetherian form $F\colon \mathbb{B} \to \mathbb{C}$ equipped with a "norm function". The norm function is the following (and the axioms it satisfy will immediately follow):

Definition 8. A *norm* function on F, is a function which assigns to each subgroup S an element an element $\|S\|$ of Q. The *order* of a group G is $|G| = \frac{\|1\|}{\|0\|}$.

The duality is extended further as:

	Expression	**Dual Expression**
For any $a, b \in Q$	$a \cdot b$	$a \cdot b$
For any subgroup G	$\|G\|$	$\|G\|$

That is the group operations and the norm of a subgroup doesn't change under duality. Consequently, the dual of the order of a group is the reciprocal of the order of the same group.

Axiom 6. For any morphism $f\colon X \to Y$, and for any subgroups A and B above the kernel of f, we have

$$\frac{\|fA\|}{\|fB\|} = \frac{\|A\|}{\|B\|}.$$

Axiom 7. If A and B are both normal or both conormal subgroups of the same group such that $A \leq B$ and $\|A\| = \|B\|$, then $A = B$.

Definition 9. A Noetherian form equipped with a norm function, will be called a *normed* Noetherian form.

Axiom 6 is true in usual finite group theory, where the norm function $\|-\|$ is just the usual cardinality function $|-|$: If $f\colon X \to Y$ is a group homomorphism between two finite groups, and A is a subgroup of X which is above the kernel N of f, then the restriction of f, $f'\colon A \to Y$, has the same kernel N. Thus $|fA| = |f'A| = \frac{|A|}{|N|}$. Similarly for B above the kernel of f, $|fB| = \frac{|B|}{|N|}$. Then divide these two equations with each other. The $|N|$'s will cancel out, and what will remain, is the equation in Axiom 6. Axiom 7 is also true in usual finite group theory.

Axiom 7 is self-dual. Axiom 6 isn't self-dual, but it is equivalent to its dual. The next theorem shows this, where 1. is the statement of Axiom 6 and 2. is its dual.

Theorem 8. *The following are equivalent:*

(1) For any $f\colon X \to Y$ and subgroups A and B above the kernel of f, we have

$$\frac{\|fA\|}{\|fB\|} = \frac{\|A\|}{\|B\|};$$

(2) for any $f\colon X \to Y$ and subgroups A and B below the image of f, we have

$$\frac{\|f^{-1}A\|}{\|f^{-1}B\|} = \frac{\|A\|}{\|B\|};$$

(3) for any morphism $f\colon X \to Y$ and subgroups A of X and B of Y, we have

$$\|fA\|\|f^{-1}B\| = \|A \vee \mathsf{Ker}f\|\|B \wedge \mathsf{Im}f\|.$$

Proof. Suppose 1. holds. Take any morphism $f\colon X \to Y$ and subgroups A and B above the image of f. Then we have

$$\frac{\|A\|}{\|B\|} = \frac{\|ff^{-1}A\|}{\|ff^{-1}B\|} = \frac{\|f^{-1}A\|}{\|f^{-1}B\|}.$$

Thus 1. implies 2.

Suppose 2. holds. Take any morphism $f\colon X \to Y$ and subgroups A of X and B of Y. Then we have

$$\frac{\|f^{-1}fA\|}{\|f^{-1}B\|} = \frac{\|f^{-1}fA\|}{\|f^{-1}ff^{-1}B\|} = \frac{\|fA\|}{\|ff^{-1}B\|},$$

from which it follows, that

$$\|fA\|\|f^{-1}B\| = \|A \vee \mathsf{Ker}f\|\|B \wedge \mathsf{Im}f\|.$$

Thus 2. implies 3.

Suppose 3. holds. Take any morphism $f\colon X \to Y$ and subgroups A and B above the kernel of f. We have

$$\|fA\|\|1^X\| = \|fA\|\|f^{-1}1^Y\| = \|A \vee \mathsf{Ker}f\|\|1^Y \wedge \mathsf{Im}f\| = \|A\|\|\mathsf{Im}f\|.$$

Similarly we have $\|fB\|\|1^Y\| = \|B\|\|\mathsf{Im}f\|$. Dividing these two equations and canceling common factors, we get

$$\frac{\|fA\|}{\|fB\|} = \frac{\|A\|}{\|B\|}.$$

So 3. implies 1.

Thus everything is equivalent. $\square$

Corollary 9. *For any morphism $f\colon X \to Y$, we have*

$$\|\mathsf{Im}f\|\|\mathsf{Ker}f\| = \|1^X\|\,\|0^Y\|\,.$$

Corollary 10. *If A is a conormal subgroup of X, then*

$$|A| = \frac{\|A\|}{\|0^X\|}.$$

And dually, if A is a normal subgroup of X, then

$$|X/A| = \frac{\|1^X\|}{\|A\|}.$$

Proof. Suppose A is conormal. Let $l\colon A \to X$ an embedding of A. We have

$$|A| = \frac{\|1^A\|}{\|0^A\|} = \frac{\|l^{-1}l1^A\|}{\|l^{-1}l0^A\|} = \frac{\|l1^A\|}{\|l0^A\|} = \frac{\|A\|}{\|0^X\|}.$$

$\square$

When assuming Axiom 6 holds, there is also an equivalence with Axiom 7.

Theorem 11. *The following are equivalent:*

(1) *If A and B are both normal or both conormal subgroups of the same group such that $A \leq B$ and $\|A\| = \|B\|$, then $A = B$;*

(2) *for any two groups X and Y such that $|X| = |Y|$, if $f\colon X \to Y$ is an embedding, then f is an isomorphism, and also if $g\colon X \to Y$ is a projection, then g is an isomorphism.*

Proof. Suppose 1. holds. Take any embedding $f\colon X \to Y$, where $|X| = |Y|$. We have

$$\frac{\|f1^X\|}{\|f0^X\|} = \frac{\|1^X\|}{\|0^X\|} = \frac{\|1^Y\|}{\|0^Y\|}.$$

Thus $\|f1^X\| = \|1^Y\|$, and thus $f1^X = 1^Y$. Thus f is an isomorphism. A dual argument will show that any projection $g\colon X \to Y$, where $|X| = |Y|$ is an isomorphism.

Suppose 2. holds. Take any conormal subgroups A and B of the same group G, such that $A \leq B$ and $\|A\| = \|B\|$. Let $l_A \colon A \to G$ and $l_B \colon B \to G$ be the respective embeddings of A and B. Since $A \leq B$, there is an $h \colon A \to B$, such that $l_A = l_B h$. h is also an embedding. We have

$$|A| = \frac{\|A\|}{\|0^G\|} = \frac{\|B\|}{\|0^G\|} = |B|.$$

Thus h is an isomorphism. And thus $A = B$. A dual argument will show that if A and B are both normal subgroups of the same group, such that $A \leq B$ and $\|A\| = \|B\|$, then $A = B$. $\square$

The following three results, are just results that one would might expect to be true.

Proposition 12. *If X is isomorphic to Y, then $|X| = |Y|$.*

Proof. Suppose that $f \colon X \to Y$ is an isomorphism. Then we have

$$|X| = \frac{\|1^X\|}{\|0^X\|} = \frac{\|f1^X\|}{\|f0^X\|} = \frac{\|1^Y\|}{\|0^Y\|} = |Y|,$$

Where 1^X and 0^X are the top and bottom subgroups of X respectively, and similarly for 1^Y and 0^Y. $\square$

Proposition 13. *If $f \colon X \to Y$ and $g \colon Y \to X$ are embeddings, then $X \cong Y$.*

Proof. $gf \colon X \to X$ is an embedding, thus is an isomorphism. Thus g is also a projection. Thus g is an isomorphism. $\square$

Theorem 14. *If the following is a short exact sequence*

$$X \xrightarrow{f} Y \xrightarrow{g} Z,$$

that is $\mathsf{Im}f = \mathsf{Ker}g$*, and f is an embedding and g is a projection, then $|Y| = |X||Z|$.*

Proof. From Corollary 9 we have $\|\mathsf{Im}f\|\|\mathsf{Ker}f\| = \left\|1^X\right\| \left\|0^Y\right\|$, or equivalently,

$$\frac{\|\mathsf{Im}f\|}{\|0^Y\|} = \frac{\left\|1^X\right\|}{\|\mathsf{Ker}f\|}.$$

Similarly we have

$$\frac{\|\mathsf{Im}g\|}{\|0^Z\|} = \frac{\left\|1^Y\right\|}{\|\mathsf{Ker}g\|}.$$

Then we have

$$|X||Z| = \frac{\left\|1^X\right\|}{\|0^X\|}\frac{\left\|1^Z\right\|}{\|0^Z\|} = \frac{\left\|1^X\right\|}{\|\mathsf{Ker}f\|}\frac{\|\mathsf{Im}g\|}{\|0^Z\|} = \frac{\|\mathsf{Im}f\|}{\|0^Y\|}\frac{\left\|1^Y\right\|}{\|\mathsf{Ker}g\|} = \frac{\left\|1^Y\right\|}{\|0^Y\|} = |Y|.$$

$\square$

A further thing one could do, is to fix a submonoid N of the codomain Q of the norm function, so that we could define when the norm of one subgroup divides the norm of another subgroup. The divisibility relation is defined as follows:

Definition 10. The divisibility relation, denoted by $\leq$ is defined on Q as, for any $a, b \in Q$,

$$a \leq b \quad \Leftrightarrow \quad ba^{-1} \in N.$$

With this, we could give an attempt to define cyclic groups:

Definition 11. Group G is *cyclic* if for any $A, B \in \mathsf{sub}(G)$, we have

$$\|A\| \leq \|B\| \Rightarrow A \leq B.$$

Only two elementary results have been found so far:

Theorem 15. *For a cyclic group G, if $m\colon M \to G$ is an embedding, then M is cyclic as well.*

Proof. Take any $A, B \in \mathsf{sub}(G)$ such that $\|A\| \leq \|B\|$. Then, by axiom 6 we have

$$\frac{\|B\|}{\|A\|} = \frac{\|mA\|}{\|mB\|}.$$

Since the left hand side is in N, the right hand side is also in N. Thus $mA \leq mB$, thus $A \leq B$, thus M is cyclic. □

Dually we get:

Theorem 16. *For a cyclic group G, if $e\colon G \to E$ is a projection, then E is cyclic as well.*

Theorem 86 show in particular that the above definition is equivalent to a finite group being cyclic. Theorem 86 also gives other equivalent conditions to when a finite group is cyclic.

2.2 Examples of Normed Noetherian Forms

The aim of this section is to create examples from known structures in such a way that for a suitable well-known structure, the resulting example is the usual finite cyclic groups.

We are going to create examples from cancellable commutative monoids with some additional structure which will imitate the modular relations on the integers. First, we are going to deduce some basic results about these monoids, then add a bit of structure.

Since we will start with a cancellable commutative monoid and the codomain of the normed function must be an abelian group, we will construct an abelian group containing the monoid. The following proposition gives a construction. This construction is essentially the same as the construction of fields from integral domains (that is, if one 'forgets' about the addition structure on integral domains and fields), which could be found in most undergraduate algebra textbooks for example in Mac Lane and Birkhoff's algebra book [8].

Proposition 17. *If N is a cancellable commutative monoid, then N could be extended to an abelian group Q whose elements are of the form ab^{-1} for $a, b \in N$.*

Proof. Define a relation R on monoid $N \times N$ by

$$(a, b)R(c, d) \quad \Leftrightarrow \quad ad = bc.$$

R is a congruence: only transitivity doesn't follow immediately. Suppose

$$(a, b)R(c, d)R(e, f).$$

Then we have

$$afc = ade = bce = bec.$$

Canceling c, we get $af = be$, thus $(a, b)R(e, f)$.

Since R is a congruence, $Q = (N \times N)/R$ is a commutative monoid with unit $1 = (1, 1)$.

Moreover for any $(a, b) \in Q$, we have

$$(a, b)(b, a) = (ab, ab) = (1, 1).$$

So Q is an abelian group.

The function $i\colon N \to Q$, defined by $a \mapsto (a, 1)$, is a morphism. Since $(a, 1) = (b, 1)$ if and only if $a1 = b1$, i is injective. Thus Q is an extension of N, which is an abelian group.

If we represent each $(a, 1)$ is Q by a, then $(1, a) = a^{-1}$. Thus for any element (a, b) in Q,

$$(a, b) = ab^{-1}.$$

Thus Q is a required abelian group. $\square$

The definition of a "divisibility relation" on a monoid might be clear, but just for completeness, here is the definition:

Definition 12. For a monoid N, the *divisibility* relation $\leq$ on N, is defined as, for any $a, b \in N$,

$$a \leq b \quad \text{if and only if} \quad an = b \text{ for some } n \in N$$

The notation $a \geq b$ will be sometimes used as an alternative way to write $b \leq a$.

For the rest of this section, N will be a fixed commutative cancellable monoid which forms a lattice under the divisibility relation, and Q will be an abelian group as described in the proposition before the above definition. The meets and joins in N will be denoted by $\wedge$ and $\vee$ respectively.

The following proposition is just for interest sake, and not useful for the rest of this section.

Proposition 18. *In a left cancellable monoid N, the divisibility relation is anti-symmetric if and only if $\forall_{a,b\in N}(ab = 1 \Rightarrow a = b = 1)$.*

Proof. Suppose $\leq$ is anti-symmetric, and $ab = 1$. Then $a \leq 1$, but also $1 \leq a$. Therefore, by anti-symmetry of $\leq$, $a = 1$. Thus also $b = 1$.

Suppose for any $a, b \in N$, if $ab = 1$ then $a = b = 1$. Suppose $x \leq y$ and $y \leq x$. Then there is some a, b in N such that, $xa = y$ and $yb = x$. Then $xab = x$, and so $ab = 1$, and so $a = 1$. Thus $x = y$, and thus $\leq$ is anti-symmetric. □

Notice that if $a \leq b$, then $\frac{b}{a} = ba^{-1}$ is in N (it is the unique element n such that $an = b$).

We have some basic results:

Lemma 19. *For $a, b, c, d \in N$, we have*

(1) If $a \leq b$ and $c \leq d$, then $ac \leq bd$;

(2) $a \leq b$ if and only if $ac \leq bc$.

(3) if $b, c \leq a$, then $b \leq c$ if and only if $\frac{a}{c} \leq \frac{a}{b}$.

Notice that for the opposite of $\leq$,

$$a \leq^{\text{op}} b \quad \Leftrightarrow \quad b \leq a \quad \Leftrightarrow \quad \exists_{n\in N}(an = b).$$

From this, we can see that $\leq^{\text{op}}$ will also satisfy the above lemma. So anything we deduce just from making use of the above lemma (and also that N is a lattice under $\leq$), the dual (that is, replace $a \leq b$ with $b \leq a$, $\wedge$ with $\vee$, and $\vee$ with $\wedge$) will also be true.

Further basic results:

Lemma 20. *For any $a, b, c, d \in N$, we have*

(1) If $d \leq a, b$, then

$$\frac{a \wedge b}{d} = \frac{a}{d} \wedge \frac{b}{d}$$

(2) $c(a \wedge b) = (ca) \wedge (cb)$

(3) If $d \leq a, b$, then

$$\frac{a \vee b}{d} = \frac{a}{d} \vee \frac{b}{d}$$

(4) $c(a \vee b) = ca \vee cb$

(5) $(a \wedge b)(a \vee b) = ab$

(6) If $c, d \leq a$, then $\frac{a}{c} \wedge \frac{a}{d} = \frac{a}{c \vee d}$.

(7) If $c, d \leq a$, then $\frac{a}{c} \vee \frac{a}{d} = \frac{a}{c \wedge d}$.

(8) If $a \wedge b = 1$ and $a \leq bc$, then $a \leq c$

(9) If $a \wedge c = 1$, then $ad \wedge c = d \wedge c$.

(10) If $a \wedge c = b \wedge c$, then $ad \wedge c = bd \wedge c$.

Proof. (1) We have $\frac{a \wedge b}{d} \leq \frac{a}{d} \wedge \frac{b}{d}$. We also have

$$d\left(\frac{a}{d} \wedge \frac{b}{d}\right) \leq d\frac{a}{d} = a.$$

And similarly $d\left(\frac{a}{d} \wedge \frac{b}{d}\right) \leq b$. Thus $d\left(\frac{a}{d} \wedge \frac{b}{d}\right) \leq a \wedge b$. By dividing by d and using the fact that $\leq$ is anti-symmetric, the result follows.

(2) We have

$$\frac{(ac) \wedge (bc)}{c} = \frac{ac}{c} \wedge \frac{bc}{c} = a \wedge b.$$

Thus $(ac) \wedge (bc) = c(a \wedge b)$.

(3) By duality, it is true.

(4) By duality, it is true.

(5) We have

$$\begin{aligned}(a \wedge b)(a \vee b) &= a(a \wedge b) \vee b(a \wedge b) \\ &= (aa \wedge ab) \vee (ab \wedge bb) \\ &\leq ab \vee ab = ab\end{aligned}$$

By duality we have $(a \vee b)(a \wedge b) \geq ab$. Thus, by the anti-symmetry, the result follows.

(6) We have from (5), $\left(\frac{a}{c} \vee \frac{a}{d}\right)\left(\frac{a}{c} \wedge \frac{a}{d}\right) = \frac{a^2}{cd}$. Multiplying both sides by cd, we get

$$\begin{aligned}a^2 &= cd\left(\frac{a}{c} \vee \frac{a}{d}\right)\left(\frac{a}{c} \wedge \frac{a}{d}\right) \\ &= (ac \vee ad)\left(\frac{a}{c} \wedge \frac{a}{d}\right) \\ &= a(c \vee d)\left(\frac{a}{c} \wedge \frac{a}{d}\right)\end{aligned}$$

Canceling an a on both sides and dividing both sides by $(c \vee d)$ (since $c \vee d \leq a$), we get the result.

(7) By duality, it is true.

(8) Since $a \wedge c = 1$, we have $(ab) \wedge (bc) = b$. Since $a \leq ab$ and $a \leq bc$, we have $a \leq b$.

(9) We have $d \wedge c \leq ad \wedge c$. Since $a \wedge c = 1$, we also have $(ad \wedge c) \wedge a = 1$. So $(ad \wedge c) \leq ad$ implies $ad \wedge c \leq d$. Since we have $ad \wedge c \leq c$ as well, $ad \wedge c \leq d \wedge c$.

(10) Suppose $a \wedge c = b \wedge c$. Then by using (9) we have

$$ad \wedge c = (a \wedge c)\left(\frac{a}{a \wedge c} d \wedge \frac{c}{a \wedge c}\right) = (a \wedge c)\left(d \wedge \frac{c}{a \wedge c}\right) = (b \wedge c)\left(d \wedge \frac{c}{b \wedge c}\right) = bd \wedge c.$$

□

Proposition 21. *For a commutative cancellable monoid N, if it is a lattice under the divisibility relation, then it is a distributive lattice.*

Proof. By using the previous lemma, we have

$$\begin{aligned}(a \wedge (b \wedge c))(a \vee (b \wedge c)) &= a(b \wedge c)\\ &= ab \wedge ac\\ &= (a \wedge b)(a \vee b) \wedge (a \wedge c)(a \vee c)\\ &\geq (a \wedge b \wedge c)(a \vee b) \wedge (a \wedge b \wedge c)(a \vee c)\\ &= (a \wedge b \wedge c)((a \vee b) \wedge (a \vee c))\end{aligned}$$

So $a \vee (b \wedge c) \geq (a \vee b) \wedge (a \vee c)$. Thus $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
By duality, we have $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$. □

The added structure to the monoid N is the following:

Definition 13. A *modular structure* is a commutative cancellable monoid N equiped with a family of equivalence relations $(\equiv_n)_{n \in N}$ satisfying the following,

(1) N is a lattice under the divisibility relation $\leq$;

(2) $x \equiv_a a$ if and only if $a \leq x$;

(3) $\equiv_a \subseteq \equiv_b$ if and only if $b \leq a$;

(4) $x \equiv_a y$ if and only if $bx \equiv_{ba} by$.

From (3) and (4), we see that these equivalence relations are congruences.
The equivalence class of x under the relation $\equiv_n$, will be denoted by $[x]_n$.

Lemma 22. *For a given modular structure N, if $k \equiv_m l$, then $k \wedge m = l \wedge m$.*

Proof.
Since $(k \wedge m) \leq m$, we have $k \equiv_{k \wedge m} l$. Since $k \wedge m \leq k$ and $\equiv_{k \wedge m}$ is transitive, we have $l \equiv_{k \wedge m} k \wedge m$. Thus $k \wedge m \leq l$. So we get $k \wedge m \leq l \wedge m$. And similarly, $l \wedge m \leq k \wedge m$. Thus $k \wedge m = l \wedge m$. □

Now for the construction: Here the notation k_* and k^* will be used for the direct and inverse image maps of a morphism k. This notation is used to make it clear what are maps and what are subgroups (since most things will just be elements of N).

Theorem 23. *From a given modular structure N, we can create two categories $\mathbb{B}$ and $\mathbb{C}$ as follows:*

	$\mathbb{B}$	$\mathbb{C}$
Objects	(n, a), *where* $a \leq n$	n
Morphisms	$[k]_m \colon (n, a) \to (m, b)$, *where* $m \leq kn$ *and* $am \leq bkn$.	$[k]_m \colon n \to m$, *where* $k \in N$ *and* $m \leq kn$
Composition	$[k]_m \circ [l]_r = [kl]_r$	$[k]_m \circ [l]_r = [kl]_r$
Identity Morphisms	$[1]_n \colon n \to n$	$[1]_n \colon n \to n$

For simplicity, we'll denote morphisms by representatives.

Then we can construct a Noetherian form as: $F \colon \mathbb{B} \to \mathbb{C}$, defined on objects as $F(n, a) = n$ and on morphisms as $F(k) = k$.

The arising structure will be:

Groups	*Elements of N.*
Subgroups	*For any $n \in N$, the subgroups of n are the divisors of n.*
Subgroup Inclusion	*For subgroups a and b of n, a is contained in b as subgroups if and only if a divides b.*
Morphisms	*For $n, m \in N$, the set of all homomorphisms from n to m, is the set of all equivalence classes $[k]_m$ such that $m \leq kn$.*
Composition	*For any $k \colon n \to m$ and $l \colon m \to r$, the composite is $l \circ k = kl$.*
Direct Image	*For $k \colon n \to m$, the direct image is defined by, for $a \leq n$,* $$k_*(a) = \frac{am}{am \wedge kn}.$$
Inverse Image	*For $k \colon n \to m$, the inverse image is defined by, for $b \leq m$,* $$k^*(b) = \frac{bkn \wedge mn}{m}.$$

For any group n and subgroup a, the embedding of a will be

$$\frac{n}{a} \colon a \to n,$$

and the projection of a will be

$$1 \colon n \to \frac{n}{a},$$

and from this follows that all subgroups are both normal and conormal.

We can construct an abelian group Q from N, by Proposition 17. Then, we can define a norm function, with codomain Q, mapping each subgroup a to a, that is, $\|a\| = a$

The proof isn't particularly deep or intricate, but it is a few pages long, since there are so many details that needs to be verified.

Proof. <u>$\mathbb{C}$ is a category:</u>

Morphisms are well-defined: Suppose $k \equiv_m k'$. Then $kn \equiv_m k'n$. So $[m]_m = [kn]_m$ if and only if $[m]_m = [k'n]_m$, that is $m \leq kn$ if and only if $m \leq k'n$. So $k\colon n \to m$ is a morphism if and only if $l\colon n \to m$ is a morphism. So morphisms are well-defined

Composition is well-defined: Suppose $k\colon n \to m$ and $l\colon m \to r$ are morphisms. Suppose $k \equiv_m k'$ and $l \equiv_r l'$. Since $l \equiv_r l'$, we have $lk' \equiv_r l'k'$. Also, Since $k \equiv_m k'$, $kl \equiv_{ml} k'l$, and so $kl \equiv_r k'l$ since $r \leq lm$. And so by transitivity, $kl \equiv_r k'l'$. And so, composition is well-defined.

Composition is associative, with identity morphisms of the form $[1]_n$, since N is a monoid with identity 1.

<u>$\mathbb{B}$ is a category:</u>

The morphisms are the same as in $\mathbb{C}$ with the same composition, except that it has an extra condition. To to check whether morphisms and composition are well-defined, we only need to check this extra condition. Suppose $l \equiv_m k$. Then, for any $a, b, n, m \in N$ such that $a \leq n$ and $b \leq m$, we have

$$\begin{aligned}
& am \leq bkn \\
\Leftrightarrow\ & \frac{m}{k \wedge m} \leq b\frac{k}{k \wedge m}\frac{n}{a} \\
\Leftrightarrow\ & \frac{m}{k \wedge m} \leq b\frac{n}{a} \\
\Leftrightarrow\ & \frac{m}{l \wedge m} \leq b\frac{n}{a} \\
\Leftrightarrow\ & am \leq bln.
\end{aligned}$$

So $k\colon (n,a) \to (m,b)$ is a morphism if and only if $l\colon (n,a) \to (m,b)$ is a morphism. So morphisms are well-defined. To show that composition is well-defined, take any pair of morphisms $k\colon (n,a) \to (m,b)$ and $l\colon (m,b) \to (o,c)$. So $am \leq bkn$ and $bo \leq clm$. Multiplying them together, we get $abmo \leq bcklmn$. Canceling bm on both sides, we get $ao \leq c(kl)n$. So $kl\colon (n,a) \to (o,c)$ is a morphism. So composition is well-defined.

And just as for $\mathbb{C}$, this does indeed form a category.

<u>F is a form:</u>

It is clear to see from the definition of F, that F is a form.

<u>Groups:</u>

The groups are objects of $\mathbb{C}$. Thus the groups are elements of N.

<u>Subgroups:</u>

Take any group n. The subgroups of n are all the elements of the form (n,a) where $a \leq n$. Thus the subgroups of n are essentially the divisors of n. For simplicity, subgroups (n,a) will mostly be denoted as a.

<u>Subgroup Inclusion:</u>

Notice that for any $l\colon (n,a) \to (m,b)$, if $Fl = k$, then $k = l$. So the statement $\exists_{l\colon (n,a)\to(m,b)}(Fl = k)$ is the same as $k\colon (n,a) \to (m,b)$ is a morphism, which is the same as $am \leq bkn$.

<u>Axiom 1:</u>

Since for any n, $1 \leq n$, so $(n,1) \in \mathbb{B}$ and $F(n,1) = n$. So F is surjective on objects.

Take any $k\colon n \to m$ in $\mathbb{C}$ and any subgroup a of n. Consider the set

$$S = \{b \leq m \mid am \leq bkn\}.$$

Since

$$am \leq am\frac{kn}{am \wedge kn} = \frac{am}{am \wedge kn}kn,$$

and

$$\frac{am}{am \wedge kn} \leq \frac{am}{am \wedge ka} = \frac{m}{m \wedge k} \leq m,$$

$\frac{am}{am\wedge kn} \in S$. Also, for any $b \in S$ we have

$$\begin{aligned} & am \leq bkm \\ \Rightarrow\ & \frac{am}{am \wedge kn} \leq b\frac{kn}{am \wedge kn} \\ \Rightarrow\ & \frac{am}{am \wedge kn} \leq b. \end{aligned}$$

Thus S has a minimum element $\frac{am}{am\wedge kn} = k_*a$.

Also, for $k \leq n \to m$ in $\mathbb{C}$ and any subgroup b of m, consider the set

$$S = \{a \leq n \mid am \leq bkn\}.$$

We have

$$\frac{bkn \wedge mn}{m}m = bkn \wedge mn \leq bkn,$$

and

$$\frac{bkn \wedge mn}{m} \leq \frac{mkn \wedge mn}{m} = kn \wedge n = n.$$

So $\frac{bkm\wedge mn}{m}$ is in S. Take any $a \in S$. Then we have

$$\begin{aligned} & am \leq bkn \\ \Rightarrow\ & am \leq bkn \wedge mn \\ \Rightarrow\ & a \leq \frac{bkn \wedge mn}{m}. \end{aligned}$$

So S has a maximum element $\frac{bkn\wedge mn}{m} = k^*b$.

Axiom 2:

For each n, $\mathsf{sub}(n)$ is a bounded lattice (under the divisibility relation), with top element n and bottom element 1. For any morphism $k\colon n \to m$, and any $a \leq n$ and $b \leq m$, we have

$$\begin{aligned}
k^*(k_*(a)) &= k^*\left(\frac{am}{am \wedge kn}\right) \\
&= \frac{(\frac{am}{am \wedge kn})kn \wedge mn}{m} \\
&= \frac{(am \vee kn) \wedge mn}{m} \\
&= \frac{(am \wedge mn) \vee (kn \wedge mn)}{m} \\
&= \frac{am \vee (kn \wedge mn)}{m} \\
&= a \vee \frac{kn \wedge mn}{m} \\
&= a \vee \mathsf{Ker}k,
\end{aligned}$$

$$\begin{aligned}
k_*(k^*(b)) &= k_*\left(\frac{bkn \wedge mn}{m}\right) \\
&= \frac{(\frac{bkn \wedge mn}{m})m}{(\frac{bkn \wedge mn}{m})m \wedge kn} \\
&= \frac{bkn \wedge mn}{bkn \wedge mn \wedge kn} \\
&= \frac{bk \wedge m}{bk \wedge m \wedge k} \\
&= \frac{bk \wedge m}{k \wedge m} \\
&= b\frac{k}{k \wedge m} \wedge \frac{m}{k \wedge m} \\
&= b \wedge \frac{m}{k \wedge m} \\
&= b \wedge \mathsf{Im}k.
\end{aligned}$$

Axiom 3:

Take any group n. For any subgroup a, consider the morphism $\frac{n}{a}\colon a \to n$. We have,

$$\mathsf{Im}\frac{n}{a} = \frac{an}{an \wedge \frac{n}{a}a} = a.$$

Suppose $k\colon m \to n$ is an arbitrary morphism such that $\mathsf{Im}k \leq a$. We have the following,

$$\begin{aligned}
\mathsf{Im}k \leq a &\Leftrightarrow \frac{n}{n \wedge k} \leq a \\
&\Rightarrow n \leq a(k \wedge n) \leq ak.
\end{aligned}$$

So $\frac{ak}{n}$ is in N. We also have the following,

$$\frac{ak}{n}m = a\frac{km}{n}.$$

The fraction $\frac{km}{n}$ exists since $k\colon m \to n$ is a morphism. Also, this computation shows that $\frac{ak}{n}\colon m \to a$ is a morphism. For this morphism, we have,

$$\frac{ak}{n}\frac{n}{a} = k.$$

Suppose $l\colon m \to a$ is morphism such that $l\frac{n}{a} = k$. We have the following,

$$\begin{aligned}\frac{ln}{a} = k &\Rightarrow \frac{ln}{a} \equiv_n k\\ &\Rightarrow ln \equiv_{an} ak\\ &\Rightarrow l \equiv_a \frac{ak}{n}.\end{aligned}$$

So, since both l and $\frac{ak}{m}$'s codomain is a, $l = \frac{ak}{n}$. So there is a unique morphism l such that $\frac{n}{a}l = k$. So $\frac{n}{a}$ is an embedding of a.

For the projection part of the axiom: For subgroup a of group n, consider the morphism $1\colon n \to \frac{n}{a}$. We have

$$\mathsf{Ker}1 = \frac{n \wedge \frac{n^2}{a}}{\frac{n}{a}} = \frac{an \wedge n^2}{n} = a.$$

Suppose $k\colon n \to m$ is a morphism such that $a \leq \mathsf{Ker}k$. We have

$$a \leq \mathsf{Ker}k = \frac{kn \wedge mn}{m} \leq \frac{kn}{m}.$$

By multiplying by m, then 'dividing' by a (since $a \leq n$) on both sides, we get $m \leq k\frac{n}{a}$. That shows you that $k\colon \frac{n}{a} \to m$ is a morphism. For this morphism, $1k = k$. Suppose $l\colon \frac{n}{a} \to m$ is a morphism such that $1l = k$. So $l \equiv_m k$, and since $k\colon \frac{n}{a} \to m$ is also a morphism, $l = k\colon \frac{n}{a} \to m$. So there is a unique morphism l such that $1l = k$. Thus $1\colon n \to \frac{n}{a}$ is a projection of a.

<u>Axiom 4:</u>
Take any morphism $k\colon n \to m$. The image of k is $\frac{m}{k\wedge m}$, and the kernel of k is $\frac{kn\wedge mn}{m}$. The projection of the kernel is

$$1\colon n \to \frac{n}{\frac{kn\wedge mn}{m}} = \frac{mn}{kn \wedge mn} = \frac{m}{k \wedge m}.$$

The embedding of the image is,

$$\frac{m}{\frac{m}{k\wedge m}} = k \wedge m\colon \frac{m}{k \wedge m} \to m.$$

The morphism $\frac{k}{k\wedge m}\colon \frac{m}{k\wedge m} \to \frac{m}{k\wedge m}$ is an isomorphism: It is clearly a morphism. The kernel of $\frac{k}{k\wedge m}$ is

$$\frac{\frac{k}{k\wedge m}\frac{m}{k\wedge m} \wedge (\frac{m}{k\wedge m})^2}{\frac{m}{k\wedge m}} = \frac{k}{k \wedge m} \wedge \frac{m}{k \wedge m} = 1.$$

And its image is,

$$\frac{\frac{m}{k\wedge m}}{\frac{m}{k\wedge m} \wedge \frac{k}{k\wedge m}} = \frac{\frac{m}{k\wedge m}}{1} = \frac{m}{k \wedge m}.$$

And composing these 3 morphisms, $1\colon n \to \frac{m}{k\wedge m}$ and $\frac{k}{k\wedge m}\colon \frac{m}{k\wedge m} \to \frac{m}{k\wedge m}$ and $k \wedge m\colon \frac{m}{k\wedge m} \to m$, we get k as a decomposition of the projection of its kernel and an isomorphism and the embedding of its image.

Axiom 5:

From verifying Axiom 3, we saw that all subgroups in any group are both normal and conormal. Thus this axiom trivially holds.

Norm:

Suppose $k\colon n \to m$ is a morphism, and a and b are above the kernel of k. Then

$$a \geq \mathsf{Ker}k = \frac{kn \wedge mn}{m} \quad \Rightarrow \quad am \geq (kn \wedge mn).$$

So

$$am \wedge kn = am \wedge nm \wedge kn = kn \wedge mn.$$

Similarly we get $bm \wedge kn = kn \wedge mn = am \wedge kn$. From this the first axiom of the norm follows:

$$\frac{k_*(a)}{k_*(b)} = \frac{\frac{am}{am\wedge kn}}{\frac{bm}{bm\wedge kn}} = \frac{am(bm \wedge kn)}{bm(am \wedge kn)} = \frac{a}{b}.$$

The assumption $\|A\| = \|B\|$ in the second axiom of the norm, in this case, implies $A = B$.

So $\|a\| = a$ does indeed define a norm. $\square$

Corollary 24. *All the groups above are cyclic groups in the sense of Definition 11.*

For suitable choices for N and $\equiv_n$, this construction would give rise to a form isomorphic to the "form of finite cyclic groups". The form of finite cyclic groups is the following form: Let $\mathbb{C}$ the category of finite cyclic groups, and $\mathbb{C}_2$ be the category where objects are pairs of finite cyclic groups (A, X) such that $X \leq A$, morphisms $f\colon (A, X) \to (B, Y)$ are group homomorphisms $f\colon A \to B$ such that $fX \leq Y$. Then the form of finite cyclic groups, is the form $S\colon \mathbb{S}_2 \to \mathbb{S}$, $(A, X) \mapsto A$, $f \mapsto f$.

In the theorem below, we will continue to use $\leq$ for the divisibility relation, and $\wedge$ and $\vee$ for gcd and lcm respectively. For the proof of the theorem below, note that for a subgroup $\langle a\rangle$ of $\mathbb{Z}_n$, $|\langle a\rangle| = \frac{n}{a\wedge n}$.

Theorem 25. *If we take N as the natural numbers without 0, and $\equiv_n$ to be the usual modular relations, that is $a \equiv_n b$ if and only if $n \mid (b - a)$, then the resulting form will be isomorphic to the form of finite cyclic groups.*

Proof. Let $F\colon \mathbb{B} \to \mathbb{C}$ denote the form arising from the above theorem. Define a map

$$G\colon \mathbb{S} \to \mathbb{C}, \quad \mathbb{Z}_n \mapsto n, f \mapsto f1.$$

G is a well-defined functor, which is isomorphism. Also, define a map

$$H\colon \mathbb{S}_2 \to \mathbb{B}, \quad (A, X) \mapsto (|A|, |X|), f \mapsto f1$$

H is well-defined on objects, and bijective on objects as well. For morphisms: take any $f\colon (A,X) \to (B,Y)$ in $\mathbb{S}_2$. Let $X = \left\langle \frac{|A|}{|X|} \right\rangle$. We have

$$|Y| \geq |fX| = \left| f \left\langle \frac{|A|}{|X|} \right\rangle \right| = \left| \left\langle f \frac{|A|}{|X|} \right\rangle \right| = \frac{|B|}{|B| \wedge f\frac{|A|}{|X|}}.$$

So we have

$$|B| \leq |Y|(|B| \wedge f\frac{|A|}{|X|} \leq |Y| f \frac{|A|}{|X|} = |Y| f1 \frac{|A|}{|X|}.$$

Multiplying by $|X|$ on both sides, we get $|X||B| \leq |Y|f1|A|$. Thus H is well-defined on morphisms. It is injective on morphisms, and it preserves identity morphisms and composition of morphisms. Only need to check that it is surjective on morphisms. Take any $k\colon (n,a) \to (m,b)$ in $\mathbb{B}$. Take the objects $(\mathbb{Z}_n, \langle \frac{n}{a} \rangle)$ and $(\mathbb{Z}_m, \langle \frac{m}{b} \rangle)$. Let $f\colon \mathbb{Z}_n \to \mathbb{Z}_m$ be the morphism where $f1 = k$. f is well-defined, since $m \leq kn$. Also, since $am \leq bkm$, we have

$$am \leq bkn \Rightarrow m \leq bk\frac{n}{a} \Rightarrow \frac{m}{m \wedge \frac{n}{a}k} \leq b.$$

Therefore we have

$$\left| f \left\langle \frac{n}{a} \right\rangle \right| = \left| \frac{n}{a} f1 \right| = \frac{m}{\frac{n}{a} f1 \wedge m} \leq b = \left| \left\langle \frac{m}{b} \right\rangle \right|.$$

Thus $f \langle \frac{n}{a} \rangle \leq \langle \frac{m}{b} \rangle$. Thus $f\colon (\mathbb{Z}_n, \langle \frac{n}{a} \rangle) \to (\mathbb{Z}_m, \langle \frac{m}{b} \rangle)$ is a morphism in $\mathbb{S}_2$ mapping to morphism $k\colon (n,a) \to (m,b)$ in $\mathbb{B}$. Thus H is an isomorphism.

We have that for any object (A,X) is $\mathbb{S}_2$, $GS(A,X) = |A| = FH(A,X)$, and also for any morphis f in $\mathbb{S}_2$, $GSf = f1 = FHf$. Thus those two forms are isomorphic. □

The rest of this section is just properties we can deduce, that these examples will have. We will assume, that we are working with that fixed normed Noetherian form which is constructed from a fixed modular structure N.

Proposition 26. *The group* 1 *is both an initial object and a terminal object.*

Proof. For any group n, $1\colon n \to 1$ is a morphism, since $1 \equiv_1 n1$. For any other morphism $k\colon n \to 1$, we have $k \equiv_1 1 \equiv_1 1n$. Thus 1 is the unique morphism from n to 1. Thus 1 is a terminal object.

Now to show that 1 is an initial object: $n\colon 1 \to n$ is a morphism. If $k\colon 1 \to n$ is a morphism, then $1k \equiv_n n$. Thus n is unique morphism from 1. □

Section 3.2 in particular shows that having a zero object and that all subgroups are both normal and conormal, implies categorical kernels and cokernels exists, and the embeddings are exactly the monomorphism (and dually, the projections are exactly the epimorphisms), and all monomorphisms are normal (and dually, all epimorphisms are conormal).

Another property that holds for the usual modular relations that holds here:

Proposition 27. *For any $a, b \in N$, we have $a \wedge b = 1$ if and only if $\exists_{k\in N}(bk \equiv_a 1)$.*

Proof. Suppose $a \wedge b = 1$. $b\colon a \to a$ is a morphism. Since $a \wedge b = 1$, $\mathsf{Im}b = \frac{a}{a\wedge b} = a$. Thus b is a projection, and consequently an isomorphism. Thus there is a $k\colon a \to a$, the inverse of b, such that $bk \equiv_a 1$.

Suppose there is a $k \in N$, such that $bk \equiv_a 1$. Then $bk \wedge a = 1 \wedge a$, which implies $b \wedge a = 1$. □

Notice that from the theory of normed Noetherian forms, for morphism $k\colon n \to m$ we have

$$n = (\mathsf{Ker}k)(\mathsf{Im}k).$$

By using this fact and an equivalence of Axiom 6, we get the following list of equivalences:

Proposition 28. *For maps $k, l\colon n \to m$ the following are equivalent*

(1) $k \wedge m = l \wedge m$;

(2) $\mathsf{Im}k = \mathsf{Im}l$;

(3) $\mathsf{Ker}k = \mathsf{Ker}l$;

(4) $k_* = l_*$;

(5) $k^* = l^*$.

Proof. Since $\mathsf{Im}k = \frac{m}{k\wedge m}$ and $\mathsf{Im}l = \frac{m}{l\wedge m}$, (1) is equivalent to (2). (2) and (3) are equivalent, since $n = (\mathsf{Ker}k)(\mathsf{Im}k)$.

Using an equivalence of Axiom 6, we have for any $a \leq n$

$$(k^*1)(k_*a) = (a \vee \mathsf{Ker}k)(1 \wedge \mathsf{Im}k) = a \vee \mathsf{Ker}k.$$

The same holds for l. From this we see that (3) implies (4). Also, (4) implies (2), which implies (3).

We have for any $b \leq m$

$$(k^*b)(k_*n) = (n \vee \mathsf{Ker}k)(b \wedge \mathsf{Im}k) = (n)(b \wedge \mathsf{Im}k).$$

The same holds for l. From this we see that (2) implies (5). And also, (5) implies (3), which implies (2).

Thus everything is equivalent. □

From $n = (\mathsf{Im}k)(\mathsf{Ker}k)$, with the help of basic results, also (readily) follows:

Proposition 29. *For any morphism $k\colon n \to m$,*

- *k is an embedding if and only if $\mathsf{Im}k = n$ if and only if $k \wedge m = \frac{m}{n}$;*
- *k is a projection if and only if $\mathsf{Ker}k = \frac{n}{m}$ if and only if $k \wedge m = 1$.*

Corollary 30. *If $k \colon n \to m$ is an embedding and $b \le m$, then $k^* b = n \wedge b$.*

Proof. We have

$$k^* b = (k^* b)(k_* 1) = (1 \vee \mathsf{Ker} k)(b \wedge \mathsf{Im} k) = b \wedge n.$$

□

Proposition 31. *For projection $f \colon m \to n$, f has a right inverse if and only if $n \wedge \frac{m}{n} = 1$.*

Proof. Suppose that there is a morphism $s \colon n \to m$ such that $fs = 1_n$. Then

$$1 = (fs)^* 1 = s^* f^* 1 = s^* \left(\frac{m}{n}\right) = n \wedge \frac{m}{n}.$$

Suppose $n \wedge \frac{m}{n} = 1$. Since f is a projection, $n \le m$. So $\frac{m}{n} \colon n \to m$ is a morphism. Moreover, since $\frac{m}{n} \wedge m = \frac{m}{n}$, $\frac{m}{n} \colon n \to m$ is an embedding. Composing f and $\frac{m}{n}$, we get

$$\left(f \circ \frac{m}{n}\right)_* n = f_* \left(\frac{nm}{nm \wedge \frac{m}{n} n}\right) = f_* n = f_* \left(n \vee \frac{m}{n}\right) = f_* m = n.$$

The third equality follows since f_* preserves joins and $\frac{m}{n}$ is the kernel of f. The fourth equality follows, since $n \wedge \frac{m}{n} = 1$ and thus their product is the same as their join.

Thus $f \circ \frac{m}{n} \colon n \to n$ is a projection, thus an isomorphism. Let $k \colon n \to n$ be the inverse. Then $\frac{m}{n} \circ k \colon n \to m$ is a right inverse of f. □

Proposition 32. *For embedding $s \colon n \to m$, s has a left inverse if and only if $n \wedge \frac{m}{n} = 1$.*

Proof. Suppose s has a left inverse $f \colon m \to n$. Then

$$1 = (fs)^* 1 = s^* f^* 1 = s^* \left(\frac{m}{n}\right) = n \wedge \frac{m}{n}.$$

Suppose $n \wedge \frac{m}{n} = 1$. We have $n \le m$, since s is an embedding. So $1 \colon m \to n$ is a morphism. Moreover, since $1 \wedge n = 1$, it is also a projection. Composing them, we get

$$(1 \circ s)^* 1 = s^* 1^* 1 = s^* \frac{m}{n} = n \wedge \frac{m}{n} = 1.$$

Thus $1 \circ s \colon n \to n$ is an embedding, thus an isomorphism. Let k be the inverse of $1 \circ s$. Then $k \circ 1$ is a left inverse of s.

□

2.3 Second Sylow Theorem

In this section we present an attempt to recapture the second Sylow Theorem.

In this section we work with a fixed normed Noetherian-Form with codomain Q of the norm function.

First, we need to know what are the "natural numbers", "prime numbers", and "p-subgroups" in this context.

Definition 14. An element of Q will be called a *natural number* if it is equal to the order of some group. The set of all natural numbers will be denoted by N.

Notice that the dual of a natural number is the reciprocal of some natural number (need not be the same natural number), and it will be called a *conatural number*.

With this submonoid, we define a relation $\leq$ on Q by, for any $a, b \in Q$,

$$a \leq b \quad \Leftrightarrow \quad ba^{-1} \in N.$$

It is clear that this relation is transitive, but cannot deduce whether it is anti-symmetric or even reflexive. Since we want Q to be a poset under $\leq$, we make the following axiom.

Axiom 8. $(Q, \leq)$ is a poset.

We will say a *divides* b if $a \leq b$, and call a a *divisor* of b. The dual of $p \leq q$ is $q \leq p$. This is because the dual of $p \leq q$ states that there is a conatural number $\frac{1}{n}$ such that $qp^{-1} = \frac{1}{n}$, which is the same as $pq^{-1} = n$, that is, $q \leq p$.

Definition 15. A *prime number* p is a natural number which has no divisors except for 1 and itself.

It turns out, that a *coprime number* is a reciprocal of a prime number: A coprime number is a conatural number $\frac{1}{p}$ such that the only conatural numbers it divides are 1 and itself. That is, if $\frac{1}{p} \leq \frac{1}{n}$, then $\frac{1}{n} = 1$ or $\frac{1}{n} = \frac{1}{p}$, but that is equivalent to if $n \leq p$, then $n = 1$ or $n = p$. So p is forced to be a prime number.

Further, we add the following axioms as well.

Axiom 9. If p is a prime and ab is a power of p, then both a and b is a power of p.

Axiom 10. The usual natural numbers $\mathbb{N}$ is contained in N.

The above axiom is needed, since we want to compare sizes of sets with some the elements in N.

Axiom 11. For any group G, $\mathsf{Sub}G$ is a finite set.

Axiom 12. If for any two subgroups X and Y, $X \leq Y$, then $\|X\| \leq \|Y\|$.

Definition 16. For a group G, and a prime number p, a *p-subgroup* of X is a conormal subgroup of G such that $|X/1| = p^a$ for some $a \in \mathbb{N}$. Dually, for coprime $\frac{1}{p}$, a *$\frac{1}{p}$-subgroup* X is a normal subgroup such that $\frac{1}{|G/X|} = \frac{1}{p^a}$ for some $a \in \mathbb{N}$, or equivalently $|G/X| = p^a$.

In any group G, the subgroup 0^G is a p-subgroup for any prime p, and 1^G is a $\frac{1}{p}$-subgroup.

Definition 17. For a prime p, a *Sylow p-subgroup* is a maximal p-subgroup. And for a coprime $\frac{1}{p}$, a *Sylow $\frac{1}{p}$-subgroup* is a minimal $\frac{1}{p}$-subgroup.

First Sylow Theorem states that if $|X| = p^a m$ where p and m is relatively prime, then it has a Sylow p-subgroup which has order p^a. The dual here would be if $|X| = p^a m$, then X has a $\frac{1}{p}$-subgroup A such that $|X/A| = p^a$, however this is false in classical group theory. Take the alternating group on 5 letters A_5. It has order $60 = 2^2 \cdot 3 \cdot 5$, but it doesn't have any (normal) subgroups of index 3 or 4. So in this self-dual context, with these definitions, we cannot recover the First Sylow Theorem.

The following lemma is useful for eventually get Second Sylow Theorem. This lemma is well-known for groups, for example it is equivalent to lemma on page 424 in [8].

Lemma 33. *For a prime p and any two Sylow p-subgroups P and Q, if P is normal in $P \vee Q$, then $P = Q$.*

Proof. From one of the isomorphism theorems we get

$$(P \vee Q)/P \cong Q/(P \wedge Q).$$

So, by taking the order on both sides, write it in terms of the norm function, and with some rearrangement, we get:

$$\frac{\|P \vee Q\|}{\|0\|}\frac{\|P \wedge Q\|}{\|0\|} = \frac{\|P\|}{\|0\|}\frac{\|Q\|}{\|0\|}.$$

The right side is a power of prime p, thus $|(P \vee Q)/1|$ must also be a power of p. Thus also a p-subgroup. Since P and Q are maximal p-subgroups, $P = P \vee Q = Q$. $\square$

Second Sylow Theorem states that any two Sylow p-subgroups are conjugates. We add the following set of relations with some properties which represents the conjugate relation. In the definition, we use $\leq$ between natural numbers to denote the divisibility relation.

Definition 18. For every subgroup A of a group G, there is an equivalence relation c_A on the set of subgroups of G, where $[X]_A$ denotes the equivalence class of X under relation c_A (and $|[X]_A|$ denotes the usual cardinality of a set), satisfying the following:

(1) $|[X]_A| \leq \frac{\|A\|}{\|A \wedge X\|}$

(2) If X is conormal and $q \in Q$, if q divides the cardinality of each $[Y]_A$ for $Y \in [X]_1$, except possibly for $[X]_A$, then q divides $|[X]_A|$ if and only if it divides $|[X]_1|$.

(3) If X is conormal and $|[X]_A| = 1$, then X is normal in $X \vee A$.

(4) If Xc_1Y, then there exists an automorphism f of G such that $fX = Y$.

Subgroups X and Y will be called *conjugates* if Xc_GY. $[X]_1$ will be denoted simply as $[X]$.

Point (2) of the definition intuitively represents that if

$$|[X]| = |[Y]_A| + |[Z]_A| + \dots |[X]_A|$$

and q divides all the terms before $|[X]_A|$, then q divides $|[X]|$ only if q divides the last term $|[X]_A|$. Since we don't have the concept of addition (some attempts of adding it made it very difficult or impossible to find suitable self-dual definition), we added this point to deal with addition indirectly when we need it.

Duality fixes these conjugacy relations. The dual of the conditions on the equivalence classes are true in classical group theory, that is when c_A is defined as Xc_AY if and only if $X = aYa^{-1}$ for some $a \in A$, since conjugacy classes of normal subgroups have cardinality 1.

We have the following lemmas.

Lemma 34. *For any subgroup X, we have $|[X]_X| = 1$.*

Proof. We have $|[X]_X| \leq \frac{\|X\|}{\|X \wedge X\|} = 1$, and thus $|[X]_X| = 1$. □

Lemma 35. *For any two conjugate subgroups X and Y, $\|X\| = \|Y\|$.*

Proof. Suppose $f \colon G \to G$ is an automorphism such that $fX = Y$. Then we have

$$\frac{\|X\|}{\|0\|} = \frac{\|fX\|}{\|f0\|} = \frac{\|Y\|}{\|0\|}.$$

And thus $\|X\| = \|Y\|$. □

Lemma 36. *In a group G, if subgroups X and Y are conjugates and X is a Sylow p-subgroup, then Y is also a Sylow p-subgroup.*

Proof. Take the embedding e_X of X and take an automorphism f of G such that $fX = Y$. Then the image of fe_X is Y. So Y is a conormal subgroup. Also since X and Y are conjugates, their norms are equal, thus their orders are also equal. Thus Y is a p-subgroup as well.

Suppose Z is any p-subgroup which contains Y. $f^{-1}Z$ is also a p-subgroup, with similar argument as above. Then we have

$$f^{-1}Z \geq f^{-1}Y = X$$

thus $f^{-1}Z = X$, and thus $Z = Y$. Thus Y is also a Sylow p-subgroup. □

In fact, the above two lemmas are true for any two "isomorphic" subgroups, in the sense of there is an isomorphism whose direct image map maps the one subgroup to the other.

Theorem 37. *For any prime p, and in any group G, any two Sylow p-subgroups are conjugates.*

Proof. Suppose that P and Q are two Sylow p-subgroups, but not conjugates. For any $Y \in [P]$, and therefor Y is also a Sylow p-subgroup, $|[Y]_Q| \neq 1$, since otherwise Y is normal in $X \vee Y$ by (3) of Definition 18 and thus equal to Y by Lemma 33. Also, $\frac{\|Q\|}{\|Y \wedge Q\|} = p^a$ for some $a \in \mathbb{N}\backslash\{0\}$. Thus p divides $|[Y]_Q|$. Thus p divides $|[P]|$, since $p \leq |[P]_Q|$. But we also have that, $|[P]_P| = 1$, and similarly for $[Y]_P \neq [P]_P$, $p \leq |[Y]_P|$. But then p also doesn't divide$|[P]|$ which is a contradiction. Thus all Sylow p-subgroups are conjugates. $\square$

The dual of Theorem 37 in usual group theory states that there is a unique Sylow $\frac{1}{p}$-subgroup for every prime p. This is true: The dual of Lemma 33 is true in usual group theory, and from this it immediately follows since every subgroup is conormal in any subgroup which contains it.

Chapter 3

Projective Theory of Biproducts

3.1 The Notion of Biproduct

In this section we introduce biproducts in projective group theory.

In this section we will be working with a fixed Noetherian form $F\colon \mathbb{B} \to \mathbb{C}$ where "biproducts" exists. Biproducts are defined as follows:

Definition 19. For groups X and Y, a *biproduct* of X and Y is a group G with four maps

$$\begin{tikzcd} X \arrow[r, shift left, "e_1"] & G \arrow[l, shift left, "p_1"] \arrow[r, shift right, "p_2"'] & Y \arrow[l, shift right, "e_2"'] \end{tikzcd}$$

such that

- $p_1e_1 = 1_X$ and $p_2e_2 = 1_Y$;
- $\mathsf{Im}e_1 = \mathsf{Ker}p_2$ and $\mathsf{Im}e_2 = \mathsf{Ker}p_1$;

and for any $f\colon W \to X$ and $g\colon W \to Y$, the diagram

$$\begin{tikzcd} X & G \arrow[l, "p_1"'] \arrow[r, "p_2"] & Y \\ & W \arrow[ul, "f"] \arrow[ur, "g"'] & \end{tikzcd}$$

has a limit, and for any $f'\colon X \to W'$ and $g'\colon Y \to W'$, the diagram

$$\begin{tikzcd} & W' & \\ X \arrow[ur, "f'"] \arrow[r, "e_1"] & G & Y \arrow[ul, "g'"'] \arrow[l, "e_2"'] \end{tikzcd}$$

has a colimit.

This definition is self-dual. Here e_i is the dual of p_i, for $i = 1, 2$.

We will make use of the following convenient way to refer to those diagrams in the definition: If G is a group equipped with four morphisms

$$\begin{tikzcd} X \arrow[r, shift left, "e_1"] & G \arrow[l, shift left, "p_1"] \arrow[r, shift right, "p_2"'] & Y \arrow[l, shift right, "e_2"'] \end{tikzcd}$$

such that $p_1e_1 = 1_X$, $p_2e_2 = 1_Y$, $e_11 = p_2^{-1}0$, $e_21 = p_1^{-1}0$, then for any $f\colon W \to X$ and $g\colon W \to Y$, $\mathsf{L}_G(X, Y)$ will denote the diagram

$$\begin{tikzcd} X & G \arrow[l, "p_1"'] \arrow[r, "p_2"] & Y \\ & W \arrow[ul, "f"] \arrow[ur, "g"'] & \end{tikzcd}$$

and for $f'\colon X \to W'$ and $g'\colon Y \to W'$, $\mathsf{C}_G(f', g')$ will denote the diagram

$$\begin{tikzcd} & W' & \\ X \arrow[ur, "f'"] \arrow[r, "e_1"] & G & Y \arrow[l, "e_2"'] \arrow[ul, "g'"'] \end{tikzcd}$$

When it is clear in which such group we are working with or referring to, the subscript G may be dropped. For further simplicity, we are going to use the following shorthanded notation: $f\colon X \to Y \leftarrow Z\colon g$ to mean that f is a morphism from X to Y and g from Z to Y. Also, $f\colon X \leftarrow Y \to Z\colon g$ will mean that f is an arrow from Y to X and g from Y to Z. It will be used for cones and cocones of those diagrams in the biproduct definition.

The following lemma is very basic results that will also be used to show that this biproduct definition coincides with usual product in classical group theory.

Lemma 38. *For any X and Y, if for*

$$\begin{tikzcd} X \arrow[r, shift left, "e_1"] & G \arrow[l, shift left, "p_1"] \arrow[r, shift right, "p_2"'] & Y \arrow[l, shift right, "e_2"'] \end{tikzcd}$$

we have

- $p_1e_1 = 1_X$ *and* $p_2e_2 = 1_Y$;
- $\mathsf{Ker}p_1 = \mathsf{Im}e_2$ *and* $\mathsf{Ker}p_2 = \mathsf{Im}e_1$;

then we have

(1) $e_11 \vee e_21 = 1$;

(2) $e_11 \wedge e_21 = 0$;

(3) $p_1^{-1}0 \vee p_2^{-1}0 = 1$;

(4) $p_1^{-1}0 \wedge p_2^{-1}0 = 0$;

(5) If A is a normal subgroup of X, then $e_1 A$ is a normal subgroup of G;

(6) If A is a conormal subgroup of X , then $p_1^{-1}A$ is a conormal subgroup of G.

(5) and (6) are also true when we replace X with Y and e_1 with e_2 and p_1 with p_2.

Proof. For (1), we have

$$e_1 1 \vee e_2 1 = e_1 1 \vee p_1^{-1} 0 = p_1^{-1} p_1 e_1 1 = p_1^{-1} 1 = 1.$$

For (2), we have

$$e_1 1 \wedge e_2 1 = e_1 e_1^{-1} e_2 1 = e_1 e_1^{-1} p_1^{-1} 0 = e_1 (p_1 e_1)^{-1} 0 = e_1 0 = 0.$$

(3) and (4) are the duals of (2) and (1) respectively.

For (5), suppose A is a normal subgroup of X. We have

$$e_1 A = e_1 e_1^{-1} p_1^{-1} A = e_1 1 \wedge p_1^{-1} A.$$

Since both $e_1 1$ and $p_1^{-1}A$ are normal, $e_1 A$ is normal.

(6) is the dual of (5). □

Now to show that this definition coincides with the usual product in classical group theory. The theorem below also relies on the fact that biproducts are isomorphic, but we'll show that later in the section.

Theorem 39. *In classical groups theory, G is a biproduct, in the above sense, of X and Y if and only if G is isomorphic to the ordinary product $G \cong X \times Y$.*

Proof. Suppose that G is a biproduct for X and Y. Then we have that $e_1 X$ and $e_2 Y$ are normal subgroups of G, such that

$$0 = e_1 X \wedge e_2 Y \quad \text{and} \quad G = e_1 X \vee e_2 Y.$$

Thus $G \cong X \times Y$.

For the converse, define

$$e_1 \colon X \to X \times Y,\ x \mapsto (x, 1)$$

and

$$e_2 \colon Y \to X \times Y,\ y \mapsto (1, y)$$

and let $p_1 \colon X \times Y \to X$ and $p_2 \colon X \times Y \to Y$ be the usual product projections. These four maps satisfies all four conditions of a biproduct: $e_1 p_1 = 1_X$, $e_2 p_2 = 1_Y$, $e_1 1 = p_2^{-1} 0$, $e_2 1 = p_1^{-1} 0$. Also, since all small limits and colimits exists (in the category of groups), the other conditions are also satisfied. □

A final basic lemma that will make computations throughout this section easier:

Lemma 40. *For any X and Y and any*

$$X \underset{p_1}{\overset{e_1}{\rightleftarrows}} G \underset{p_2}{\overset{e_2}{\leftrightarrows}} Y$$

such that $p_1e_1 = 1_X$, $p_2e_2 = 1_Y$, $e_1 1 = p_2^{-1}0$, $e_2 1 = p_1^{-1}0$, we have for any $A \in \mathsf{sub}X$ and $B \in \mathsf{sub}Y$, where at least A or B is normal or conormal,

$$e_1A \vee e_2B = p_1^{-1}A \wedge p_2^{-1}B.$$

Proof. First notice that

$$e_1A = e_1e_1^{-1}p_1^{-1}A = e_1 1 \wedge p_1^{-1}A$$

and similarly

$$e_2B = e_2 1 \wedge p_2^{-1}B.$$

These are just special cases of this lemma where $A = 0$ or $B = 0$.

Suppose A is normal. Then we have

$$\begin{aligned}
&e_1A \vee e_2B\\
=&(e_1 1 \wedge p_1^{-1}A) \vee (e_2 1 \wedge p_2^{-1}B)\\
=&((e_1 1 \wedge p_1^{-1}A) \vee e_2 1) \wedge p_2^{-1}B\\
=&(p_1^{-1}A \wedge (e_1 1 \vee e_2 1)) \wedge p_2^{-1}B\\
=&p_1^{-1}A \wedge p_2^{-1}B.
\end{aligned}$$

The second equality follows from the fact that $e_1 1 \wedge p_1^{-1}A$ is normal and less than $p_2^{-1}B$, and that $e_2 1$ is conormal. The third one follows, since $e_2 1$ is normal and $e_1 1$ is conormal and $p_1^{-1}A \geq e_2 1$.

Dually, if A is conormal, then $e_1A \vee e_2B = p_1^{-1}A \wedge p_2^{-1}B$..

The case where B is normal or conormal is proved similarly as where A is normal or conormal (just interchange 1 and 2, and A and B). □

Theorem 41. *Let*

$$X \underset{p_1}{\overset{e_1}{\rightleftarrows}} G \underset{p_2}{\overset{e_2}{\leftrightarrows}} Y$$

be a biproduct of X and Y.

For any $f\colon X \to W$ and $g\colon Y \to W$, if

$$e\colon W \to C \leftarrow G\colon m$$

is the colimit of $\mathsf{C}(f, g)$, then e is a projection.

And dually for any $f\colon W \to X$ and $g\colon W \to Y$, if

$$m\colon W \leftarrow L \to G\colon e$$

is the limit of of $\mathsf{L}(f, g)$, then m is an embedding.

Proof. Let $I = \mathsf{Im}e$, and let $h\colon I \to C$ be the embedding corresponding to I. We have the following diagram

$$\begin{tikzcd}
 & & W \arrow[dl, "e"'] \arrow[dr, dashed, "a"] & & \\
 & C \arrow[rr, dashed, "k"'] & & I \arrow[ll, "h"'] & \\
X \arrow[uurr, bend left, "f"] \arrow[rr, "e_1"'] & & G \arrow[ul, "m"] \arrow[ur, dashed, "b"'] & & Y \arrow[uull, bend right, "g"'] \arrow[ll, "e_2"]
\end{tikzcd}$$

Morphism a exists such that $ha = e$, since $\mathsf{Im}e \leq I$. We (always) have $\mathsf{Im}m \leq I$, since

$$\begin{aligned}
m1 &= m(e_1 1 \vee e_2 1)\\
&= me_1 1 \vee me_2 1\\
&= ef1 \vee eg1\\
&= e(f1 \vee g1)\\
&\leq \mathsf{Im}e = I.
\end{aligned}$$

Thus morphism b exists such that $hb = m$.

We have

$$hbe_1 = me_1 = ef = haf$$

Which implies $be_1 = af$, since h is an embedding (thus a monomorphism). Similarly $be_2 = ag$. Thus

$$a\colon W \to I \leftarrow G\colon b$$

is a cocone of $\mathsf{C}(f, g)$. Thus there exists a morphism $k\colon C \to I$ such that $ke = a$ and $km = b$. Composing h and k, we get a morphism $hk\colon C \to C$ such that $(hk)e = e$ and $(hk)m = m$. But $1_C\colon C \to C$ is the unique such morphism. Thus $hk = 1_C$, and thus h is a projection. Thus e is a projection. $\square$

Theorem 42. *For X and Y, if*

$$\begin{tikzcd}
X \arrow[r, shift left, "e_1"] & G \arrow[l, shift left, "p_1"] \arrow[r, shift right, "p_2"'] & Y \arrow[l, shift right, "e_2"']
\end{tikzcd}$$

is a biproduct for X and Y, then

(1) e_1 and e_2 are jointly epic;

(2) p_1 and p_2 are jointly monic.

Note: (2) is the dual of (1).

Proof. Suppose $e\colon G \to C \leftarrow G\colon m$ is the colimit of $\mathsf{C}(e_1, e_2)$. Consider the diagram

$$\begin{tikzcd}
 & & G \arrow[dl, "e"'] \arrow[dr, "1_G"] & & \\
 & C \arrow[rr, dashed, "k"'] & & G & \\
X \arrow[rr, "e_1"'] \arrow[uurr, bend left, "e_1"] & & G \arrow[ul, "m"] \arrow[ur, "1_G"'] & & Y \arrow[ll, "e_2"] \arrow[uull, bend right, "e_2"']
\end{tikzcd}$$

$1_G\colon G \to G \leftarrow G\colon 1_G$ is a cocone of $\mathsf{C}(e_1, e_2)$. Thus there exists a morphism $k\colon C \to G$ such that $ke = 1_g$ and $km = 1_G$. Since $ke = 1_G$, e is an embedding, thus an isomorphism. Also, k is then its inverse. Thus k is also an isomorphism. Thus $1_G\colon G \to G \leftarrow G\colon 1_G$ is also a colimit of $\mathsf{C}(e_1, e_2)$.

Suppose for $u, v\colon G \to W$, we have $ue_1 = ve_1$ and $ue_2 = ve_2$. Then $u\colon G \to W \leftarrow G\colon v$ is a cocone of $\mathsf{C}(e_1, e_2)$, thus there exists a unique $k\colon G \to W$ such that $1_G k = u$ and $1_G k = v$. Thus $u = v$ and thus e_1 and e_2 are jointly epic. $\square$

Lemma 43. *Suppose*

$$\begin{tikzcd}
X \arrow[r, shift left, "e_1"] & G \arrow[l, shift left, "p_1"] \arrow[r, shift right, "p_2"'] & Y \arrow[l, shift right, "e_2"']
\end{tikzcd}$$

is a biproduct of X and Y. For any $f\colon X \to W$ and $g\colon Y \to W$, we have that any cocone $e\colon W \to C \leftarrow G\colon m$ of $\mathsf{C}(f, g)$ is the colimit of $\mathsf{C}(f, g)$ if and only if

- *e is a projection;*
- *for any cocone of $\mathsf{C}(f, g)$*

  $$d\colon W \to L \leftarrow G\colon n$$

  we have $\mathsf{Ker}e \leq \mathsf{Ker}d$.

Proof. Suppose that $e\colon W \to C \leftarrow G\colon m$ is the colimit of $\mathsf{C}(f, g)$. Then e is a projection, and for any cocone $d\colon W \to L \leftarrow G\colon n$ of $\mathsf{C}(f, g)$, there is a $h\colon C \to L$ such that $he = d$. Then

$$\mathsf{Ker}e = e^*0 \leq e^*h^*0 = d^*0 = \mathsf{Ker}d.$$

For the converse, suppose $e\colon W \to C \leftarrow G\colon m$ is a cocone of $\mathsf{C}(f, g)$ having those properties. Take any cocone $d\colon W \to L \leftarrow G\colon n$ of $\mathsf{C}(f, g)$. Since $\mathsf{Ker}e \leq \mathsf{Ker}d$ and e a projection, there is an unique $h\colon C \to L$ such that $he = d$. We also have

$$ne_1 = df = hef = hme_1.$$

Similarly, $ne_2 = hme_2$. Thus $n = hm$, since e_1 and e_2 are jointly epic. Since h is unique, $e\colon W \to C \leftarrow G\colon m$ is the colimit of $\mathsf{C}(f, g)$. $\square$

3.2 Pointedness

Proposition 44. *If the codomain category of a Noetherian form with biproducts is non-empty, then it is pointed.*

Proof. For group G, let $l\colon 0 \to G$ be the embedding of $0 \in \mathsf{sub}G$. We have

$$1 = l^{-1}l1 = l^{-1}0 = 0.$$

So $\mathsf{sub}(0)$ has exactly one element. Also, in 0×0 we have

$$1 = e_1 1 \vee e_2 1 = e_1 0 \vee e_2 0 = 0.$$

Thus $\mathsf{sub}(0 \times 0)$ also have just one element. Consequently the embeddings e_1 and e_2 of the product are isomorphisms, with respective inverses p_1 and p_2.

Take any $f, g\colon 0 \to 0$. Suppose $e\colon 0 \to C \leftarrow 0 \times 0\colon m$ is the colimit of $\mathsf{C}_{0\times 0}(f, g)$. Since e is a projection and 0 is its domain, e is an isomorphism. We have

$$m = me_1p_1 = efp_1.$$

And so

$$g = e^{-1}eg = e^{-1}me_2 = e^{-1}efp_1e_2 = fp_1e_2.$$

The above equation is true for any $f, g\colon 0 \to 0$. In particular, for $f = 1_0$ and $g = 1_0$, we get $p_1e_2 = 1_0$, from which it follows that $1_0\colon 0 \to 0$ is the only morphism from 0 to 0.

For any group H, there is a morphism $i\colon 0 \to H$. A way to construct such a morphism, is to take the biproduct $0 \times H$ and compose a suitable projection and embedding of the biproduct. Since $|\mathsf{sub}0| = 1$, this morphism is an embedding. Thus it is an embedding of its image $0 \in \mathsf{sub}H$. For any morphism from $f\colon 0 \to H$, its image is also 0, and thus there exists $h\colon 0 \to 0$ such that $hi = f$. But since 1_0 is the only morphism from 0 to 0, $f = i$, thus 0 is an initial object. Dually, 0 is a terminal object. $\square$

Throughout the rest of this section, we will be working with a fixed Noetherian form whose codomain is a pointed category.

Proposition 45. *Let T denote the zero object. Then we have $|\mathsf{sub}T| = 1$. Moreover, for any group G such that $|\mathsf{sub}G| = 1$, G is also a zero object. Furthermore a morphism is a 0-morphism if and only if its kernel is 1 if and only if its image is 0.*

Proof. Let $l\colon L \to T$ be an embedding of 0 in T. There also exists an $r\colon T \to L$, since T is an initial object. Since $lr\colon T \to T$, $lr = 1_T$, thus l is an isomorphism. We have

$$1 = \mathsf{Im}l \leq 0 \leq 1.$$

Thus $1 = 0$ in $\mathsf{sub}T$, and thus $\mathsf{sub}T$ only has one element.

Take any group G such that $\mathsf{sub}G$ only has one element. Then the unique morphism $T \to G$ will trivially be an isomorphism. Thus G is also a zero object.

Now to prove that equivalences: Suppose $f\colon X \to Y$ is a 0-morphism. Then $f = lr$, where $r\colon X \to T$ and $l\colon T \to Y$. Then

$$f(1) = lr(1) = l(0) = 0.$$

Suppose $f\colon X \to Y$ is any morphism with trivial image. Then

$$f^{-1}0 = f^{-1}f1 = 1.$$

Suppose $f\colon X \to Y$ is a morphism with kernel 1. Since the unique morphism $X \to T$ is a projection and has kernel 1, it is a projection of 1. Since f also have kernel 1, f factors through $X \to T$. Thus f is a 0-morphism. □

Proposition 46. *For any map $f\colon X \to Y$, the embedding of the kernel of f, $k\colon \underline{\mathsf{Ker}f}/1 \to X$, is the categorical kernel of f. Dually, the projection of the image of f, $c\colon Y \to Y/\overline{\mathsf{Im}f}$, is the categorical cokernel of f.*

Proof. Since $\mathsf{Im}k \leq \mathsf{Ker}f$, fk has image 0, thus is a 0-morphism. Suppose $l\colon L \to X$ is morphism such that fl is a 0-morphism. Then $\mathsf{Im} \leq \mathsf{Ker}f$. Since k is the embedding of $\mathsf{Ker}f$, l uniquely factorizes through k. Thus k is the categorical kernel of f. □

Proposition 47. *If every normal subgroup is conormal, then a morphism is an embedding if and only if it is a monomorphism. And dually, if every conormal subgroup is normal, then a morphism is a projection if and only if it is an epimorphism.*

Proof. We already have that every embedding is a monomorphism.

Suppose that f is a monomorphism. Let K be the kernel of f. Since K is normal, K is conormal by assumption. The embedding of K, $k\colon K \to X$, is the categorical kernel of K. But since the categorical kernel of monomorphism is the zero object, K is also a zero object. Thus the image of k is 0. That is, the kernel of f is 0. Thus it is an embedding.

□

Proposition 48. *If every normal subgroup is conormal, then every projection is a categorical cokernel of some morphism. And dually, if every conormal subgroup is normal, then every embedding is a categorical kernel of some morphism.*

Proof. Suppose every normal subgroup is conormal. Take any projection $f\colon X \to Y$. Then $k\colon K \to X$ is the categorical kernel of f, where K is the kernel of f, and k is the embedding of K. We have that fk is a 0-morphism. Suppose $c\colon X \to C$ is a morphism such that ck is a 0-morphism. Then $c(k(1)) = 0$. So

$$\mathsf{Ker}p = K = k(1) \leq \mathsf{Ker}c.$$

Since f is a projection, it is a projection of its kernel. Thus c will factorize uniquely through f. Thus f is the categorical cokernel of $k\colon K \to X$. □

3.3 Monoidality of Biproduct

In this section we work with a fixed Noetherian form with biproducts.

Proposition 49. *Suppose*

$$\begin{tikzcd} X \arrow[r, shift left, "e_1"] & G \arrow[l, shift left, "p_1"] \arrow[r, shift right, "p_2"'] & Y \arrow[l, shift right, "e_2"'] \end{tikzcd}$$

satisfies $e_1 1 = p_2^{-1} 0$, $e_2 1 = p_1^{-1} 0$, $p_1 e_1 = 1$ *and* $p_2 e_2 = 1$, *and*

$$\begin{tikzcd} A \arrow[r, shift left, "d_1"] & H \arrow[l, shift left, "q_1"] \arrow[r, shift right, "q_2"'] & B \arrow[l, shift right, "d_2"'] \end{tikzcd}$$

is a biproduct, and $f\colon A \to X$ *and* $g\colon B \to Y$ *are morphisms. Then there exists a unique morphism* $f \times g\colon H \to G$ *such that*

- $(f \times g)d_1 = e_1 f$,
- $(f \times g)d_2 = e_2 g$,
- $p_1(f \times g) = f q_1$,
- $p_2(f \times g) = g q_2$.

Further more, we have

- $\mathsf{Im}(f \times g) = e_1\mathsf{Im}f \vee e_2\mathsf{Im}g = p_1^{-1}\mathsf{Im}f \wedge p_2^{-1}\mathsf{Im}g$;
- $\mathsf{Ker}(f \times g) = q_1^{-1}\mathsf{Ker}f \wedge q_2^{-1}\mathsf{Ker}g = d_1\mathsf{Ker}f \vee d_2\mathsf{Ker}g$.

Consequently, $f \times g$ *is a projection if and only if both* f *and* g *are projections, and* $f \times g$ *is an embedding if and only if both* f *and* g *are embeddings.*

Proof. Suppose $e\colon G \to C \leftarrow H\colon m$ is the colimit of $\mathsf{C}_H(e_1 f, e_2 g)$. Since both $p_1\colon G \to X \leftarrow H\colon f q_1$ and $p_2\colon G \to Y \leftarrow H\colon g q_2$ are cocones of $\mathsf{C}_H(e_1 f, e_2 g)$,

$$\mathsf{Ker}e \leq \mathsf{Ker}p_1 \wedge \mathsf{Ker}p_2 = 0.$$

Thus e is an isomorphism. Let $h = e^{-1}m\colon H \to G$. Then

$$hd_1 = e^{-1}md_1 = e^{-1}ee_1 f = e_1 f.$$

Similarly $hd_2 = e_2 g$. Also

$$p_1 h d_1 = f = f q_1 d_1 \quad \text{and} \quad p_1 h d_2 = 0 = f q_1 d_2.$$

Since d_1 and d_2 are jointly epic, $p_1 h = f q_1$. And similarly $p_2 h = f q_2$. Thus h is the unique required morphism $f \times g$.

Moreover, we have

$$\begin{aligned}\mathsf{Im}(f \times g) &= (f \times g)1 \\ &= (f \times g)(d_1 1 \vee d_2 1) \\ &= (f \times g)d_1 1 \vee (f \times g)d_2 1 \\ &= e_1 f 1 \vee e_2 g 1 \\ &= e_1 \mathsf{Im} f \vee e_2 \mathsf{Im} g\end{aligned} \qquad \begin{aligned}\mathsf{Ker}(f \times g) &= (f \times g)^{-1}0 \\ &= (f \times g)^{-1}(p_1^{-1}0 \wedge p_2^{-1}0) \\ &= (f \times g)^{-1}p_1^{-1}0 \wedge (f \times g)^{-1}p_2^{-1}0 \\ &= q_1^{-1}f^{-1}0 \wedge q_2^{-1}g^{-1}0 \\ &= q_1^{-1}\mathsf{Ker} f \wedge q_2^{-1}\mathsf{Ker} g\end{aligned}$$

The other equalities for image and kernel follows from Lemma 40. □

Dually, such a unique map also exists if G is a biproduct and H satisfies some of the conditions of a biproduct.

Corollary 50. *Biproducts are unique up to isomorphism.*

Proof. If both G and H are a biproduct of X and Y, then $1_X \times 1_Y : G \to H$ is an isomorphism. □

For groups X and Y, let $X \times Y$ denote a chosen biproduct of X and Y.

Corollary 51. *The following holds for any groups and morphisms:*

- $1_X \times 1_Y = 1_{X \times Y}$*;*
- $(u \times v)(f \times g) = uf \times vg$*, when ever the compositions are defined.*

Theorem 52. *Suppose for*

$$\begin{tikzcd} X \arrow[r, shift left, "d_1"] & H \arrow[l, shift left, "q_1"] \arrow[r, shift left, "q_2"'] & Y \arrow[l, shift left, "d_2"'] \end{tikzcd}$$

we have

- $q_1 d_1 = 1_X$*;*
- $q_2 d_2 = 1_Y$*;*
- $\mathsf{Ker}(q_1) = \mathsf{Im}(d_2)$*;*
- $\mathsf{Ker}(q_2) = \mathsf{Im}(d_1)$*.*

Then H with those four maps is a biproduct.

Proof. Suppose $X \times Y$ is the biproduct of X and Y with respective embeddings and projections e_1, e_2, p_1 and p_2. Let $h: X \times Y \to H$ be the unique isomorphism such that $he_1 = d_1$, $he_2 = d_2$, $q_1 h = p_1$, and $q_2 h = p_2$. For $f: X \to W$ and $g: Y \to W$, suppose

$$e: W \to C \leftarrow X \times Y : m$$

is the colimit of $\mathsf{C}_{X\times Y}(f,g)$. Consider

$$e\colon W \to C \leftarrow H\colon mh^{-1}.$$

It is a cocone of $\mathsf{C}_H(f,g)$, since

$$mh^{-1}d_1 = me_1 = ef \quad \text{and} \quad mh^{-1}d_2 = me_2 = eg.$$

Take any cocone of $\mathsf{C}_H(f,g)$

$$d\colon W \to L \leftarrow H\colon n.$$

Then

$$d\colon W \to L \leftarrow X \times Y\colon nh$$

is a cocone of $\mathsf{C}_{X\times Y}(f,g)$. Thus there is an unique $k\colon C \to L$ such that $ke = d$ and $km = nh$. That is, there is an unique $k\colon C \to L$ such that $ke = d$ and $kmh^{-1} = n$. Thus

$$e\colon W \to C \leftarrow H\colon mh^{-1}$$

is the colimit of $\mathsf{C}_H(f,g)$.

Dually it will follow that: For any $f\colon W \to X$ and $g\colon W \to Y$,

$$e\colon W \leftarrow L \to H\colon hm$$

is the limit of $\mathsf{L}_H(f,g)$, where

$$e\colon W \leftarrow L \to G\colon m$$

is the limit of $\mathsf{L}_{X\times Y}(f,g)$.

Thus H with those four maps is a biproduct of X and Y. $\square$

The corollary below, will make use of the Second Isomorphism Theorem.

Corollary 53. *If G has two subgroups X and Y such that*

- *X and Y are both normal and conormal;*
- *$X \vee Y = 1$;*
- *$X \wedge Y = 0$,*

then G is a product of X and Y.

Proof. Notice that $G/X \cong Y$ (Second Isomorphism Theorem). Let $e_1\colon X \to G$ and $e_2\colon Y \to G$ be the embeddings corresponding to X and Y. Compose the projection corresponding to X, $G \to G/X$, with the isomorphism $G/X \cong Y$, and denote it by f. We have

$$fe_2 1 = fY = f(Y \vee X) = f1 = 1.$$

And also

$$(fe_2)^{-1}0 = e_2^{-1}f^{-1}0 = e_2^{-1}(X) = e_2^{-1}(X \wedge Y) = 0.$$

Thus fe_2 is an isomorphism. Let the inverse be a. Let $p_2 = af$. Then $p_2e_2 = 1_Y$ and

$$\mathsf{Ker}p_2 = X = \mathsf{Im}e_1.$$

Similar we can get a map $p_1 : G \to X$ such that $p_1e_1 = 1_X$ and $\mathsf{Ker}p_1 = \mathsf{Im}e_2$. Thus $G \cong X \times Y$. □

Corollary 54. *If $s : A \to B$ is an embedding and $f : B \to A$ is a projection such that $fs = 1_A$ and $\mathsf{Im}s$ is normal and $\mathsf{Ker}f$ is conormal, then*

$$B \cong \mathsf{Im}s \times \mathsf{Ker}f.$$

Proof. Both $\mathsf{Im}s$ and $\mathsf{Ker}f$ are normal and conormal. Also

$$0 = s1_A^{-1}0 = ss^{-1}f^{-1}0 = \mathsf{Im}s \wedge \mathsf{Ker}f$$

And dually

$$1 = \mathsf{Im}s \vee \mathsf{Ker}f$$

And thus $B \cong \mathsf{Im}s \times \mathsf{Ker}f$. □

Throughout the rest of this section, the biproduct of X and Y will be denoted by $X\times Y$, and the embeddings will be denoted by $e_1^{X\times Y} : X \to X\times Y$, $e_2^{X\times Y} : Y \to X\times Y$ and the projections by $p_1^{X\times Y} : X \times Y \to X$ and $p_2^{X\times Y} \to Y$.

The rest of this section is devoted to showing that these biproducts induces a monoidal structure on the codomain of the Noetherian form $F : \mathbb{B} \to \mathbb{C}$. Let 0 denote the zero object.

Lemma 55. *For any groups X, Y and Z,*

$$\begin{tikzcd} X \times Y \arrow[r, shift left, "1_X \times e_1^{Y\times Z}"] & X \times (Y \times Z) \arrow[l, shift left, "1_X \times p_1^{Y\times Z}"] \arrow[r, shift right, "p_2^{Y\times Z}p_2^{X\times(Y\times Z)}"'] & Z \arrow[l, shift right, "e_2^{X\times(Y\times Z)}e_2^{Y\times Z}"'] \end{tikzcd}$$

is a biproduct of $X \times Y$ and Z.

Proof. We have

$$((1_X \times p_1^{Y\times Z})(1_X \times e_1^{Y\times Z}) = (1_X1_X \times p_1^{Y\times Z}e_1^{Y\times Z} = 1_X \times 1_Y = 1_{X\times Y}$$

and also

$$p_2^{Y\times Z}p_2^{X\times(Y\times Z)}e_2^{X\times(Y\times Z)}e_2^{Y\times Z} = p_2^{Y\times Z}e_2^{Y\times Z} = 1_Z.$$

By Proposition 49, we also have

$$
\begin{aligned}
&\mathsf{Ker}(1_X \times p_1^{Y\times Z}) \\
=&e_1^{X\times(Y\times Z)}1_X^{-1}0 \vee e_2^{X\times(Y\times Z)}(p_1^{Y\times Z})^{-1}0 \\
=&e_1^{X\times(Y\times Z)}0 \vee e_2^{X\times(Y\times Z)}e_2^{Y\times Z}1 \\
=&e_2^{X\times(Y\times Z)}e_2^{Y\times Z}1 \\
=&\mathsf{Im}(e_2^{X\times(Y\times Z)}e_2^{Y\times Z}).
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{Im}(1_X \times e_1^{Y\times Z}) \\
=&(p_1^{X\times(Y\times Z)})^{-1}1_X 1 \wedge (p_2^{X\times(Y\times Z)})^{-1}e_1^{Y\times Z}1 \\
=&(p_1^{X\times(Y\times Z)})^{-1}1 \wedge (p_2^{X\times(Y\times Z)})^{-1}(p_2^{Y\times Z})^{-1}0 \\
=&(p_2^{X\times(Y\times Z)})^{-1}(p_2^{Y\times Z})^{-1}0 \\
=&\mathsf{Ker}(p_2^{Y\times Z}p_2^{X\times(Y\times Z)}).
\end{aligned}
$$

Thus $X \times (Y \times Z)$ is a biproduct of $X \times Y$ and Z with those four maps. □

Corollary 56. *For any groups X, Y and Z, we have*

- $1_X \times e_1^{Y\times Z}$ *and* $e_2^{X\times(Y\times Z)}e_2^{Y\times Z}$ *are jointly epic;*
- $1_X \times p_1^{Y\times Z}$ *and* $p_2^{Y\times Z}p_2^{X\times(Y\times Z)}$ *are jointly monic.*

Corollary 51 shows that the biproduct $\times \colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ is a functor.

Theorem 57. *For any groups X, Y and Z, there is a (unique) natural isomorphism*

$$\alpha\colon X \times (Y \times Z) \to (X \times Y) \times Z$$

such that

- $\alpha(1_X \times e_1^{Y\times Z}) = e_1^{(X\times Y)\times Z}$;
- $\alpha e_2^{X\times(Y\times Z)}e_2^{Y\times Z} = e_2^{(X\times Y)\times Z}$;
- $p_1^{(X\times Y)\times Z}\alpha = 1_X \times p_1^{Y\times Z}$;
- $p_2^{(X\times Y)\times Z}\alpha = p_2^{Y\times Z}p_2^{X\times(Y\times Z)}$.

In particular, biproduct of groups are associative (up to isomorphism).

Proof. From Lemma 55 and Proposition 49, such an isomorphism α exists.

To confirm the naturality of α, take any $f\colon A \to X$, $g\colon B \to Y$ and $h\colon C \to Z$, and consider the following diagram:

$$
\begin{array}{ccc}
A \times (B \times C) & \xrightarrow{\alpha} & (A \times B) \times C \\
\downarrow{\scriptstyle f \times (g \times h)} & & \downarrow{\scriptstyle (f \times g) \times h} \\
X \times (Y \times Z) & \xrightarrow{\alpha} & (X \times Y) \times Z)
\end{array}
$$

We have

$$\begin{aligned}
&((f\times g)\times h)\alpha(1_A\times e_1^{B\times C}) \\
=&((f\times g)\times h)e_1^{(A\times B)\times C} \\
=&e_1^{(X\times Y)\times Z}(f\times g) \\
=&\alpha(1_X\times e_1^{Y\times Z})(f\times g) \\
=&\alpha(1_Xf\times e_1^{Y\times Z}g) \\
=&\alpha(f1_A\times (g\times h)e_1^{B\times C}) \\
=&\alpha(f\times(g\times h))(1_A\times e_1^{B\times C})
\end{aligned}
\qquad
\begin{aligned}
&((f\times g)\times h)\alpha(e_2^{A\times(B\times C)}e_2^{B\times C}) \\
=&((f\times g)\times h)e_2^{(A\times B)\times C} \\
=&e_2^{(X\times Y)\times Z}h \\
=&\alpha(e_2^{X\times(Y\times Z)}e_2^{Y\times Z})h \\
=&\alpha e_2^{X\times(Y\times Z)}(g\times h)e_2^{B\times C} \\
=&\alpha(f\times(g\times h))(e_2^{A\times(B\times C)}e_2^{B\times C}).
\end{aligned}$$

Since $1_A\times e_1^{B\times C}$ and $e_2^{A\times(B\times C)}e_2^{B\times C}$ is jointly epic, that diagram commutes. Thus α is a natural transformation.

□

Proposition 58. *For any group X, the morphisms*

$$p_2^{0\times X}\colon 0\times X\to X \quad \textit{and} \quad p_1^{X\times 0}X\times 0\to X$$

are natural isomorphisms, with inverses $e_2^{0\times X}$ and $e_1^{X\times 0}$ respectively.

Proof. The kernel of $p_2^{0\times X}$ is $e_1^{0\times X}1 = e_1^{0\times X}0 = 0$, since $\mathsf{sub}0$ only has one element. Thus $p_2^{0\times X}$ is an isomorphism. Similarly $p_1^{X\times 0}$ is an isomorphism.

For the naturality, for any $f\colon A\to X$, consider the diagram

$$\begin{tikzcd}
0\times A \arrow[r, "p_2"] \arrow[d, "1_0\times f"] & A \arrow[d, "f"] \\
0\times X \arrow[r, "p_2"] & X
\end{tikzcd}$$

From the definition of ‘biproduct of morphisms’, the diagram commutes. Thus $p_2^{0\times X}$ is natural in X. Similarly $p_1^{X\times 0}$ is natural in X.

Since $p_2^{0\times X}e_2^{0\times X} = 1_X$, $e_2^{0\times X}$ is the inverse of $p_2^{0\times X}$. Similarly $e_1^{X\times 0}$ is the inverse of $p_1^{X\times 0}$. □

Proposition 59. *We have that $p_1^{0\times 0} = p_2^{0\times 0}$.*

Proof. Since both of those morphisms have the same domain, and also have codomain 0, they are equal. □

Proposition 60. *For any A and C, the following diagram commutes*

$$\begin{tikzcd}
A \times (0 \times C) \arrow[r, "\alpha"] \arrow[d, "1_A \times p_2^{0\times C}"] & (A \times 0) \times C \arrow[d, "p_1^{A\times 0} \times 1_C"] \\
A \times C \arrow[r, "1_{A\times C}"] & A \times C
\end{tikzcd}$$

Proof. We have

$$\begin{aligned}
&(p_1^{A\times 0} \times 1_C)\alpha(1_A \times e_1^{0\times C}) \\
=&(p_1^{A\times 0} \times 1_C)e_1^{(A\times 0)\times C} \\
=&e_1^{A\times C}p_1^{A\times 0} \\
=&(1_A \times 0)e_1^{A\times 0}p_1^{A\times 0} \\
=&1_A \times 0 \\
=&(1_A \times p_2^{0\times C})(1_A \times e_1^{0\times C})
\end{aligned}
\qquad
\begin{aligned}
&(p_1^{A\times 0} \times 1_C)\alpha(e_2^{A\times(0\times C)}e_2^{0\times C}) \\
=&(p_1^{A\times 0} \times 1_C)e_2^{(A\times 0)\times C} \\
=&e_2^{A\times C} \\
=&e_2^{A\times C}p_2^{0\times C}e_2^{0\times C} \\
=&(1_A \times p_2^{0\times C})(e_2^{A\times(0\times C)}e_2^{0\times C})
\end{aligned}$$

Since $1_A \times e_1^{0\times C}$ and $e_2^{A\times(0\times C)}e_2^{0\times C}$ are jointly epic, the diagram commutes. □

Lemma 61. *For any groups X, Y and Z, $\alpha\colon X\times(Y\times Z) \to (X\times Y)\times Z$ satisfies the following:*

(1) $\alpha e_1^{X\times(Y\times Z)} = e_1^{(X\times Y)\times Z}e_1^{X\times Y}$;

(2) $\alpha e_2^{X\times(Y\times Z)} = e_2^{X\times Y} \times 1_Z$.

Proof. For (1), we have

$$p_1^{(X\times Y)\times Z}\alpha e_1^{X\times(Y\times Z)} = (1_X \times p_1^{Y\times Z})e_1^{X\times(Y\times Z)} = e_1^{X\times Y} = p_1^{(X\times Y)\times Z}e_1^{(X\times Y)\times Z}e_1^{X\times Y}$$
$$p_2^{(X\times Y)\times Z}\alpha e_1^{X\times(Y\times Z)} = p_2^{Y\times Z}p_2^{X\times(Y\times Z)}e_1^{X\times(Y\times Z)} = 0 = p_2^{(X\times Y)\times Z}e_1^{(X\times Y)\times Z}e_1^{X\times Y}.$$

Thus (1) holds.

For (2), we have

$$p_1^{(X\times Y)\times Z}\alpha e_2^{X\times(Y\times Z)} = (1_X \times p_1^{Y\times Z})e_2^{X\times(Y\times Z)} = e_2^{X\times Y}p_1^{Y\times Z} = p_1^{(X\times Y)\times Z}(e_2^{X\times Y} \times 1_Z)$$
$$p_2^{(X\times Y)\times Z}\alpha e_2^{X\times(Y\times Z)} = p_2^{Y\times Z}p_2^{X\times(Y\times Z)}e_2^{X\times(Y\times Z)} = p_2^{Y\times Z} = p_2^{(X\times Y)\times Z}(e_2^{X\times Y} \times 1_Z).$$

Thus (2) holds as well. □

Proposition 62. *For any groups A, B, C, and D, the following diagram commutes*

$$\begin{tikzcd}
A \times (B \times (C \times D)) \arrow[r, "\alpha_1"] \arrow[d, "1_A \times \alpha_3"] & (A \times B) \times (C \times D) \arrow[r, "\alpha_2"] & ((A \times B) \times C) \times D \\
A \times ((B \times C) \times D) \arrow[rr, "\alpha_4"] & & (A \times (B \times C)) \times D \arrow[u, "\alpha_5 \times 1_D"']
\end{tikzcd}$$

Proof. We have

$$
\begin{aligned}
&(\alpha_5 \times 1_D)\alpha_4(1_A \times \alpha_3)e_1^{A\times(B\times(C\times D))}\\
=&(\alpha_5 \times 1_D)\alpha_4 e_1^{A\times((B\times C)\times D)}\\
=&(\alpha_5 \times 1_D)e_1^{(A\times(B\times C))\times D}e_1^{A\times(B\times C)}\\
=&e_1^{((A\times B)\times C)\times D}\alpha_5 e_1^{A\times(B\times C)}\\
=&e_1^{((A\times B)\times C)\times D}e_1^{(A\times B)\times C}e_1^{A\times B}\\
=&\alpha_2 e_1^{(A\times B)\times(C\times D)}e_1^{A\times B}\\
=&\alpha_2\alpha_1 e_1^{A\times(B\times(C\times D))}.
\end{aligned}
$$

We also have:

$$
\begin{aligned}
&(\alpha_5 \times 1_D)\alpha_4(1_A \times \alpha_3)e_2^{A\times(B\times(C\times D))}\\
=&(\alpha_5 \times 1_D)\alpha_4 e_2^{A\times((B\times C)\times D)}\alpha_3\\
=&(\alpha_5 \times 1_D)(e_2^{A\times(B\times C)} \times 1_D)\alpha_3\\
=&(\alpha_5 e_2^{A\times(B\times C)} \times 1_D)\alpha_3\\
=&((e_2^{A\times B} \times 1_C) \times 1_D)\alpha_3\\
=&\alpha_2(e_2^{A\times B} \times (1_C \times 1_D)), \quad \text{since } \alpha \text{ is a natural isomorphism}\\
=&\alpha_2(e_2^{A\times B} \times 1_{C\times D})\\
=&\alpha_2\alpha_1 e_2^{A\times(B\times(C\times D))}.
\end{aligned}
$$

Thus the diagram commutes. □

Putting the last few theorems and propositions together, we get:

Theorem 63. $\langle \mathbb{C}, \times, 0, \alpha, p_2^{0\times -}, p_1^{-\times 0}\rangle$ *is a monoidal category.*

3.4 Commutators

Throughout this section, we will work with a fixed Noetherian form with biproducts.

Definition 20. For a group G and conormal subgroups X and Y, the *commutator* $[X,Y]_G$ is defined as follows: If

$$e\colon G \to C \leftarrow X \times Y : m$$

is the colimit of $\mathsf{C}_{X\times Y}(x,y)$, where $x\colon X \to G$ and $y\colon Y \to G$ are the respective embeddings of X and Y, then

$$[X,Y]_G = \mathsf{Ker}(e).$$

From the proof of Theorem 39, we see that in usual group theory, this commutator of X and Y would be the normal closure of the usual commutator of X and Y.

From Lemma 43 it follows that the projection in any colimit of $\mathsf{C}_{X\times Y}(x,y)$ has the same kernel, that is, if $u\colon G \to L \leftarrow X \times Y\colon v$ is another colimit, then $\mathsf{Ker}u = \mathsf{Ker}e$. Thus the commutator is well-defined.

Even more generally, we get:

Theorem 64. *For any $f\colon X \to W$ and $g\colon Y \to W$,if*

$$e\colon W \to C \leftarrow X \times Y\colon m$$

is the colimit of $\mathsf{C}_{X\times Y}(f,g)$, then

$$\mathsf{Ker}e = [\mathsf{Im}f, \mathsf{Im}g]_W.$$

Proof. Suppose $f = ak$ and $g = bl$ where $a\colon \mathsf{Im}f \to W$ is the embedding of the image of f and k is a projection of the kernel of f and $b\colon \mathsf{Im}g \to W$ is the embedding of the image of g and l is a projection of the kernel of g. Consider the following diagram, where

$$u\colon W \to L \leftarrow \mathsf{Im}f \times \mathsf{Im}g\colon v$$

is the colimit of $\mathsf{C}_{\mathsf{Im}f\times\mathsf{Im}g}(a,b)$,

$$\begin{tikzcd}
 & & W \arrow[dl, "u"'] \arrow[dr, "e"] & & \\
 & L \arrow[rr, dashed, shift left] & & C \arrow[ll, dashed, shift left] & \\
\mathsf{Im}f \arrow[uurr, bend left, "a"] \arrow[rr, "d_1"'] & & \mathsf{Im}f \times \mathsf{Im}g \arrow[ul, "v"] \arrow[ur, dashed, "m'"'] & & \mathsf{Im}g \arrow[uull, bend right, "b"'] \arrow[ll, "d_2"] \\
X \arrow[u, "k"] \arrow[rr, "e_1"'] & & X \times Y \arrow[u, "k\times l"] \arrow[uur, bend right] & & Y \arrow[u, "l"'] \arrow[ll, "e_2"]
\end{tikzcd}$$

where the unnamed arrow is m.

Since $v(k\times l)\colon X \times Y \to L \leftarrow W\colon u$ forms a cocone of $\mathsf{C}_{X\times Y}(f,g)$, we have $u^{-1}0 \geq e^{-1}0$.

Since we have

$$\begin{aligned}
&m(k\times l)^{-1}0\\
=&m(e_1k^{-1}0 \vee e_2l^{-1}0)\\
=&me_1k^{-1}0 \vee me_2l^{-1}0\\
=&efk^{-1}0 \vee egl^{-1}0\\
=&0,
\end{aligned}$$

$\mathsf{Ker}m \geq \mathsf{Ker}(k \times l)$. And since $k \times l$ is a projection, there exists unique $m'\colon \mathsf{Im}f \times \mathsf{Im}g \to C$ such that $m'(k \times l) = m$.

We also have

$$m'd_1k = m'(k \times l)e_1 = me_1 = ef = eak.$$

Since k is a projection, $m'd_1 = ea$. Similarly $m'd_2 = eb$. Thus C together with e and m' forms a cocone of $\mathsf{C}(a, b)$. Thus $e^{-1}0 \geq u^{-1}0$.

Thus $e^{-1}0 = u^{-1}0 = [\mathsf{Im}f, \mathsf{Im}g]_W$. □

Just an expected basic property:

Proposition 65. *For a product $X \times Y$, with respective embeddings e_1 and e_2,*

$$[e_1 1, e_2 1] = 0.$$

Proof. Since $1_X \times 1_Y\colon X \times Y \to X \times Y \leftarrow X \times Y\colon 1_{X\times Y}$ is a cocone of $\mathsf{C}_{X\times Y}(e_1, e_2)$, we have $[e_1 1, e_2 1] = 0$. □

Proposition 66. *If A, B, X, and Y are conormal subgroups of G, with $X \leq A$ and $Y \leq B$, then*

$$[X, Y] \leq [A, B].$$

Proof. Let $a\colon A \to G$ be the embedding of A. Since $X \leq A$, the embedding of X factors through a. Let $x\colon X \to A$ be the morphism such that $ax\colon X \to G$ is the embedding of X. Similarly, let $b\colon B \to G$ be the embedding of B, and $by\colon Y \to G$ be the embedding of Y.

If $e\colon G \to C \leftarrow A \times B\colon m$ is the colimit of $\mathsf{C}_{A\times B}(a, b)$, then

$$e\colon G \to C \leftarrow X \times Y\colon m(x \times y)$$

is a cocone of $\mathsf{C}_{X\times Y}(ax, by)$. Thus the kernel of e is greater or equal to the kernel of the colimit of $\mathsf{C}(ax, by)$. Thus

$$[X, Y] \leq [A, B].$$

□

Proposition 67. *For any conormal subgroups X and Y of G, we have*

$$[X, Y] \leq \overline{X}.$$

Proof. Let $x\colon X \to G$ and $y\colon Y \to G$ be embeddings with respective images being X and Y. Then,

$$p\colon G \to G/\overline{X} \leftarrow X \times Y\colon pyp_2$$

is a cocone of $\mathsf{C}(x, y)$, where p is the projection of X. Thus

$$\overline{X} = \mathsf{Ker}p \geq [X, Y].$$

□

Proposition 68. *Suppose $X \times Y$ is a biproduct of X and Y with respective embeddings e_1 and e_2. Then if for $f\colon X \to W$ and $g\colon Y \to W$, $[\mathsf{Im} f, \mathsf{Im} g] = 0$, then there exists an unique $h\colon X \times Y \to W$ such that $he_1 = f$ and $he_2 = g$.*

Proof. Suppose $e\colon W \to C \leftarrow X \times Y\colon m$ is the colimit of $\mathsf{C}(f, g)$. Then $\mathsf{Ker} e = 0$, and since e is a projection, e is an isomorphism. We have

$$e^{-1}me_1 = e^{-1}ef = f$$

and similarly $e^{-1}me_2 = g$.

Thus $e^{-1}m\colon X \times Y \to W$ is our desired h. Uniqueness follows from the jointly epicness of e_1 and e_2. □

Proposition 69. *For any group G and conormal subgroups X and Y such that $X \vee Y = 1$, if $[X, Y] = 0$, then both X and Y are normal subgroups of G.*

Proof. Since $[X, Y] = 0$, there is a morphism $m\colon X \times Y \to G$ such that me_1 is the embedding of X and me_2 is the embedding of Y. m is a projection, since

$$m1 = m(e_1 1 \vee e_2 1) = me_1 1 \vee me_2 1 = X \vee Y = 1.$$

Since $e_1 1$ and $e_2 1$ are normal subgroups of $X \times Y$, $me_1 1$ and $me_2 1$ are normal subgroups of G, that is, X and Y are normal subgroups of G. □

With the last few propositions together, we get:

Proposition 70. *For any group G such that $[G, G] = 0$, any conormal subgroup is normal.*

Theorem 71. *If group G has conormal subgroups X and Y such that*

- $X \vee Y = 1$,
- $X \wedge Y = 0$,
- $[X, Y]_G = 0$,

then $G \cong X \times Y$.

Proof. Those conditions implies that X and Y are also normal subgroups. Then by Corollary 53 the result follows. □

Proposition 72. *Suppose A, X, B are groups with trivial commutators and*

$$\begin{tikzcd} A \arrow[r, "g"] & X \arrow[r, shift left, "f"] & B \arrow[l, dashed, shift left, "s"] \end{tikzcd}$$

is a split short exact sequence, that is $\mathsf{Ker} f = \mathsf{Im} g$ and g is an embedding and f is a projection such that $fs = 1_B$, then

$$X \cong A \times B.$$

Proof. The image of s is normal, since the image of s is conormal and X has trivial commutators. Also, the kernel of f is conormal, since it is the image of g. Thus, by Corollary 54, we have

$$X \cong \mathsf{Ker}f \times \mathsf{Im}s \cong A \times B.$$

$\square$

Theorem 73. *For any $f\colon G \to H$ and conormal subgroups X and Y of G, we have*

$$\overline{f[X,Y]_G} = [fX, fY]_H.$$

Proof. Suppose e_1 and e_2 are the respective biproduct embeddings of product $X \times Y$. Suppose that $x\colon X \to G$ and $y\colon Y \to G$ are the embeddings of X and Y respectively. Suppose

$$e\colon G \to C \leftarrow X \times Y : m$$

is the colimit of $\mathsf{C}(x, y)$. And suppose that

$$d\colon H \to L \leftarrow X \times Y : n$$

is the colimit of $\mathsf{C}(fx, fy)$. Since

$$df\colon G \to L \leftarrow X \times Y : n$$

is a cocone of $\mathsf{C}(x, y)$, there is a unique $h\colon C \to L$ such that $he = df$ and $hm = n$.

Suppose that p is the projection of $fe^{-1}0$, and that $q\colon C \to D$ is the unique morphism such that $qe = pf$. Consider the following diagram

$$\begin{tikzcd}
H \arrow[dr, "p"] \arrow[drr, bend left, "d"] & & \\
G \arrow[u, "f"] \arrow[d, "e"'] & D \arrow[r, dashed, shift left, "k"] & L \arrow[l, dashed, shift left, "l"] \\
C \arrow[ur, "q"] \arrow[urr, bend right, "h"] & & \\
X \times Y \arrow[u, "m"] \arrow[uurr, bend right, "n"'] & &
\end{tikzcd}$$

By definition of p and q, and that e is a projection, and by Lemma 7, the full subdiagram containing C, G, H, and D is pushout diagram. Since we have $he = df$, there exists a unique k such that $kp = d$ and $kq = h$. We also have

$$(qm)e_1 = qex = (p)fx \quad \text{and} \quad (qm)e_2 = qey = (p)fy.$$

Thus $p\colon H \to D \leftarrow X \times Y : qm$ is a cocone of $\mathsf{C}(fx, fy)$. Thus there is a unique $l\colon L \to D$ such that $ln = qm$ and $ld = p$. We have

$$kln = kqm = hm = n \quad \text{and} \quad kld = kp = d.$$

Since L is a colimit, $kl = 1_L$. Thus l is an embedding. Since $ld = p$ and p is a projection, l is a projection. Thus l is an isomorphism, thus

$$\overline{f[X,Y]} = \mathsf{Ker}p = \mathsf{Ker}d = [fX, fY].$$

$\square$

Corollary 74. *If $[G,G]_G = 0$ and $f\colon G \to H$ is a projection, then $[H,H]_H = 0$.*

Corollary 75. *If $[G,G]_G = 0$ and $f\colon X \to G$ is an embedding, then $[X,X]_X = 0$.*

Corollary 76. *For any morphism $f\colon G \to H$ and conormal subgroups X and Y of G, we have $[fX, fY] = 0$ if and only if $\mathsf{Ker}f \geq [X,Y]$.*

Proof. We have

$$\begin{aligned} & [fX, fY] = 0 \\ \Leftrightarrow\quad & \overline{f[X,Y]} = 0 \\ \Leftrightarrow\quad & f[X,Y] = 0 \\ \Leftrightarrow\quad & \mathsf{Ker}f \geq [X,Y]. \end{aligned}$$

$\square$

Proposition 77. *For any group G and conormal subgroups X and Y such that $X \vee Y = 1$, if $[X,Y] \leq X$, then X is a normal subgroup of G.*

Proof. Suppose $p\colon G \to G/[X,Y]$ is the projection of $[X,Y]$. We have $[pX, pY] = 0$, and $pX \vee pY = 1$, and pX and pY are conormal subgroups. Thus by Proposition 69, pX is a normal subgroup of $G/[X,Y]$. Since X contains the kernel of p, $X = p^{-1}pX$. Thus X has to be normal as well. $\square$

The above result together with Proposition 67 gives:

Corollary 78. *For any group G and conormal subgroup X, X is normal if and only if $[G,X] \leq X$.*

Proposition 79. *For groups X and Y, we have*

$$[X \times Y, X \times Y]_{X\times Y} = e_1[X,X]_X \vee e_2[Y,Y]_Y.$$

Proof. Suppose

$$e\colon X \times Y \to C \leftarrow (X \times Y) \times (X \times Y)\colon m$$

is the colimit of $\mathsf{C}_{(X\times Y)\times(X\times Y)}(1_{X\times Y}, 1_{X\times Y})$. And

$$e_X\colon X \to C_X \leftarrow X \times X\colon m_X$$

is the colimit of $\mathsf{C}_{X\times X}(1_X, 1_X)$. We have, for $i = 1, 2$,

$$m(e_1^{X\times Y} \times e_1^{X\times Y})e_i^{X\times X} = me_i^{(X\times Y)^2}e_1^{X\times Y} = ee_1^{X\times Y}.$$

So $ee_1\colon X \to C \leftarrow X \times X\colon m(e_1^{X\times Y} \times e_1^{X\times Y})$ is a cocone of $\mathsf{C}_{X\times X}(1_X, 1_X)$. Thus

$$[X,X]_X \leq e_1^{-1}e^{-1}0 \quad \Rightarrow \quad e_1[X,X]_X \leq e^{-1}0 = [X\times Y, X\times Y].$$

Similarly we get $e_2[Y,Y]_Y \leq [X\times Y, X\times Y]$. Thus

$$e_1[X,X]_X \vee e_2[Y,Y]_Y \leq [X\times Y, X\times Y].$$

We also have, for $i = 1, 2$,

$$m_X(p_1^{X\times Y} \times p_1^{X\times Y})e_i^{(X\times Y)^2} = m_X e_i^{X\times X} p_1^{X\times Y} = e_X p_1^{X\times Y}.$$

Thus $e_X p_1\colon X\times Y \to C_X \leftarrow (X\times Y)^2\colon m_X(p_1 \times p_1)$ is a cocone of $\mathsf{C}(1_{X\times Y}, 1_{X\times Y})$. Thus we have

$$[X\times Y, X\times Y] = e^{-1}0 \leq p_1^{-1}e_X^{-1}0 = p_1^{-1}[X,X].$$

Similarly we have $[X\times Y, X\times Y] \leq p_2^{-1}[Y,Y]$. Thus we have

$$\begin{aligned}[X\times Y, X\times Y] \leq& p_1^{-1}[X,X] \wedge p_2^{-1}[Y,Y]\\ =& e_1[X,X] \vee e_2[Y,Y].\end{aligned}$$

The result then follows, since $e^{-1}0 = [X\times Y, X\times Y]_{X\times Y}$. $\square$

Corollary 80. *The commutator of the biproduct of two groups with trivial commutators, is trivial.*

Theorem 81. *Let $\mathbb{C}$ be a category equipped with a Noetherian form with biproducts, and $\mathbb{A}$ denote the full subcategory of the category of all groups with trivial commutators. Then, $\mathbb{A}$ is a reflective subcategory of $\mathbb{C}$.*

Proof. Take any $G \in \mathbb{C}_0$ and any morphism $f\colon G \to H$, where $[H,H]_H = 0$. Then $[fG, fG] = 0$, and so by Theorem 76 $\mathsf{Ker} f \geq [G,G]$. Thus, by one of the axioms of projective group theory, there is a unique $h\colon G/[G,G] \to H$ such that $he = f$, where $e\colon G \to G/[G,G]$ is the projection of $[G,G]$. Since $G/[G,G]$ has trivial commutators (by Theorem 76), $G/[G,G]$ is the reflection of G in $\mathbb{A}$. And thus $\mathbb{A}$ is a reflective subcategory of $\mathbb{C}$. $\square$

Proposition 82. *Internal monoids are exactly groups with trivial commutators.*

Proof. Suppose $(M, m\colon M\times M \to M, u\colon 0 \to M)$ is an internal monoid. Then in particular the following diagram commutes

$$\begin{tikzcd}
0\times M \arrow[r, "u\times 1"] \arrow[dr, "p_2^{0\times M}"'] & M\times M \arrow[d, "m"] \\
 & M
\end{tikzcd}$$

Then we have

$$me_2^{M\times M} = m(u\times 1)e_2^{0\times M} = p_2^{0\times M}e_2^{0\times M} = 1_M.$$

Similarly we get that $me_1^{M\times M} = 1_M$. So $1_M\colon M \to M \leftarrow M\times M\colon m$ has to be the colimit of $\mathsf{C}_{M\times M}(1_M, 1_M)$. Thus $[M,M] = \mathsf{Ker}1_M = 0$.

Conversely, suppose $[M,M]=0$. Let $m\colon M\times M \to M$ be the unique morphism such that $me_1^{M\times M} = 1_M = me_2^{M\times M}$, and let $u\colon 0\to M$ be the unique 0-morphism. Then following diagram commutes

$$\begin{tikzcd}
0\times M \arrow[r, "u\times 1"] \arrow[dr, "p_2^{0\times M}"'] & M\times M \arrow[d, "m"] & M\times 0 \arrow[l, "1\times u"'] \arrow[dl, "p_1^{M\times 0}"] \\
& M &
\end{tikzcd}$$

since

$$m(u\times 1)e_2^{0\times M} = me_2^{M\times M} = 1_M = p_2^{0\times M}e_2^{0\times M},$$

$$m(u\times 1)e_1^{0\times M} = u = p_2^{0\times M}e_1^{0\times M}.$$

Similarly the other triangle commutes.

Consider the diagram:

$$\begin{tikzcd}
M\times(M\times M) \arrow[r, "\alpha"] \arrow[d, "1\times m"] & (M\times M)\times M \arrow[r, "m\times 1"] & M\times M \arrow[d, "m"] \\
M\times M \arrow[rr, "m"] & & M
\end{tikzcd}$$

We have

$$\begin{aligned}
& m(m\times 1)\alpha(1\times e_1^{M\times M}) \\
=& m(m\times 1)e_1^{(M\times M)\times M} \\
=& me_1^{M\times M}m \\
=& m \\
=& m(1\times 1) \\
=& m(1\times me_1^{M\times M}) \\
=& m(1\times m)(1\times e_1^{M\times M})
\end{aligned}
\qquad
\begin{aligned}
& m(m\times 1)\alpha e_2^{M\times(M\times M)}e_2^{M\times M} \\
=& m(m\times 1)e_2^{(M\times M)\times M} \\
=& me_2^{M\times M} \\
=& 1 \\
=& me_2^{M\times M}me_2^{M\times M} \\
=& m(1\times m)e_2^{M\times(M\times M)}e_2^{M\times M}
\end{aligned}$$

Thus the diagram commutes. Thus (M,m,u) is an internal monoid. $\square$

Chapter 4

Some Remarks in Classical Group Theory

4.1 Distinguishing Cyclic Groups

In this section we explore how we could identify cyclic groups among other groups. This question came up from thinking about how one could define cyclic groups in projective group theory.

The following theorem is due to Ore proved in [9], which will also be used in some proofs in this section:

Theorem 83. *A group is locally cyclic if and only if its subgroup lattice is distributive.*

A group is locally cyclic if every finitely generated subgroup is cyclic. So in the special case of finite groups, this becomes: A finite group is cyclic if and only if its subgroup lattice is distributive.

Distinguishing Cyclic Groups Among Finite Groups

We will make use of the following two lemmas:

Lemma 84. *Suppose G is a finite group, and H and N are normal and cyclic subgroups and have relatively prime order, then $H \vee N$ is a normal cyclic subgroup.*

Proof. Since the order of H and N is relatively prime, $H \wedge N = 0$. Thus $H \times N \cong H \vee N$. Since both are cyclic, and have relatively prime order, $H \vee N$ is also cyclic. Since both H and N are normal subgroups, $H \vee N$ is a normal subgroup as well. $\square$

This is a formulation of First Sylow Theorem in [2] (p. 324):

Lemma 85. *Let G be a finite group and let $|G| = p^n m$ where $n \geq 1$ and prime p does not divide m. Then*

(1) G contains a subgroup of order p^i for each i where $1 \leq i \leq n$,

(2) *Every subgroup H of G of order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i < n$.*

The main result in this section is, where $\leq$ on $\mathbb{N}$ will denote the divisibility relation, and not the usual order relation:

Theorem 86. *For a finite group G, the following are equivalent:*

(1) *G is cyclic;*

(2) $\forall_{A,B \in \mathsf{sub}G}(A \cong B \Rightarrow A = B)$;

(3) $\forall_{A,B \in \mathsf{sub}G}(|A| = |B| \Rightarrow A = B)$;

(4) $\forall_{A,B \in \mathsf{sub}G}(|A| \leq |B| \Rightarrow A \leq B)$;

(5) *for any two parallel morphisms $m, f \colon M \to G$ into G, where m is a monomorphism, there is a unique $h \colon M \to M$ such that $mh = f$.*

Proof. (1) implies (2). Suppose (2) holds. Since for any subgroup N and element g, N and gNg^{-1} are isomorphic, they are forced to be the same subgroup. Thus all subgroups are normal. Also, for every Sylow p-subgroup S_p, $\mathsf{sub}S_p$ has to be a chain by Lemma 85. In particular the subgroup lattice is distributive, thus S_p is a cyclic group. By applying Lemma 84 inductively, we get that $G = \bigvee_{p \text{ prime}} S_p$ is cyclic, where S_p represents the unique Sylow p-subgroup for each prime p. Thus (1) is equivalent to (2).

(1) implies (3). Also, (3) implies (2), which implies (1). Thus (1) is equivalent to (3).

(1) implies (4). Also, (4) implies (3), which implies (1). Thus (1) is equivalent to (4).

Suppose (1) is true. Since $\mathsf{Im}f \cong M/\mathsf{Ker}f$, we have $|\mathsf{Im}f| \leq |M| = |\mathsf{Im}m|$. Since G is cyclic, we have $\mathsf{Im}f \leq \mathsf{Im}m$. Since m is a monomorphism and $\mathsf{Im}f \leq \mathsf{Im}m$, there exists a unique $h \colon M \to M$ such that $mh = f$, namely the morphism defined by $hx = a$ where a is the unique element of M such that $fx = ma$. So (1) implies (5).

Suppose (5) holds. Take any subgroups A and B of G such that $A \cong B$. Then there are two parallel morphisms $m, n \colon A \to G$, where m is the inclusion of A into G and n is an isomorphism $A \to B$ followed by the inclusion of B into G. Then there is an $h \colon A \to A$ such that $mh = n$. Since n is a monomorphism, h is also a monomorphism. Since A is finite, h is therefore an isomorphism. Since h is an isomorphism and $mh = n$, $\mathsf{Im}m = \mathsf{Im}n$. That is, $A = B$. So (5) implies (2), which implies (1). Thus (1) is equivalent to (5). □

The "dual" (assuming the dual of finite groups is finite groups) of (5) is that for any two parallel morphisms $e, g \colon G \to E$ from G, where e is an epimorphism, there is an $h \colon E \to E$ such that $he = g$. The finite groups satisfying this is not only cyclic groups. For example, finite simple groups satisfies this property as well.

Distinguishing Cyclic Groups Among Finite Abelian Groups

The main result of this section is that a finite abelian group A is cyclic if and only if $(\mathsf{hom}(A, A), +, 0)$ is cyclic.

We will prove that classification by making use of the following lemmas:

Lemma 87. *For any $n, m \in \mathbb{N}$ we have $|\mathsf{hom}(\mathbb{Z}_n, \mathbb{Z}_m)| = \gcd(n, m)$.*

Proof. Any morphism from $\mathbb{Z}_n$ is uniquely determine where it maps 1 to. Let k denote the group homomorphism $\mathbb{Z}_n \to \mathbb{Z}_m$ mapping 1 to k. We have

$$\begin{aligned} & k \text{ is a morphism} \\ \Leftrightarrow\ & m \mid kn \\ \Leftrightarrow\ & \frac{m}{\gcd(m,n)} \mid k\frac{n}{\gcd(m,n)} \\ \Leftrightarrow\ & \frac{m}{\gcd(m,n)} \mid k. \end{aligned}$$

There is exactly $\gcd(m, n)$ such values for k satisfying less than m. □

Lemma 88. *For any two finite abelian groups A and B, we have that $|\mathsf{End}(A)||\mathsf{End}(B)|$ divides $|\mathsf{End}(A \oplus B)|$.*

Proof. The following bijections follows from the universal property of product and coproduct:

$$\begin{aligned} & \mathsf{hom}(A \oplus B, A \oplus B) \\ \approx\ & \mathsf{hom}(A \oplus B, A) \times \mathsf{hom}(A \oplus B, B) \\ \approx\ & \mathsf{hom}(A, A) \times \mathsf{hom}(A, B) \times \mathsf{hom}(B, A) \times \mathsf{hom}(B, B), \end{aligned}$$

Taking cardinalities of the first and last sets, we get the result. □

By inductively applying the above lemma, we get:

Corollary 89. *If $A \cong \mathbb{Z}_{p^{a_1}} \times \ldots \times \mathbb{Z}_{p^{a_k}} \times B$, then $p^{a_1+\ldots+a_k}$ divides $|\mathsf{hom}(A, A)|$.*

Now for the result.

Theorem 90. *In the abelian category of finite abelian groups, a group A is cyclic if and only if $(\mathsf{hom}(A, A), +, 0)$ is a cyclic. Furthermore,*

$$\mathsf{hom}(\mathbb{Z}_n, \mathbb{Z}_n) \cong \mathbb{Z}_n.$$

Proof. Suppose A is a finite cyclic group $\mathbb{Z}_n$. Since $|\mathsf{hom}(\mathbb{Z}_n, \mathbb{Z}_n)| = n$, and $1_{\mathbb{Z}_n}$ have order n in group $\mathsf{hom}(\mathbb{Z}_n, \mathbb{Z}_n)$, $\mathsf{hom}(\mathbb{Z}_n, \mathbb{Z}_n)$ is a cyclic group of order n.

Conversely, suppose that A is a non-cyclic finite abelian group. Then

$$A \cong \mathbb{Z}_{p^{a_1}} \times \ldots \times \mathbb{Z}_{p^{a_k}} \times B,$$

where p is some prime, $a_1, \ldots, a_k \neq 0$, and $k \geq 2$, and $p \nmid |B|$. Let $a = \max\{a_1, \ldots, a_k\}$. Then, for any $x \in A$, we have $p^{a+1} \nmid \mathsf{o}(x)$, the order of x. Since for any $f \in \mathsf{hom}(A, A)$, $\mathsf{o}(f) = \mathsf{lcm}\{y \in A \mid y \in \mathsf{Im} f\}$, we also have $p^{a+1} \nmid \mathsf{o}(f)$. But since $p^{a+1} \mid |\mathsf{hom}(A, A)|$, $\mathsf{hom}(A, A)$ cannot be cyclic. □

4.2 Coinner Automorphisms

In this section we will show that the only "coinner automorphism" of a group is exactly the identity morphism.

In the paper [10] of P. Schupp, the following characterization of inner automorphisms is proved:

Theorem 91. *Let G be a group and let α be an automorphism of G. The automorphism α is an inner automorphism of G if and only if α has the property that whenever G is embedded in a group H then α extends to some automorphism of H.*

The statement of the following theorem is a slight generalization of his characterization.

Theorem 92. *If $\alpha\colon G \to G$ is an automorphism of group G, then α is an inner automorphism if and only if for any homomorphism $f\colon G \to H$ there is an automorphism i of H such that the following diagram commutes:*

$$\begin{tikzcd} H \arrow[r, "i"] & H \\ G \arrow[u, "f"] \arrow[r, "\alpha"] & G \arrow[u, "f"'] \end{tikzcd}$$

Proof. Suppose α is an inner automorphism of G, suppose $\alpha(x) = gxg^{-1}$ for all $x \in G$. Take any $f\colon G \to H$. Define $i\colon H \to H$ as $i(h) = f(g)hf(g)^{-1}$. i is in particular an automorphism. We have, for any $x \in G$,

$$f\alpha(x) = f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = if(x).$$

Thus the diagram commute.

Conversely, suppose that for any $f\colon G \to H$, there is an automorphism i of H such that $if = f\alpha$. In particular for any embedding $f\colon G \to H$, α extends to an automorphism of H. Then by the previous theorem, α is an inner automorphism of G. $\square$

If the above characterization is used as a definition for inner automorphisms, then the dual is:

Definition 21. An automorphism $\alpha\colon G \to G$ is a *coinner automorphism* if and only if for any homomorphism $f\colon H \to G$ there is an automorphism i of H such that

$$\begin{tikzcd} G \arrow[r, "\alpha"] & G \\ H \arrow[u, "f"'] \arrow[r, "i"] & H \arrow[u, "f"'] \end{tikzcd}$$

commutes.

Notice that 1_G is a coinner automorphism: just pick $i = 1_H$.

To show that the coinner automorphisms are exactly the identity morphisms, we will be making use of "semidirect products" of groups which was found in Mac Lane and Birkhoff's Algebra Book [8].

Definition 22. For groups B and H and a group homomorphism $\theta\colon H \to \mathsf{Aut}B$, one could define an operation on $B \times H$ as

$$(b, g)(c, h) = (b\theta g(c), gh).$$

$B \times H$ under this operation is called the *semidirect* product of B and H relative to θ, and will be denoted by $B \times_\theta H$.

Proposition 93. *For groups B and H and a group homomorphism $\theta\colon H \to \mathsf{Aut}B$, $B \times_\theta H$ is a group.*

Proof. The operation is associative: For any $a, b, c \in B$ and $f, g, h \in H$, we have

$$\begin{aligned}((a, f)(b, g))(c, h) &= (a\theta f(b), fg)(c, h)\\ &= ((a\theta f(b))\theta(fg)(c), (fg)h)\\ &= (a(\theta f(b))(\theta f(\theta g(c))), f(gh))\\ &= (a\theta f(b\theta(g)c), f(gh))\\ &= (a, f)(b\theta g(c), gh)\\ &= (a, f)((b, g)(c, h)).\end{aligned}$$

Also, for any $b \in B$ and $h \in H$, we have

$$(1, 1)(b, h) = (1\theta(1)b, 1h) = (b, h)$$

Thus $(1, 1)$ is a left unit for this operation. And for any $b \in B$ and $h \in H$, we have

$$(\theta(h^{-1})b^{-1}, h^{-1})(b, h) = ((\theta(h^{-1})b^{-1})(\theta(h^{-1})b), h^{-1}h) = (1, 1).$$

Thus every element has a left inverse. Thus $B \times_\theta H$ is a group. $\square$

A consequence of the following lemma is that we only need to prove that the coinner automorphisms of cyclic groups are the identity morphisms:

Lemma 94. *If $c\colon G \to G$ is coinner, and the following diagram commutes*

$$\begin{tikzcd} G \arrow[r, "c"] & G \\ S \arrow[u, "m"] \arrow[r, "s"] & S \arrow[u, "m"'] \end{tikzcd}$$

where m is a monomorphism and s in an automorphism, then s is also coinner.

Proof. For any $f\colon H \to S$, consider diagram

$$\begin{tikzcd} G \arrow[r, "c"] & G \\ S \arrow[u, "m"] \arrow[r, "s"] & S \arrow[u, "m"] \\ H \arrow[u, "f"] & H \arrow[u, "f"] \end{tikzcd}$$

Since c is a coinner automorphism, there exists $i \in \mathsf{Aut}H$ such that $mfi = cmf$. Since we also have $cm = ms$, we have $mfi = cmf = msf$. Since m is a monomorphism, $fi = sf$. Thus s is also coinner. $\square$

First we are going to show that the coinner automorphisms of cyclic groups are the identity morphisms, then we are going to show how this lemma is applied to prove the classification of coinner automorphisms.

Theorem 95. *The only coinner automorphism of* $\mathbb{Z}$ *is* $1_{\mathbb{Z}}$.

Proof. There are only two automorphisms of $\mathbb{Z}$: the identity and u, which maps 1 to -1.

We are going to construct a homomorphism $f\colon H \to \mathbb{Z}$ such that there is no automorphism i of H such that $fi = uf$. The domain will be a suitable semidirect product: Let $u_k\colon \mathbb{Z}_5 \to \mathbb{Z}_5$ denote the homomorphism mapping 1 to k. Let $\varphi\colon \mathbb{Z} \to \mathsf{Aut}(\mathbb{Z}_5)$ be the group homomorphism mapping 1 to u_2. So $4n$ maps to $u_1 = 1_{\mathbb{Z}_5}$, $4n+1$ to u_2, $4n+2$ to u_4, $4n+3$ to u_3. Take the homomorphism $\pi_2\colon H \to \mathbb{Z}$ mapping (a, b) to b, and suppose there is an automorphism i of H such that $\pi_2 i = u\pi_2$. Then i fixes the kernel of π_2. Thus i restricts to an automorphism j of $\mathbb{Z}_5$. So for any $a \in \mathbb{Z}_5$, we have $i(a, 0) = (ja, 0)$. Since $\pi_2 i = u\pi_2$, for any $(a, b) \in H$ we have $i(a, b) = (y, -b)$ for some y. For $b \in \mathbb{Z}$, let $x_b \in \mathbb{Z}_5$ be the element such that $i(0, b) = (x_b, -b)$. Since i is a morphism, we have

$$\begin{aligned} i((0,2) + (1,0)) &= i(\varphi(2)1, 2) \\ &= i(4, 2) \\ &= i((4,0) + (0,2)) \\ &= (j4, 0) + (x_2, 3) \\ &= (j4 + x_2, 3). \end{aligned}$$

And also

$$\begin{aligned} i(0,2) + i(1,0) &= (x_2, 3) + (j1, 0) \\ &= (x_2 + \varphi(3)j1, 3) \\ &= (3j1 + x_2, 3) \\ &= (j3 + x_2, 3). \end{aligned}$$

Thus $j4 = j3$, but this cannot be, since j is an automorphism. Contradiction. So there doesn't exist an $i \in \mathsf{Aut}(H)$ such that $\pi_2 i = u\pi_2$. Thus $u\colon \mathbb{Z} \to \mathbb{Z}$ in not coinner. Thus the only coinner automorphism of $\mathbb{Z}$ is the identity. $\square$

To show that the only coinner automorphisms of $\mathbb{Z}_n$ is the identity, we are going to make use of the following two well-known theorems:

Theorem 96. *If F is a finite field, then $(F^*, \cdot, 1)$ is cyclic.*

Corollary 97. *For a prime p, $\mathsf{Aut}(\mathbb{Z}_p)$ is cyclic and isomorphic to $\mathbb{Z}_{p-1}$.*

Proof. Any homomorphism of $\mathbb{Z}_p$ is uniquely determined to where 1 is mapped to. The automorphisms is exactly those homomorphisms mapping 1 to the non-identity elements. So the map $\mathsf{Aut}(\mathbb{Z}_p) \to \mathbb{Z}_p^*$, $f \mapsto f(1)$, is a bijection. That map is also a morphism of function composition to multiplication, thus an isomorphism. Since the codomain is a cyclic group by the previous theorem, $\mathsf{Aut}(\mathbb{Z}_p)$ is a cyclic group (with order $p-1$). $\square$

Theorem 98 (Dirichlet's Theorem On Arithmetic Progressions)**.** *If a and d are relatively prime natural numbers, then the set $\{a, a+d, a+2d, \ldots\}$ contains infinitely many primes.*

Lemma 99. *If $\alpha\colon G \to G$ is coinner, then for any $g \in G$, $\alpha g = g$ or $\alpha g = g^{-1}$.*

Proof. Take the homomorphism $f_g\colon \mathbb{Z} \to G$ which maps 1 to g. Since α is a coinner automorphism, there is an automorphism i of $\mathbb{Z}$ such that $f_g i = \alpha f_g$. There is only two automorphisms of $\mathbb{Z}$: the identity morphism and the morphism that maps 1 to -1. If i is the identity morphism, then plugging in 1 on both sides, we get $g = \alpha g$. If i is the other automorphism, then plugging in 1 on both sides, we get $g^{-1} = \alpha g$. $\square$

Theorem 100. *The only coinner automorphism of $\mathbb{Z}_n$, for $n \in \mathbb{N}$, is the identity.*

Proof. This is clear for $n = 0$ and $n = 1$ and $n = 2$. So suppose $n \geqslant 3$. The only other possible coinner automorphism (other than identity) is $u\colon \mathbb{Z}_n \to \mathbb{Z}_n$ mapping 1 to $n-1$.

There is a prime number of the form $q = 1 + dn$ for $d \in \mathbb{N}$. Then $\mathsf{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_{dn}$. So there exists some injective group morphism

$$\varphi\colon \mathbb{Z}_n \to \mathsf{Aut}(\mathbb{Z}_q).$$

Let $H = \mathbb{Z}_q \times_\varphi \mathbb{Z}_n$. And suppose $\alpha\colon H \to H$ is an automorphism such that $\pi_2\alpha = u\pi_2$. α fixes the kernel of π_2, thus restricts to an isomorphism β of $\mathbb{Z}_q$. Thus for any $a \in \mathbb{Z}_q$,

$$\alpha(a, 0) = (\beta a, 0).$$

Let $\alpha(0,1) = (x, n-1)$ and suppose $\varphi(1) = u_y$, the automorphism mapping 1 to y. Then

$$\begin{aligned}
\alpha((0,1)+(1,0)) &= \alpha(\varphi(1)1, 1)\\
&= \alpha(y,1)\\
&= \alpha(y,0) + \alpha(0,1)\\
&= (\beta y, 0) + (x, n-1)\\
&= (\beta y + x, n-1)\\
&= (y\beta 1 + x, n-1).
\end{aligned}$$

And also

$$\begin{aligned}
\alpha(0,1) + \alpha(1,0) &= (x, n-1) + (\beta 1, 0)\\
&= (x + \varphi(n-1)(\beta 1), n-1)\\
&= (x + \varphi(1)^{-1}(\beta 1), n-1)\\
&= ((\varphi(1)^{-1}(\beta 1) + x, n-1).
\end{aligned}$$

So we have

$$\begin{aligned}
&y\beta 1 = (\varphi(1)^{-1})(\beta 1)\\
&\text{implies } \varphi(1)(y\beta 1) = \beta 1\\
&\text{implies } y^2\beta 1 = \beta 1\\
&\text{implies } y^2 = 1 \text{ since } \beta \text{ is an isomorphism and } 1 \neq 0
\end{aligned}$$

But $y^2 = 1 \pmod{q-1}$ implies that the order of $\varphi(1)$ is 2 and not n, contradicting the fact that φ is an injective group homomorphism. Thus the only coinner automorphism $\mathbb{Z}_n \to \mathbb{Z}_n$ is the identity. $\square$

Theorem 101. *For any group G, if $c\colon G \to G$ is coinner, then $c = 1_G$.*

Proof. Take any $g \in G$. Let H be the cyclic subgroup generated by g, and $f\colon H \to G$ be the embedding of H into G. Since c is a coinner automorphism, there is an automorphism i of H such that $fi = cf$. Furthermore, since f is a monomorphism, i is also a coinner automorphism. Since H is a cyclic group, $i = 1_H$. We have

$$c(g) = cf(g) = fi(g) = f(g) = g.$$

Thus c fixes every element g of G. Thus c is the identity morphism. $\square$

4.3 On Sylow $\frac{1}{p}$-Subgroups and Their Conjugacy

Note: An examiner pointed out that a $\frac{1}{p}$-Sylow subgroup is closely related to a p-complement which is a special kind of Hall subgroup. There is extensive literature about such subgroups. For instance, it is known that the conjecture that was made in this section is true for all finite solvable groups (much more is true by a theorem of P. Hall [6]). From this one can recover Proposition 107 (by a theorem of Burnside [1]) and Proposition 111 (by the fact that a group with order square free is supersolvable). The examiner also did a calculation with GAP (a computer algebra system) that shows that the group $\mathsf{PSL}(3,2)$ (the second smallest non-abelian simple group) with order $2^3 \cdot 3 \cdot 7$ has two conjugacy classes of subgroups of order $2^3 \cdot 3$.

In this section we make a conjecture that the dual of a proposed definition of Sylow p-subgroups are conjugates. We will prove that this conjecture holds for some cases.

Definition 23. For a group G and prime p, a $\frac{1}{p}$-subgroup is a subgroup with index in G a power of p. A Sylow $\frac{1}{p}$-subgroup is a minimal such subgroup.

I'm making the following conjecture:

Conjecture 102. *For any group G and any prime p, all Sylow $\frac{1}{p}$-subgroups are conjugates.*

In some special cases I can demonstrate that they are conjugates.

Corollary 103. *If a group G contains a normal Sylow $\frac{1}{p}$-subgroup, then G has exactly one Sylow $\frac{1}{p}$-subgroup (and therefor satisfies the conjecture).*

Since in usual group theory Axiom 6 and its dual is true, where the norm function is order function, we have the following direct consequence:

Lemma 104. *For surjective morphism $f\colon G \to H$, and $X \leq H$, and $\mathsf{Ker}f \leq Y \leq G$, we have*

$$\frac{|G|}{|f^{-1}X|} = \frac{|H|}{|X|} \quad \textit{and} \quad \frac{|G|}{|Y|} = \frac{|H|}{|fY|}$$

Proposition 105. *If group A satisfies the conjecture, and $f\colon A \to B$ is a surjective homomorphism, then B also satisfies the conjecture.*

Proof. Suppose $X \in \mathsf{sub}B$ is a Sylow $\frac{1}{p}$-subgroup. The index of $f^{-1}X$ in A is still a power of p. Suppose that $U \leq f^{-1}X$ is a Sylow $\frac{1}{p}$-subgroup of A. We have,

$$\frac{|A|}{|U \vee \mathsf{Ker}f|} = \frac{|A|}{|f^{-1}fU|} = \frac{|B|}{|fU|}.$$

Since $U \leq (U \vee \mathsf{Ker}f)$, $\frac{|A|}{|U \vee \mathsf{Ker}f|}$ is a power of p. So index of fU is a power of p, and $fU \leq ff^{-1}X = X$. Since X is minimal subgroup with index power of p, $fU = X$.

Suppose Y is another Sylow $\frac{1}{p}$-subgroup of B. Then, by the same argument as above, there exists a Sylow $\frac{1}{p}$-subgroup V of A such that $fV = Y$. Since A satisfies the conjecture, there is some $g \in A$ such that $gUg^{-1} = V$. So,

$$(fg)X(fg)^{-1} = (fg)fU(fg)^{-1} = f(gUg^{-1}) = fV = Y.$$

And thus B also satisfies the conjecture. $\square$

Proposition 106. *If $|A| = p^a n$ and $|B| = p^b m$, where p does not divide m or n, and the order of a Sylow $\frac{1}{p}$-subgroup in A and in B are n and m respectively, and A and B satisfy the conjecture, and any Sylow $\frac{1}{p}$-subgroup of $A \times B$ has order nm, then $A \times B$ satisfies the conjecture.*

Proof. Suppose P is a Sylow $\frac{1}{p}$-subgroup of $A \times B$. Since $0 \times B = \pi_1^{-1}0$ is a normal subgroup of $A \times B$, we have

$$|(0 \times B) \vee P|\,|(0 \times B) \wedge P| = |P|\,|0 \times B|\,.$$

Notice $(0 \times B) \vee P = \pi_1 P \times B$. So by substituting in the orders and using the fact that $|X \times Y| = |X||Y|$, we get that $|\pi_1 P| \leq nm$ (where $\leq$ here means divides). But since it is a subgroup of A, $|\pi_1 P| \leq p^a n$. And thus $|\pi_1 P| \leq \mathsf{gcd}(p^a n, nm) = n$. Similarly $|\pi_2 P| \leq m$. We have

$$mn = |P| \leq |\pi_1 P \times \pi_2 P| \leq mn.$$

Thus $|\pi_1 P \times \pi_2 P| = nm$. And so $|\pi_1 P| = n$ and $|\pi_2 P| = m$, and thus $\pi_1 P$ and $\pi_2 P$ are Sylow $\frac{1}{p}$-subgroups of A and B respectively, and also $P = \pi_1 P \times \pi_2 P$.

So if you have another Sylow $\frac{1}{p}$-subgroup Q of $A \times B$, then $Q = \pi_1 Q \times \pi_2 Q$. Since $\pi_1 Q$ and $\pi_1 P$ are conjugates, and $\pi_2 Q$ and $\pi_2 P$ are also conjugates, P and Q are conjugates. $\square$

Just a remark, if a group has order $p^a q^b$ for distinct primes p and q, then a Sylow $\frac{1}{p}$-subgroup is a Sylow q-subgroup, and thus all Sylow $\frac{1}{p}$-subgroup are conjugates.

Proposition 107. *If a group has order $p^a q^b$ for natural numbers a and b and distinct primes p and q, then this group satisfies the conjecture.*

Proof. A Sylow $\frac{1}{p}$-subgroup here is exactly a Sylow q-subgroup. Thus all Sylow $\frac{1}{p}$-subgroups are conjugates (and all Sylow $\frac{1}{q}$-subgroups). $\square$

The following lemma is an analog of some lemma for Sylow subgroups.

Lemma 108. *If P is a Sylow $\frac{1}{p}$-subgroup, and X is a $\frac{1}{p}$-subgroup, and $X \leq \mathsf{N}(P)$, the normalizer of P, then $P \leq X$.*

Proof. We have $X \vee P \leq \mathsf{N}(P)$. So $P \triangleleft P \vee X$, and $P \wedge X \triangleleft X$. By the diamond isomorphism theorem their corresponding quotients are isomorphic. Taking cardinalities (and some rearrangement), and then, we get

$$|P \vee X||P \wedge X| = |P||X|.$$

Taking reciprocals on both sides, and multiplying both sides by $|G|^2$, we get (for some α),

$$\frac{|G|}{|P \wedge X|}\frac{|G|}{|P \vee X|} = \frac{|G|}{|P|}\frac{|G|}{|X|} = p^\alpha.$$

So in particular the index of $P \wedge X$ is a power of p, but P is minimal such. So $P \wedge X = P$, and thus $P \leq X$. $\square$

The following lemma is from [8] (Theorem II.21):

Lemma 109. *If a finite group G acts on a set X, then the number of points in the orbit of a point $y \in X$ is the index $[G : F_y]$ in G of the subgroup F_y fixing y.*

For a group G and subgroup Q, if Q acts on subgroups of G as $(q, S) \mapsto qSq^{-1}$, then denote the orbit of S by $[S]_Q$.

Corollary 110. *For a group G and subgroup Q, if Q acts on subgroups of G as $(q, S) = qSq^{-1}$, then for any subgroup S,*

$$|[S]_Q| = \frac{|Q|}{|Q \wedge \mathsf{N}(Q)|}.$$

For the following proof, we will use $\leq$ to denote divides.

Proposition 111. *If G is a group with order pqr, for distinct primes p, q, and r, then G satisfies the conjecture.*

Proof. With out loss of generality, suppose $p < q < r$.

Suppose that there exist Sylow $\frac{1}{p}$-subgroups P and Q which are not conjugates. We have $|P| = qr = |Q|$. Since they aren't conjugates, $\mathsf{N}(P) = P$. So $|[P]_G| = \frac{|G|}{|N_G(P)|} = p$. We also have that $|[P]_Q|$ has less elements than $|[P]_G| = p$, and also $|[P]_Q|$ divides $|Q| = qr$, thus $[P]_Q| = 1$, and thus $Q = Q \wedge \mathsf{N}(P)$, thus $Q = P$, which is a contradiction. Thus all Sylow $\frac{1}{p}$-subgroups are conjugates, and in fact there is at most one $\frac{1}{p}$-subgroup.

Suppose that there exist Sylow $\frac{1}{q}$-subgroups P and Q which are not conjugates. Again, then the normalizer of $\mathsf{N}(P) = P$, and so $|[P]_G| = q$. For any $X \in [P]_G$, $|[X]_Q| \neq 1$, since X is a $\frac{1}{p}$-subgroup and if $|[X]_Q = 1|$ then $X \leq \mathsf{N}_G(Q)$ which implies $X = Q$ thus Q and P are conjugates. For any $X \in [P]_G$, we have $|[X]_Q|$ divides $|Q| = pr$ and $|[X]_Q|$ is less than $|[P]_G| = q$. Thus $|[X]_Q| = p$. But that implies that $|[P]_G|$ is divisible by p. Contradiction. So all Sylow $\frac{1}{q}$-subgroups are conjugates.

Suppose that there exist Sylow $\frac{1}{r}$-subgroups P and Q which are not conjugates. Then $|[P]_G| = r$, since $\mathsf{N}(P) = P$. P has order pq, thus has a Sylow q-subgroup. Let n_q^P denote the number of Sylow q-subgroups in P. n_q^P divides pq and is equal to 1 mod q. So it has to be 1 (since $p < q$). Since any two Sylow q-subgroups in G are conjugates, any Sylow q-subgroup is contained in some X in $[P]_G$. So the number of Sylow q-subgroups in G, n_q, has to be less than r. Furthermore n_q divides pqr and is equal to 1 mod q, so $n_q = 1$ or $n_q = p$. Suppose $n_q = p$. Let S denote a Sylow q-subgroup of G. Then

$$p = n_q = |[S]_G| = \frac{|G|}{|\mathsf{N}(S)|} = \frac{pqr}{\mathsf{N}(S)}.$$

which implies $\mathsf{N}S = qr$. Thus N is the unique Sylow $\frac{1}{p}$-subgroup of G. For any other Sylow q-subgroup R, we have $R \leq \mathsf{N}(R) = \mathsf{N}(S)$, which implies $R = S$.

Contradiction. Thus $n_q = 1$. Then every X in $[P]_G$ and Q contains S as subgroup. For every X in $[P]_G$, we have

$$q = |S| \leq |X \wedge Q| < |Q| = pq.$$

So $X \wedge Q = S$. Then for every X in $[P]_G$, $|[X]_Q| = \frac{|Q|}{|Q \wedge \mathsf{N} X|} = \frac{|Q|}{|Q \wedge X|} = p$. But that implies that p divides r. Contradiction. So all Sylow $\frac{1}{r}$-subgroups has to be conjugates. $\square$

References

[1] W. Burnside, 1904, On Groups of Order $p^\alpha q^\beta$, Proc. London Math. Soc. (s2-1 (1)): 388392, doi:10.1112/plms/s2-1.1.388

[2] J. B. Fraleigh, A First Course in Abstract Algebra. 7th Ed. Pearson, 2003

[3] P. Freyd, Abelian Categories, Harper and Row, 1964

[4] A. Goswami and Z. Janelidze, Duality in non-abelian algebra IV. Duality for groups and a universal isomorphism theorem, preprint (arXiv:1704.01863)

[5] M. Grandis, On the categorical foundations of homological and homotopical algebra, Cah. Top. Gom. Diff. Catg. 33 (1992), 135–175

[6] P. Hall, 1928, A note on soluble groups, Journal L. M. S., 3(2): 98105, doi:10.1112/jlms/s1-3.2.98

[7] G. Janelidze, L. Márki, and W. Tholen, Semi-abelian categories. J. Pure Appl. Algebra 168 (2002), 367–386

[8] S. Mac Lane and G. D. Birkhoff, Algebra (third edition), AMS Chelsea Publishing, 1999

[9] O. Ore, Structures and group theory. II, Duke Math. J. 4, 1938, 247–269

[10] P. E. Schupp, A Characterization of Inner Automorphisms, Proceedings of the American Mathematical Society, Vol. 101, No. 2 (Oct., 1987), 226–228