Group theory

Course by: Professor Mariusz Wodzicki[0.1]
Notes by: Jackson Van Dyke[0.2]

Spring 2018

[0.1] With some visiting lectures given by Professor Nicolai Reshetikhin.

[0.2] Any errors introduced are my own.

Contents

0.1 Introduction

These notes were taken from Math 257 at UC Berkeley in spring 2018. The instructor was Professor Wodzicki. This course will focus on the structural theory of groups. There is of course much to be said about the representation theory of groups, but this will not be the focus of this course. It is recommended that the reader have some prior familiarity with algebraic structures before reading these notes.

When developing basic algebraic notions, it is common to first build a *semigroup*, which is a set equipped with a single associative binary relation. Then adding the additional criteria that this relation has an identity, turns this structure into a *monoid*. We finally insist on the existence of inverses, to get a *group*. We then add a second binary relation to get notions of *rings*, *fields*, and eventually *algebras*. These are all obviously important, particularly algebras, which show up everywhere. But these structures are important for what they *are*. This stands in juxtaposition with groups, which are primarily of interest for what they *do*. Particularly given how rudimentary the notion of a group is.

Group theory is at its core, the study of invariants. Take for example, geometric invariant theory. It is a basic fact regarding three dimensional cubic surfaces, that any non-singular such surface will contain exactly 27 lines. This is of course a surprising fact, but it provides a certain shared rigidity between these surfaces, and we can cleverly employ groups to give us a grasp on the symmetries and mappings between these surfaces. After all, a line must map to a line.

This is just one place we see the beauty and usefulness of groups. We start by introducing the preliminary concept of a biset, and develop some of the canonical G-set formalism in this more general context. After this, we reduce our concern to groups and G-sets. In this portion of the course we prove Burnside's theorem. We then consider Nilpotent groups. Here we meet p-groups, the Sylow theorems, the commutator calculus, and even some discussion of Lie-algebras. We then take a slight detour to consider Affine groups and Hopf algebras.

The next portion of these notes focuses briefly on the representation theory of groups.[0.1] After this we consider solvable groups, and begin our study of the Schur-Zassenhaus theorem. We prove the abelian case of this theorem with some methods from group homology. We then meet the Frattini argument and the more general solvable case of the Schur-Zassenhaus theorem. The final portion of these notes is on transfer and fusion. We take a novel approach to this, considering it from the point of view of Gauge groups, a concept we borrow from mathematical physics.

[0.1] This was the portion of the course taught by Professor Nicolai Reshetikhin.

Chapter 1

Preliminaries

We will be taking an approach similar to the general approach taken by Grothendieck. In particular, we will be starting very simple, introducing only what we absolutely need. We introduce some (likely new) concepts having to do with bisets, and introduce some categorical language you have likely seen before. We then introduce some basic definitions and examples of groups and group action. We take this opportunity to fix some notation for all of this.

1.1 Bisets

Definition 1.1. Given a set A, then a *left A-set* is a set X equipped with a pairing

$$\begin{aligned} A, X &\longrightarrow X \\ a, x &\longmapsto ax \end{aligned}$$

and a *right A-set* is a set X equipped with a pairing

$$\begin{aligned} X, A &\longrightarrow X \\ x, a &\longmapsto xa \end{aligned}$$

Remark 1.1. An A-set can be viewed as $\left(X, (\lambda_a)_{a\in A}\right)$ where λ_a are operations on X.

Definition 1.2. A function $f : X \to X'$ is a morphism of A-sets iff

$$f\left(ax\right) = af\left(x\right)$$

for all $a \in A$ and all $x \in X$.

Definition 1.3. A set X is an (A, B)-set iff it is a left A-set and right B-set. This is sometimes written ${}_AX_B$.

Remark 1.2. If $A = B$, we refer to (A, A) sets as A-bisets.

Definition 1.4. An (A, B)-set X is A, B *associative* iff for all $a \in A$, $b \in B$, $x \in X$, we have

$$(ax)\,b = a\,(xb)$$

It is also said to be A-*associative* iff $(a_1 a_2)\,x = a_1\,(a_2 x)$ for all $a_1, a_2 \in A$ and all $x \in X$. It is also said to be B-*associative* iff $(x b_1)\,b_2 = x\,(b_1 b_2)$.

This can also be written:

$$\left(X, (\lambda_a)_{a\in A}, (\rho_b)_{b\in B}\right)$$

So this can be viewed as a set paired with a lot of unary operations classified in two different ways. Then associativity states that there is a sense in which the different types of operations associate with one another. So we have associativity with no notion of explicit composition. We will be assuming all of our bisets are associative from now on.

Definition 1.5. A *category* $\mathbf{C}$ is a collection of objects $\mathrm{Obj}\,(\mathbf{C})$ such that for any $A, B \in \mathrm{Obj}\,(\mathbf{C})$, there is a collection $\mathrm{Mor}\,(A, B)$ of maps (or arrows or morphisms) from A to B. Also, for each $A, B, C \in \mathrm{Obj}\,(\mathbf{C})$ we have a function

$$\mathrm{Mor}\,(B, C) \times \mathrm{Mor}\,(A, B) \to \mathrm{Mor}\,(A, C)$$

where $(g, f) \mapsto g \circ f$ called composition. We also have the following conditions: Furthermore, for each $A \in \mathrm{Obj}\,(\mathbf{C})$, we have some element $\mathrm{id}_A \in \mathrm{Mor}\,(A, A)$ called the identity on A such that

1. Associativity: For each $f \in \mathrm{Mor}\,(A, B)\,, g \in \mathrm{Mor}\,(B, C)$ and $h \in \mathrm{Mor}\,(C, D)$ we have $(h \circ g) \circ f = h \circ (g \circ f)$.
2. Identity laws: For all $A, B \in \mathrm{Obj}\,(\mathbf{C})$, we have $\mathrm{id}_A \in \mathrm{Mor}\,(A, A)$ and $\mathrm{id}_B \in \mathrm{Mor}\,(B, B)$ such that for all $f \in \mathrm{Mor}\,(A, B)$, we have $f \circ \mathrm{id}_A = f = \mathrm{id}_B \circ f$.

We introduce some basic examples of categories.

Example 1.1. The category **Set** has sets as objects, and the morphisms are set theoretic functions. We also have the category **Grp** where the objects are groups, and the morphisms are homomorphisms. There are analogous categories for many algebraic structures. We also have the category **Top** which consists of topological spaces, where the morphisms are given by continuous maps. Not all categories are sets with additional structure. This type of category is called a *concrete category*.

Example 1.2. As an example of a category which is not a set with additional structure, consider the category with a single object, $\bullet$, let $\mathrm{Mor}\,(\bullet, \bullet) = G$ for some group G.

Example 1.3. If we fix a group G, then the G-sets form a category. We write this category as G-**set**. We also write two such G-sets as (X, λ) and (X', λ'). Then the morphisms in this category are elements of $\mathrm{Mor}_{\mathbf{Set}}(X, X')$ such that the following diagram commutes:

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\lambda_g"] & X' \arrow[d, "\lambda'_g"] \\
X \arrow[r, "f"] & X'
\end{tikzcd}$$

Example 1.4. Let's return to the setting of bisets. For any two sets A, B, there is a category with (A, B)-sets as the objects. We write this category **A-Set-B**.

Definition 1.6. Let A, B, C be sets. Now consider the bisets: ${}_AX_B$, ${}_BY_C$, and ${}_AZ_C$. Then $\alpha : X, Y \to Z.$ is A, B, C *balanced* iff

$$\alpha(ax, y) = a\alpha(x, y) \qquad \alpha(xb, y) = \alpha(x, by) \qquad \alpha(x, yc) = \alpha(x, y)c \tag{1.1}$$

respectively.

Now look at all of the A,B,C balanced pairings. These form a category in a natural way: given the following balanced pairings,

$$\begin{tikzcd}
 & Z \arrow[dd, dotted, "f"] \\
X, Y \arrow[ur, "\alpha"] \arrow[dr, "\alpha'"] & \\
 & Z'
\end{tikzcd}$$

then the morphism from $\alpha \to \alpha'$ in this category is given by a map $f : Z \to Z'$ such that the above diagram commutes. Now suppose you already have one such balanced pairing. Then if we apply any morphism of the corresponding bisets to the values, this is balanced automatically. This is said to be produced from the original pairing.

Definition 1.7. The target of the universal balanced pairing will be denoted by $X \times_B Y$. We will call this the tensor product of bisets.

Consider the following pairing

$$X, Y \longrightarrow X \times Y$$

$$x, y \longmapsto (x, y)$$

then this is already (A, C) balanced. Now compose this with a quotient map from an equivalence relation $\sim_B$

$$\begin{tikzcd}
X, Y \arrow[r] \arrow[dr] & X \times Y \arrow[d] \\
 & X \times Y / \sim_B
\end{tikzcd}$$

where $\sim_B$ is given by $(xb, y) \sim_B (x, by)$ now it is obvious the diagonal is B-balanced, so this is a balanced pairing.

Now we fix 3 sets: A,B,C, and corresponding bisets: ${}_AX_B$ ${}_BY_C$ ${}_AZ_C$. We have two categories to consider here:

$$\begin{tikzcd}
\textbf{A-Set-B} \arrow[d, shift right, "(\cdot)\times_B Y"'] \\
\textbf{A-Set-C} \arrow[u, shift right, "\mathrm{Hom}_{\mathbf{Mod}\text{-}C}(Y;\cdot)"']
\end{tikzcd}$$

The two functors in this diagram are the tensor product functor, and the Hom functor.

Definition 1.8 (Adjunction)**.** Let $\mathbf{A}, \mathbf{B}$ be categories. An *adjunction* from $\mathbf{A}$ to $\mathbf{B}$ is a triple $\langle F, G, \varphi \rangle : \mathbf{A} \to \mathbf{B}$ where F, G are functors such that:

$$\begin{tikzcd}
\mathbf{A} \arrow[r, shift left, "F"] & \mathbf{B} \arrow[l, shift left, "G"]
\end{tikzcd}$$

and φ is a function bringing pairs (a, b) for $a \in \mathrm{Obj}\,(\mathbf{A})$ and $b \in \mathrm{Obj}\,(\mathbf{B})$ to a bijection

$$\varphi_{a,b} : \mathrm{Mor}\,(Fa, b) \cong (a, Gb)$$

which is natural in x, a. The functors F, G are also said to be *adjoint*.

Proposition 1.1. *The tensor product functor is left adjoint to the* Hom *functor.*

Definition 1.9. A map between left A-sets $X \to X'$ is said to be *A-equivariant* or simply *equivariant* iff $f\,(ax) = af\,(x)$ for all $a \in A$ and for all $x \in X$.

Note that the equivariant maps between two A-sets X, Y are given exactly by $\mathrm{Hom}_{A\text{-}\mathbf{Set}}\,(X, Y)$.

Now we have the following diagram:

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbf{A-SetB}}\,({}_AX_B, \mathrm{Hom}_{\mathbf{Set-C}}\,({}_BY_C, {}_AZ_C)) \arrow[d, leftrightarrow, "\alpha_{X,Y}"] \\
\mathrm{Hom}_{\mathbf{A-Set-C}}\,(X \times_B Y, Z)
\end{tikzcd}$$

for every X and every Z, there is a bijection such that for any other pair X', Z' and the corresponding new Hom set, we get a commutative squares.

$$\begin{tikzcd}
X, Y \arrow[r, "\gamma"] \arrow[dr] & Z \arrow[d, dash] \\
& X \times_B Y
\end{tikzcd}$$

Example 1.5. Note the following equivalences:

$$\emptyset - \mathbf{Set} - \mathbf{B} = \mathbf{Set} - \mathbf{B} \tag{1.2}$$

$$A - \mathbf{Set} - \emptyset = \mathbf{A} - \mathbf{Set} \tag{1.3}$$

$$\emptyset - \mathbf{Set} - \emptyset = \mathbf{Set} \tag{1.4}$$

1.2 Groups and G-sets

Definition 1.10 (Group)**.** A set G with a binary relation (if $a, b \in G$, written $a \times b, a + b, a \cdot b, a \circ b$ or just ab) is a group iff this relation is associative, each element has an inverse, and there is an identity. In other words, for all $a, b, c \in G$,

1. There exists $e \in G$ such that $ea = ae = a$
2. There exists $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$
3. $a\,(bc) = (ab)\,c$

Definition 1.11 (Subgroup)**.** Let G be a group. A subset $H \subseteq G$ is a *subgroup* of G iff it contains the identity of G, is closed under the law of composition, and contains all inverses. This is often written $H < G$. We will sometimes write the set of all subgroups of a group G as $\operatorname{Sgr} G$.

Definition 1.12. Let G be a group and S a set. Then a map $\cdot : G \times S \to S$ is a *left action* of G on S iff for all $s \in S$ and all $g, h \in G$ we have:

1. $g \cdot (h \cdot s) = (gh) \cdot s$
2. $e \cdot s = s$

where e is the identity for G. A *right action* is a map $\cdot : S \times G \to S$ which satisfies the analogous properties.

Definition 1.13. Let G be a group. A set S is a *left G-set* iff we have an action of G on S

$$\varphi : G \times S \to S$$

such that for all $g, h \in G$ and for all $s \in S$ we have

$$\varphi\,(g, \varphi\,(h, s)) = \varphi\,(gh, s)$$

This action is also sometimes written $\varphi\,(g, s) = gs$ or $\varphi\,(g, s) = g \cdot s$. In this case the condition is just $(gh)\,s = g\,(hs)$. We define a *right G-set* similarly.

Proposition 1.2. *Let G be a group and S be a G-set. Then for all $g \in G$ with inverse g^{-1} we have*

$$g \cdot \left(g^{-1} \cdot x\right) = x = g^{-1} \cdot (g \cdot x)$$

Definition 1.14. We have four actions of a group G on itself. For $g \in G$ and $x \in X = G$,

1. Trivial: $g \cdot x \coloneqq x$
2. Left regular: $g \cdot x \coloneqq gx$ (makes G a left G-set) We write this map $\lambda : G \to \operatorname{Aut} G$.
3. Right regular: $x \cdot g \coloneqq xg$ (makes G a right G-set) We write this map $\rho : G \to \operatorname{Aut} G$.

4. Adjoint action: $g \cdot x \coloneqq gxg^{-1} = {}^{g}x$ We write this map $\operatorname{ad} : G \to \operatorname{Aut} G$.

Note that we call $gxg^{-1} = {}^{x}g = x^{g^{-1}}$ is called the conjugate of x by g. Note[1.1] also that we write: $g^{-1}xg = x^{g} = {}^{g^{-1}}x$ Note that we can "turn a left action into a right action" with the definition $g \cdot x \coloneqq xg^{-1}$ and vice versa.

Remark 1.3. Consider G as a $G \times G$ set by the action

$$(g_1, g_2)\, x \coloneqq g_1 x g_2^{-1}$$

So notice this is like combining left and right regular action. But then there is the diagonal homomorphism:

$$G \xrightarrow{\Delta} G \times G$$

so if we take $\Delta^{*}G$, we get precisely the adjoint representation of G on G. So this is how three standard actions on G (left, right, conjugation) are related to each other. The adjoint is the pullback of the combined left and right action of G on itself.

Example 1.6. We now note that $G_S \subseteq \mathcal{P}(S)$ (or G/S) is the largest trivial G quotient set. In addition, $X^G \subseteq X$ is the largest trivial G subset.

Definition 1.15. Let G be a group, and S be a G-set. Then the *orbit* of an element $s \in S$ is

$$\mathcal{O}_s = \{g \cdot s \mid g \in G\}$$

This is sometimes also written Gs. The *stabilizer* of $s \in S$ is

$$\operatorname{Stab}_G(s) = \{g \in G \mid g \cdot s = s\}$$

This is sometimes written G_s. We will write the collection of orbits of an action of G on S as G_S. This is also sometimes written G/S.

Warning 1.1. In other fields, such as symplectic geometry, the stabilizer is called the isotropy group of x.

Proposition 1.3. *If $y \in Gx$, then we have that $Gx = Gy$. In addition, $\emptyset \neq Gx \cap Gy$ iff $Gx = Gy$.*

Proof. Take an arbitrary element $a \in Gy$. Then there is some $g_a \in G$ such that $g_a \cdot y = a$. Then g_a has an inverse, g_a^{-1}, so we have $g_a^{-1}(g \cdot y) = y = g_a^{-1}a$. But since $y \in Gx$, there is some $h \in G$ such that $h \cdot x = y$, so $h \cdot x = y = g_a^{-1} \cdot a$, so we have $(g_a h) \cdot x = a$, and $a \in Gx$ as desired.

Take an arbitrary element $b \in Gx$. Then there is some $g_b \in G$ such that $g_b \cdot x = b$. Then, as before, $y = h \cdot x$, so $g_b^{-1} \cdot b = x = h^{-1} \cdot y$ so $b = \left(g_b h^{-1}\right) \cdot y$ and $b \in Gy$ as desired. ☐

[1.1] Some authors have the opposite convention for conjugation.

Proposition 1.4. *The action of a group G on a set S automatically gives an action on the power set $\mathcal{P}(S)$.*

Definition 1.16 (Coset)**.** Let G be a group and $H \subseteq G$ a subgroup. Then the *left cosets* of H are sets of the form $gH = \{gh \mid h \in H\}$ for any $g \in G$. The *right cosets* of H are sets of the form $Hg = \{hg \mid h \in H\}$ for any $g \in G$.

Definition 1.17 (Normal)**.** Let G be a group, and H a subgroup. Then H is *normal* iff for all $g \in G$, $gH = Hg$. This is often written $H \triangleleft G$.

Example 1.7. It follows somewhat directly from the definition of a normal subgroup, that the set of cosets of any normal subgroup forms a group itself, called the quotient group, and written G/H.

Definition 1.18. An element $g \in G$ is said to *normalize* a subgroup $H < G$ iff ${}^{g}H = gHg^{-1} = \mathrm{ad}_g(H) = H$.

Definition 1.19. Let $H < G$, then the *normalizer* of H in G:

$$N_G(H) = \left\{n \in G \mid nHn^{-1} = H\right\}$$

Example 1.8. If $H, K < G$, then $K < N_G(H)$ implies HK is closed under multiplication and taking inverses.

Definition 1.20. The centralizer of an element $x \in G$, is

$$C_G(x) = \{g \in G \mid gx = xg\} = \mathrm{Stab}_G(x)$$

where the action is understood to be conjugation of G on itself. We can also define this for $X \subset G$:

$$C_G(X) = \{g \in G \mid \forall x \in X, gx = xg\}$$

We write $C_G(G) = Z(G) = ZG$ and call this the *center* of G.

Example 1.9. Notice that the elements in $C_G(x)$ can equivalently be characterized as the elements $g \in G$, such that

$$1 = [g, x] = gxg^{-1}x^{-1} = gx(xg)^{-1}$$

Now note that $gxg^{-1}x^{-1} = {}^{g}xx^{-1}$ so since $[x, g]^{-1} = [g, x]$ then ${}^{g}xx^{-1} = 1$ iff ${}^{x}gg^{-1} = 1$.

Definition 1.21. Let S be a G-set. A subset $E \subseteq S$ is *G-invariant* iff $gE = E$.

Warning 1.2. This doesn't mean they are untouched by G, it just means the action of G never takes an element of E outside of E.

Example 1.10. Orbits are all clearly invariant, but they are in fact even more than invariant.

Definition 1.22. Let S be a G-set. Then G acts *transitively* on S iff for any two elements $s, t \in S$, there is some $g \in G$ such that $g \cdot s = t$.

Proposition 1.5. *If G acts transitively on a G-set S, then there is only one orbit.*

When G acts transitively on a G-set X, X is sometimes called a transitive G-set. This is also called a homogeneous G-set.

Definition 1.23. A point $s \in S$ is *fixed* by the action of G iff $g \cdot x = x$ for all $g \in G$. The set of all fixed points of the action of G is written X^G. It is sometimes also written $\operatorname{Fix}_G X$.

Example 1.11. Every homomorphism of groups has a kernel and image. In particular,

$$\begin{tikzcd} C\left(G\right) \arrow[r] & G \arrow[r, "\mathrm{ad}"] & \mathrm{ad}\left(G\right) \arrow[r, hook] & \operatorname{Aut} G \end{tikzcd}$$

where $\mathrm{ad}\left(G\right)$ denotes the image of G under self adjoint. We also write $\mathrm{ad}\left(G\right) = \mathrm{Inn}\left(G\right)$ which is called the collection of inner automorphisms. Note $\left(\mathrm{ad}_g\right)^{-1} = \mathrm{ad}_{g^{-1}}$.

Let $H < G$. Since $hH = H$ iff $h \in H$, we obtain the induced action of $N_G\left(H\right)/H$ on G/H. Notice this is a right action which commutes with a left regular action by G. Then $g\left(xH\right) \coloneqq \left(gxH\right)$ but $\left(xH\right)n \eqqcolon \left(xn\right)H$. and they obviously commute, so now G/H is a subgroup of a $\left(G, N_G\left(H\right)/H\right)$ biset.

Definition 1.24. The action of a group G on a G-set X is *free* iff the stabilizer of every point is trivial. Equivalently, the existence of an $x \in X$ with $gx = hx$ implies $g = h$.

Definition 1.25. A composable pair of group homomorphisms

$$\begin{tikzcd} G'' & G \arrow[l, two heads, "p"'] & G' \arrow[l, tail, "i"'] \end{tikzcd}$$

is said to be an *extension* iff

1. i is injective ($\ker i = \{e'\}$)
2. $\operatorname{im} i = \ker p$
3. p is surjective ($\operatorname{im} p = G''$)

We say that a group G is an extension of a group G'' by a group G' if there exists an extension with G in the middle, G'' is isomorphic to the quotient group via p, and G' is isomorphic to a subgroup G via i.

Definition 1.26. A *trivial extension* is of the form

$$\begin{tikzcd} G'' & G'' \times G' \arrow[l, "p''"'] & G' \arrow[l, "i'"'] \\ & (e'', g') & g' \arrow[l, mapsto] \\ g' & (g'', g') \arrow[l, mapsto] & \end{tikzcd}$$

More generally, a trivial extension is the one which is isomorphic to a standard trivial extension.

Remark 1.4. Group extensions have applications to anomolies in quantum field theory.

Definition 1.27. Write ${}^{G}H$ to be the conjugacy class of subgroups containing H. Note that $\mathrm{Stab}_G\, H = N_G\left(H\right)$.

Proposition 1.6. *In* G-**set**, ${}^{G}H = G/N_G\left(H\right)$.

We will denote the category of extensions of groups by **ExtGr** where objects are extensions. Consider two extensions $\mathcal{F}, \mathcal{E}$:

$$\begin{tikzcd}
H' \arrow[d, "\kappa"] & G' \arrow[l, "\sim"'] \arrow[d, "\iota"] \\
H \arrow[d, "\rho"] & G \arrow[l, "\sim"'] \arrow[d, "\pi"] \\
H'' & G'' \arrow[l, "\sim"']
\end{tikzcd}$$

a morphism $\mathrm{Mor}_{\mathbf{ExtGr}}\left(\mathcal{F}, \mathcal{E}\right)$ consists of the three horizontal isomorphisms in the diagram, such that everything commutes.

Example 1.12. Consider $G = HK$ such that K normalizes H, and additionally, assume that $H \cap K = \{e\}$. Note this is equivalent to saying $G = HK$ is a unique factorization. If I take a homomorphism: ι is inclusion, π canonical quotient. Then this is a classic example of an extension of groups:

$$\begin{tikzcd}
G/H & G \arrow[l, two heads, "\pi"'] & H \arrow[l, hook', "\iota"']
\end{tikzcd}$$

A general extension is isomorphic to this one.

Proposition 1.7. *If we have an extension:*

$$\begin{tikzcd}
G'' & G \arrow[l, two heads, "p"'] & G' \arrow[l, tail, "i"']
\end{tikzcd}$$

then $\left|G\right| = \left|G'\right| \left|G''\right|$.

Proof. This is Lagrange's theorem. ☐

Example 1.13. Meta-cyclic groups are groups G such that

$$C'' \leftarrow G \leftarrow C'$$

One can continue this way, to get to an equivalent construciton of solvable groups.

1.3 Exercises

Exercise 1.3.1. Let $n \in G$ normalize $H < G$. Show that for any $x, x' \in G$, it is the case that $xH = x'H$ implies $xnH = x'nH$.

Exercise 1.3.2. Show that the action of $N_G(H)/H$ is free. Equivalently show that $xnH = xH$ iff $n \in H$.

Exercise 1.3.3. Construct mutually inverse $N_G(H)/H$ equivariant maps between $X \times_G G/H$ and X_H for every right G-set X.

Exercise 1.3.4. For every left G-set X, construct mutually inverse $N_G(H)/H$ equivariant maps between $\mathrm{Hom}_{\mathbf{G-Set}}(G/H, X)$ and X^H.

1.4 Inverse and direct image functors

We now present some notable special cases of the exercises in the previous section. First we offer some definitions and fix some notation.

Definition 1.28. Let $\varphi : G \to G'$ be a group homomorphism and, for a right/left G'-set X', let $\varphi^* X'$ denote the underlying set equipped with the action of G:

$$x'g \coloneqq x'\varphi(g) \qquad\qquad gx' \coloneqq \varphi(g)\,x'$$

for the right and left cases respectively. The functor φ_* is defined to be a left adjoint functor to φ^*. $\varphi_!$ is defined to be a right adjoint to φ^*. In particular, φ^* is called the inverse image, and φ_* is called the direct image. There is no agreed upon name for $\varphi_!$ at this abstract level.[1.2]

In particular, we have the functor which takes

$$\begin{tikzcd}
\mathbf{Set}\text{-}G \arrow[d, shift right=4, "\varphi_*"'] \arrow[d, shift left=4, "\varphi_!"] \\
\mathbf{Set}\text{-}G' \arrow[u, "\varphi^*"']
\end{tikzcd}$$

So exercises 3,4 show that these are adjoint.

Now we can consider G' as a (G', G')-biset, (G, G')-biset, (G', G)-biset, and (G, G)-biset. (G', G') and (G, G) are uninteresting. We use the (G, G') structure. For a trivial subgroup $H < G$,

$$X' \times_{G'} {}_{G'}G'_G \simeq \varphi^* X' \simeq \mathrm{Hom}_{\mathbf{Set}\text{-}G'}\left({}_G G'_{G'}, X\right)$$

since G acts on the right. But what is remarkable, is that it now appears in two different clothes so to speak. Both dressed as the tensor product, and the Hom functor. So now explicitly we write:

$$\varphi_* X = \left(X \times_G G'\right)_{G'} \qquad\qquad \varphi_! X \coloneqq \mathrm{Hom}_{\mathbf{Set}\text{-}G}\left({}_{G'}G'_G, X\right)$$

[1.2] We will meet many names for these functors in special cases.

Now we see some special cases of these functors from group theory and actions of groups. Let $H < G$ and $\varphi : H \hookrightarrow G$. Then $\iota^* = \mathrm{Res}_H^G$ is the restriction functor and $\iota = \mathrm{Ind}_H^G$ is the induction functor. Also, $\iota_! = \mathrm{Coind}_H^G$ is called the coinduction functor.

Now a special case (of this special case) is when $H = 1$. Then H-sets are just sets. So in this case, Res_1^G is Forget, which has left and right adjoint. The induction from 1 is called the free G-set functor. There is also co-induction, then Coind_1^G is the cofree G-set.

Now let $H \lhd G \overset{\pi}{\twoheadrightarrow} G/H$ Then $\pi^* = \mathrm{Inf}_{G/H}^G$ is called inflation $\pi_* = \mathrm{Def}_{G/H}^G$ is called deflation, and $\pi_!$ is the H-fixed points functor. So when $G = N_G(H)$ then this goes to $N_G(H)/H$.

When $G = H$, then $\pi : G \to 1$. The map π^* is inclusion of **Set**-G in **Set**-G and here, $\pi_* X = X_G$ and $\pi_! X = X^G$.

1.5 Exercises

Let $H, K < G$

Exercise 1.5.1. Given two $x, y \in G$, then $HxK \cap HyK \neq 0$ iff $HxK = HyK$

Exercise 1.5.2. Given an element x of some G-set X, show that the G-equivariant map from G to X which sends $e \mapsto x$ induces an isomorphism of G-sets from $G/H \xrightarrow{\sim} \mathcal{O}_x$ where $\mathcal{O}_x$ is the orbit, and $H = \mathrm{Stab}_G\, x$. Essentially, show

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "h"'] & & X \\
& G/H \arrow[ur, dashed, "\varphi"'] &
\end{tikzcd}$$

Exercise 1.5.3. Show that $\mathrm{Stab}_H(xK)$[1.3] is exactly equal to $H \cap {}^xK$

Exercise 1.5.4. Show that $HK = KH$ iff HK is a subgroup of G.

We now take: $H, K, L < G$ and $H < K$.

$$\begin{tikzcd}
H \arrow[r, hook] & K \arrow[r, hook] & G \\
& & L \arrow[u, hook]
\end{tikzcd}$$

Exercise 1.5.5. Show that $HL \cap K = H(L \cap K)$.

Exercise 1.5.6. Show that $HL = KL$ and $H \cap L = K \cap L$ iff $H = K$.

[1.3] This is really Stab of a point in $\mathrm{Res}_H^G(G/K)$.

Chapter 2

Properties G-sets

2.1 Properties of G-sets

We now present some corollaries of the preceding exercises:

Corollary 2.1. *We have the following equality:*

$$(G/K)^H = \{cK \mid H \subseteq {}^{x}K\}$$

Corollary 2.2. *The set H is a subgroup of a conjugate of K iff $(G/K)^H \neq \emptyset$.*

Corollary 2.3. *Let $|H| = |K| < \infty$. Then H and K are conjugate, iff $(G/K)^H \neq \emptyset$.*

Corollary 2.4. *We have:*

$$(G/H)^H = \{xH \mid x \in N_G(H)\} \qquad\qquad \frac{N_G(H)}{H} \subseteq (G/H)^H$$

In particular, $\left|(G/H)^H\right| = |N_G(H) : H|$.

Definition 2.1. A flag is a linearly ordered subset of a partially ordered set $s_0 \leq s_1 \leq \cdots \leq s_k$.

Definition 2.2. A subgroup $H < G$ is *k-subnormal* iff there is a finite flag of subgroups $\{H_i\}_{i=1}^{k}$ such that

$$H \triangleleft H_1 \triangleleft \cdots \triangleleft H_k = G$$

Proposition 2.1. *A subgroup $H < G$ is subnormal iff*

$$H \triangleleft N_G(H) \triangleleft N_G(N_G(H)) \triangleleft \cdots$$

eventually reaches G.

Note that if $H \lhd N_G(H) < G$ then the index of H in $N_G(H)$ is equal to $\left|(G/H)^H\right|$ and the index of G in $N_G(H)$ is the number of conjugates of H in G. This is because $\operatorname{Stab}_G(H) = N_G(H)$ if we consider the G-set X consisting of subgroups of G acted on by G via conjugation.

We now consider $\operatorname{Hom}_{G\textbf{-set}}(X, Y)$. In particular, we look at the orbital decomposition. Any G-set X can be written

$$X = \coprod_{\mathcal{O} \in X_G} \mathcal{O}$$

Now every orbit $\mathcal{O} = \mathcal{O}_x$ for any $x \in \mathcal{O}$. As such, we have the canonical isomorphism $\mathcal{O}_x \simeq G/\operatorname{Stab}_G x$. In addition, up to non-canonical isomorphism:

$$X \simeq \bigcup_{x \in I} G/\operatorname{Stab}_G x$$

where I is the set of representatives of the orbits.

Definition 2.3. A complete set $S \subseteq X$ of representatives of orbits of a G-set X is said to be a *transversal.*

$$\begin{tikzcd}
S \arrow[r, hook] \arrow[dr, "\sim"] & X \arrow[d, two heads] \\
 & X_G
\end{tikzcd}$$

We will often write this set of representatives as $[\![x]\!]$.

Example 2.1. For $X = H$, we have that a transversal contains one element from each coset of H.

Remark 2.1. Choosing a transversal is referred to as Gauge fixing in the physics literature.

A subset $S \subseteq X$ is a transversal precisely when $\varphi : S \to X$ is a bijection in the following diagram:

$$\begin{tikzcd}
S \arrow[r, hook] \arrow[dr, "\varphi"'] & X \arrow[d, two heads, "\pi"] \\
 & X
\end{tikzcd}$$

As it turns out, this give us a functor from G-**set** $\to \operatorname{Transversals}(X) \subseteq \mathcal{P}(X)$

Then a general isomorphism in

$$\operatorname{Hom}_{G\textbf{-set}}(X, Y)$$

is given by a matrix whose entries correspond to morphisms from $G/H \to G/K$.

Proposition 2.2. *We have a canonical isomorphism between*

$$\mathcal{O}_x \simeq G/H$$

where $H = \operatorname{Stab}_G x$.

Proposition 2.3. *If $x' \in \mathcal{O}_x$ and $x' = gx$ for some $g \in G$, then*

$$\operatorname{Stab}_G gx = {}^g \operatorname{Stab}_G x$$

We now present a corollary which is a consequence of propositions 2.2 and 2.3.

Corollary 2.5. *Let $H, K < G$, then $G/H \simeq G/K$ iff H and K are conjugate subgroups.*

Definition 2.4. We write $H <^G K$ if there exists $x \in G$ such that $H < {}^x K$. Also, $H =^G K$ if there exists $x \in G$ such that $H = {}^x K$.

Take $\operatorname{Sgr} G$ to be the set of all subgroups of $G \subseteq \mathcal{P}(G)$. We consider this to be a G-set with G acting by conjugation. So on this G-set, $<^G$ and $=^G$ are relations. It is clear they are reflexive and transitive, but it is not necessarily weakly antisymmetric, so it is not ordered and is instead only preordered[2.1] This is because a priori there is no reason we cannot have the following in the general case:

$$H <^G K <^G H \qquad\qquad H \neq^G K$$

If G is finite, this counterexample can clearly not be the case, so the finite groups this is an order.

Exercise 2.1.1. Is there is a simple argument which means $H <^G K <^G H$ implies $H =^G K$ for infinite groups? Infinitely generated groups?

It is however the case that $=^G$ gives an equivalence relation, and in fact:

$$\operatorname{Sgr} G / \left(=^G\right) = \left(\operatorname{Sgr} G\right)_G$$

which is the set of conjugacy classes of subgroups of G. Now the set of conjugacy classes of subgroups, is equipped with partial order.

Lemma 2.1. *In general, a pre-ordered set $(H, \prec)$ induces a partial order on itself: if we define $\sim$ iff $x \prec y$ and $y \prec x$ then $H/\sim$ becomes a partially ordered set.*

Let us return to the above observations. For group G and G-set X, consider X^H. Then suppose $H =^G K$. In general X^H, X^K are two different subsets of X. But if $K = {}^g H$, then the action by g identifies X^H with X^K.

Now look at the category G-**set** and define $|\mathrm{Fix}_H|$ as follows:

$$X \xmapsto{|\mathrm{Fix}_H|} \left|X^H\right|$$

For finite G-sets, this is clearly always valued in $\mathbb{N}$. Now we have the following:

Proposition 2.4. $|\mathrm{Fix}_H| = |\mathrm{Fix}_K|$ *iff $H =^G K$.*

[2.1] This is also called quasi-ordered.

Proof. If $H =^G K$, then clearly $|\text{Fix}_H| = |\text{Fix}_K|$. In the other direction, let $|\text{Fix}_H| = |\text{Fix}_K|$, then proceed by contradiction. Assume $H \neq^G K$. Now we just need to build one G-set such that $|\text{Fix}_H| \neq |\text{Fix}_K|$. ☐

Proposition 2.5. *Let X, Y be G-sets for some group G. Take $X \cup Y$ under the assumption that $X \cap Y = \emptyset$. Then*

$$(X \cup Y)^H = X^H \cup Y^H$$

for any $H < G$.

We now introduce a "multiplication" bifunctor on G-**set**. This is another sort of categorical tensor product, which is different from the tensor product we saw earlier. Consider the catesian product of the underlying sets[2.2], $X \times Y$, and notice G acts as follows:

1. If X is a G-set, X' is a G'-set, then $X \times X'$ is naturally a $G \times G'$ set where

$$(g, g')(x, x') = (gx, g'x')$$

2. G diagonally imbedded into $G \times G$, written: $G \xrightarrow{\Delta} G \times G$ is a canonical group homomorphism. Thus, given two G-sets X and Y, we define

$$\Delta^* (X \times Y)$$

where we consider the induced functor

$$G\text{-}\mathbf{set} \longleftarrow G \times G\text{-}\mathbf{Set}$$

$$X \otimes Y \longleftarrow X \boxtimes Y$$

This map is a canonical comultiplication. In fact, what we have here is what is a co-commutative, co-associative. co-binary structure. And then, a free vector space on a given set becomes, automatically, a co-algebra structure on the vector space. So if we take a group, and consider a k-vector space with basis G, we have a canonical co-associative co-unital co-commutative co-algebra structure. But G is a group, so this group multiplication will also induce multiplication here. Then automatically, this group multiplication is actually, by homomorphisms of co-algebras. In other words, it is a bi-algebra. But there is an identity element here, making sure it is actually a unital algebra. Now writing all of this down together gives us a Hopf algebra. So a group algebra is really just a Hopf algebra. We will talk more about this later.

In any case, $X \otimes Y$, $g(x, y) = (gx, gy)$.

Proposition 2.6. *Let X, Y be G-sets for some group G. Take $X \otimes Y$ as identified above. Then*

$$(X \otimes Y)^H = X^H \times Y^H$$

So now look at the class of finite G-sets, and we see that this is a sort of semi-ring category, because now we have

$$C \otimes (A \amalg B) = C \otimes A \amalg C \otimes B$$

[2.2] This is in fact a tensor product in **Set**.

2.2 Burnside ring

Definition 2.5 (Semi-ring)**.** Ring except without the assumption that it is an abelian group under addition, and rather a commutative semi-group. We still assume distributivity.[2.3]

So now we effectively have three operations. We have two operations involving pairs of G-sets, and we also have an operation which associates fixed points, so to speak. So we now wish to consider only fixed points of a given H. Notice if $X \cong Y$, then $X^H \cong Y^H$ canonically. Now if $H =^G K$, then the corresponding sets are still isomorphic. So what we actually find, is that all of these operations, are operations on the actual set. We have this because every finite G-set has the composition:

$$X = \bigcup_{\mathcal{O} \in X_G} \mathcal{O} \simeq \coprod_{x \in [\![x]\!]} G / \operatorname{Stab}_G x$$

where we have fixed the transversal $[\![x]\!]$. So the picture here, is that we drop $X \to X_G$, so the orbits live in X running in one direction, then the transversal runs perpendicularly through these orbits, determining one representative for each one.

So we get now, that the class of isomorphism classes of finite G-sets for any group G is a set. And in fact, this set canonically inherits the structure of addition and multiplication. Explicitly, given two G-sets X, Y, we take:

$$[X] + [Y] \coloneqq [X \amalg Y] \qquad\qquad [X]\,[Y] \coloneqq [X \otimes Y]$$

Recall that $X \otimes Y = \Delta^* (X \times Y) = \Delta^* (X \boxtimes Y)$. Now, because all of this associativity and such were given up to isomorphism classes, we get these properties properly. So we have a semi-ring. We now need to force additive inverses to get a ring. So take the following formal differences:

$$[X] - [Y] \sim [X'] - [Y'] \iff [X] + [Y'] = [X'] + [Y]$$

Of course we don't even need this, because this is really just saying:

$$X \amalg Y' \simeq X' \amalg Y$$

Such isomorphism classes comprise what is called the burnside ring $B(G)$. We take 0 to be $[\emptyset]$, and take 1 to be $[G/G]$.

In particular, this is given by:

$$\mathbb{Z}\left[x_H\right]_{H \in \operatorname{Sgr} G_G / \text{some relations}}$$

so when G is finite, this is just a quotient of a finitely generated polynomial ring.

[2.3] Some people assume $1, 0$ are both still present. This causes issue, because without the full structure, this requires the explicit assumption that $0 \times 0 = 0$ and other such things.

Recall again that

$$\bigcup_{H\in[\![\mathrm{Sgr}]\!]} G/H$$

where $H \in [\![\mathrm{Sgr}]\!]$ is generic notation for any complete set of representatives of conjugacy classes of subgroups under G. Note we have the natural isomorphism $\mathcal{O}_x \simeq G/\operatorname{Stab}_G x$. Each such isomorphism $\mathcal{O} \simeq G/H$ is called a trivialization.

So we have seen that the set of isomorphism classes of finite G-sets forms a semi-ring. We desire to build this a different way. Now if we look at the category of unital rings, $\mathbf{Ring}_1$, then this is of course a sub-category of unital semi-rings with 0, $\mathbf{Semiring}_{0,1}$. In fact this inclusion has a left adjoint functor. This means that for every semi-ring S, we get a ring $K(S)$ called the K-functor construction.

Example 2.2. If you apply this to the semi-ring of isomorphism classes of vector bundles on a topological space then you get the K-functor of the underlying topological space.

This semi-ring then has the following property. If we have any homomorphism of a semi-ring S with $0, 1$ into any proper ring R, then there is a canonical map $S \to K(s)$ such that there is a unique map $K(S) \to R$. And this is in fact a homomorphism in $\mathbf{Ring}_1$. Note that commutativity of multiplication is not required here.

$$\begin{tikzcd}
& K(S) \arrow[dl, dashed, "\exists!"'] & \\
R & & A \arrow[ll] \arrow[ul]
\end{tikzcd}$$

In other words, we are seeing that elements of $K(S)$ are formal differences $s - t$ where $s, t \in S$. Now equivalence relation on this is: $(s, t) \sim (s', t')$ iff $s + t' = s' + t$. For Abelian monoids this is very simple, however for non-abelian ones this would much trickier. In any case, under this relation,

$$[(s, t)] + [(s', t')] = [(s + s', t + t')]$$

So now if this is indeed equivalence, let us go back to our situation where S would be precisely the semiring of isomorphism classes and so on, so the letters s, t are just isomorphism classes.

So we have seen this process happen in two steps. First produce the appropriate set of isomorphism classes in the appropriate category. Then if we have a sort of addition and multiplication, then we just inherit the semi-ring structure. Next we just have to apply the missing additive inverses. This is easy when addition is Abelian. In any case, the elements of such $K(S)$ can be considered as isomorphism classes, when s, t are not actually in S, but in the original structure.

So the Burnside ring of a group G is simply the ring whose elements can be thought of as formal differences of finite G-sets $X - Y$ subject to the equivalence relations we have seen. This is wonderful, because it's directly built so

$$X - Y \sim X' - Y'$$

iff there exists a G-set Z such that $X \amalg Y' \amalg Z \simeq X' \amalg Y \amalg Z$ in G-**set**. It is in fact quite clear where Z comes from here. Two elements of a group are the same if when we add a third element they are still equal. But now if we want to pass directly from G-**set** to the Burnside ring, this will not be some sort of relation (as it would be without Z) but we need Z here to have actual isomorphism. This corresponds to the fact that the formal difference $Z - Z$ represents 0 for every Z. So this is the whole point.

Exercise 2.2.1. Verify that the set of equivalence classes by this equivalence (formal differences divided by $\sim$) is in fact a ring, and has the universal property that if we take the semi-ring of isomorphism classes of finite G-sets, then any hom from this semiring to any ring R, would induce (or extend if injective) a map from $B(G)$ to R.

$$\begin{tikzcd}
& B(G) \arrow[dl, dashed, "\tilde{\varphi}"'] & \\
R & & \{[X] \mid X \in \mathrm{Obj}\left(G\text{-}\mathbf{set}_{\mathrm{finite}}\right)\} \arrow[ll] \arrow[ul]
\end{tikzcd}$$

where the collection of finite equivalence classes $[X]$ is understood to have the semi-ring structure as discussed above.

To recap, we have now seen two ways to obtain the Burnside ring. First, we can associate finite G-sets with the corresponding set of isomorphism classes, which inherits a semi-ring structure from the disjoint union and tensor product.

Secondly, there is a general construction involving reflection of subcategory of unital rings, in the category of unital semi-rings with zero. And if you apply this to our particular situation (and others) the whole process can be done in one step. The elements are now equivalence classes of formal difference of objects of the original category where equivalence is simply given by isomorphisms in the original category.

Definition 2.6. In general, $X \simeq Y$ stably iff there exists some Z such that

$$X \amalg Z \simeq Y \amalg Z$$

This is why elements of these K-functor groups are called stable isomorphism classes.

We now come to Burnside's theorem:

Theorem 2.1 (Burnside)**.** *Suppose G is a finite group. Consider the map which brings the isomorphism class of a finite G-set X, [X], to the family of numbers which are cardinalities of the sets of fixed points for H ∈* $\llbracket \mathrm{Sgr} \rrbracket$*.*

$$[X] \mapsto \left(\left|H^H\right|\right)_{H \in \llbracket \mathrm{Sgr} \rrbracket}$$

Note this is an isomorphism of unital semi-rings with zeros. But this second thing is the ring, $\mathbb{Z}^{\llbracket \mathrm{Sgr} \rrbracket}$*, since for each* H *the target is* $\mathbb{Z}$*. So this canonically factorizes through the burnside ring:*

$$\begin{tikzcd}
{[X]} \arrow[rr, mapsto] \arrow[dr] & & \left(\left|H^H\right|\right)_{H\in\llbracket \mathrm{Sgr} \rrbracket} \\
& B\left(G\right) \arrow[ur, dashed] &
\end{tikzcd}$$

In particular, this is injective.

This looks quite a bit different from the usual form of Burnside's theorem:

Theorem 2.2 (Burnside)**.** *Let* G *be a finite group, and let* X, Y *be two finite* G*-sets such that* $X \simeq Y$ *in* G-**set** *iff* $\left|X^H\right| = \left|Y^H\right|$ *for all subgroups* $H < G$*.*

We first recall three observations which we have already seen. Then we introduce some concepts about working with unordered infinite dimensional matrices, and prove the theorem.

1. Recall that if $H' = {}^gH$, then $X^{H'} = g\left(X^H\right)$. In particular, since multiplication by g is bijective, these cardinalities are always equal. So it is sufficient to show the previous result for only $H \in \llbracket \mathrm{Sgr} \rrbracket$.
2. Recall that the relation on Sgr, $H <^G K$, induces a partial order.
3. Recall that we have $H <^G K$ iff $\left(G/H\right)^K \neq \emptyset$. This is extremely important because each of these X can be written:

   $$X = \bigcup_{\mathcal{O} \in X_G} \mathcal{O}$$

   which means

   $$X^H = \bigcup_{\mathcal{O} \in X_G} \mathcal{O}^H$$

   so

   $$\left|X^H\right| = \sum_{\mathcal{O} \in X_G} \left|\mathcal{O}^H\right|$$

Example 2.3. Rings of matrices in general can be defined perfectly well without any ordering of the indices. Explicitly, for some $S \times T$ matrix A and some $T \times U$ matrix B, we have:

$$\left(AB\right)_{su} = \sum_{t \in T} a_{st} b_{tu}$$

where this sum can even be over an infinite set, as long as these products are nonzero for only finitely many of these infinite possible entries.

Explicitly, if we have any vector spaces V,W with a basis X and Y respectively, and we have some linear transformation $\Lambda : V \to W$, this can be expressed in two ways: First as left multiplication by some matrix $L_A \left(c_x\right)_{x\in X}$, where c_x is an $X \times 1$ matrix, and L_A has finitely many non-zero entries in every column. But if we represent this as right multiplication by matrix R_B, then it will be the same c_x, but now written as row vector. This is of course just a $1 \times X$ matrix, and now R_B has finitely many non-zero terms in every row. Note we only had to insist on this finiteness in the matrices, and not in the vectors. This is because from the definition of a basis of a vector space, we automatically have that the terms in c_x will only be nonzero for finitely many.

Now we can prove the theorem:

Proof. ($\Longrightarrow$): This is obvious.
($\Longleftarrow$): Note we are actually assigning

$$X \mapsto \left(\left|X^H\right|\right)_{H\in\llbracket\mathrm{Sgr}\rrbracket}$$

which factorizes in the following way:

$$\begin{tikzcd}
X \arrow[rr, mapsto] \arrow[dr, mapsto] & & \left(\left|X^H\right|\right)_{H\in\llbracket\mathrm{Sgr}\rrbracket} \\
& {[X]} \arrow[ur, mapsto] &
\end{tikzcd}$$

where

$$[X] = \sum_{K\in\llbracket\mathrm{Sgr}\rrbracket} c_K \left[G/K\right]$$

where c_K is telling us the number of orbits $\mathcal{O}$ of X such that the conjugacy class of stabilizers of points of $\mathcal{O}$ contains H:

$$c_K \coloneqq \left|\left\{\mathcal{O} \in X_G \mid \left[\operatorname{Stab}_G x\right] \supseteq K, x \in \mathcal{O}\right\}\right|$$

In fact we have:

$$\left\{K < G \,\middle|\, K = \operatorname{Stab}_G x, x \in \mathcal{O}\right\} = [K]$$

for any such H. Notice if I do this for Y,

$$[Y] = \sum_{K\in\llbracket\mathrm{Sgr}\rrbracket} d_K \left[G/K\right]$$

then these two conjugacy classes are equal iff X and Y are isomorphic. Now it is clear, that due to the fact the fixed point set preserves disjoint union (and product) we find that if we now count cardinalities, we would find that for all $H \in \llbracket\mathrm{Sgr}\rrbracket$ we get

$$\left|X^H\right| = \sum_{K\in\llbracket\mathrm{Sgr}\rrbracket} c_K \left|\left(G/K\right)^H\right|$$

so we are effectively working with a generalized version of a system of equations.

As we have seen, we can basically reduce this setup to be a system of equations. For this proof we write: $S = [\![\mathrm{Sgr}]\!]$ Now consider the S by S matrix:

$$M \coloneqq \left(\left|(G/K)^H\right|\right)$$

We call this M because it if often referred to as the matrix of marks. Here H, K are the indices of M. In any case, this equality is expressed as saying that we apply this matrix as follows:

$$\left(\left|(G/K)^H\right|\right)(c_K - d_K)_{K \in [\![\mathrm{Sgr}]\!]}$$

which gives us zero. Now if this matrix, which is finite since $[\![\mathrm{Sgr}]\!]$ is finite, is invertible over the rationals, then we have $\det(M) \neq 0$, and $c_K - d_K = 0$ for all $K \in [\![\mathrm{Sgr}]\!]$. And this of course means $X \simeq Y$ in G-**set**. So now we only need to show that this matrix is upper triangular.

Now recall from the previous remarks, that

$$\left|(G/K)^H\right| > 0$$

iff $H <^G K$. So this matrix is even strictly upper triangular, because whenever this holds, this is strictly positive. In other words the "lower triangle" region is where $H \not<^G K$, and these entries are certainly zero, which can be seen by counting cardinalities. But for all the other entries, and in particular the main diagonal, we have that the entries are strictly positive, and our determinant is therefore nonzero as desired. Note in fact this determinant is yet another invariant in the category of finite groups. ☐

The previous proof not only proves the theorem, but gives us even more. In particular, we get that

$$\det M = \prod_{H \in [\![\mathrm{Sgr}]\!]} \left|(G/H)^H\right|$$

But we also know that

$$(G/H)^H = N_G(H)/H = \{gH \mid g \in N_G(H)\}$$

so

$$\det M = \prod_{H \in [\![\mathrm{Sgr}]\!]} |N_G(H)/H|$$

Now notice, each of these terms in the product divide $|G|$. So this is a product of numbers, which are divisible exclusively by those primes which divide G. Of course in general there are prime factors of G which do not divide this product. But this still shows us that in order to invert the determinant, we don't need to invert all natural numbers, but rather only the primes which divide the order of G. We now have an immediate corollary which is effectively just rewriting Burnside's theorem as we saw it before:

Corollary 2.6. *The semiring of isomorphism classes of finite G-sets, is mapped by fixed point counting into*

$$\prod_{(\mathrm{Sgr}\, G)_G} \mathbb{Z}$$

where explicitly

$$[X] \mapsto \left(\left|X^H\right|\right)_{H \in [\![\mathrm{Sgr}]\!]}$$

In particular, the Burnside theorem tells us that this is injective.

So we have found at least one ring, which contains this as a subring. Now the universal ring, through which every such homomorphism factorizes, is, by definition, the Burnside ring. In particular, this is the ring where two G-sets are not just isomorphic, but stably isomorphic.

Corollary 2.7. *Two finite G-sets are isomorphic iff they are stably isomorphic.*

In other words, we have retrieved the orignal form of Burnside's theorem that we initially saw.

2.3 Exercises

These three exercises are calculating how three functors act in relation to a subgroup. Let $H < G$ for some finite group G. We have $G\text{-}\mathbf{set}_{\text{finite}}$ and $H\text{-}\mathbf{Set}_{\text{finite}}$ then we have

$$\mathrm{Res}_H^G : G\text{-}\mathbf{set}_{\text{finite}} \leftrightarrow H\text{-}\mathbf{Set}_{\text{finite}} : \mathrm{Ind}_H^G$$

Note that Res brings finite G-sets to finite H-sets regardless of the cardinality of G, but Ind only brings finite H-sets to finite G-sets, because G is finite itself. It might not be particularly elegant, but we know objects in either one of these categories are given by the disjoint union of their orbits. So we can take advantage of this structure. In particular, recall that if we have $\varphi : G \to G'$, then the functors φ_*, φ^* are additive.[2.4] In fact, φ^* is even multiplicative, but the others are not.

Exercise 2.3.1. Let $K < H$. Construct two mutually inverse G-equivariant maps between $G \times_H H/K$ and G/K where G is considered as a (G, H) biset.

Exercise 2.3.2. Consider G/K. This is of course a finite G-set. Now consider the restriction:

$$\mathrm{Res}_H^G (G/K) \simeq \bigcup_{a \in [\![H \backslash G/K]\!]} G/\left(H \cap {}^aK\right)$$

where the union is over the elements of the transversal of double cosets.

Exercise 2.3.3. Calculate the product of homogeneous G-sets.

[2.4] Here this means the disjoint union is preserved.

2.4 Consequences of the exercises

As a result of the third exercise in the previous section, we get the following proposition:

Proposition 2.7. *Let $H, K < G$. Then we have the non-canonical*[2.5] *isomorphism:*

$$G/H \otimes G/K \simeq \bigcup_{x \in [\![H \backslash G/K]\!]} G/H \cap {}^{x}K$$

This is referred to as the "multiplication formula."

Example 2.4. Take some group with prime order. Now such a group is Abelian and simple, so the only non-trivial subgroups are the trivial group, and the group itself. Then we can write down the corresponding Burnside ring. In particular, this will be a quotient of the polynomial ring in two variables. One variable corresponds to each subgroup. So what happens in the multiplication formula for $K = G$. Then we get that

$$G/H \otimes G/G \simeq G/H$$

so indeed, this product formula is consistent with the notion that G/G is the multiplicative identity with respect to this product.

Recall from exercise 2, that if we take

$$\mathrm{Res}_H^G (G/K) \simeq \bigcup_{x \in [\![H \backslash G/K]\!]} H/H \cap {}^{x}K$$

Also recall the formula from exercise one for the induction. Finally recall that if we take the induced representation $\mathrm{Ind}_H^G (H/L)$, this is canonically isomorphic to G/L. Now combining these, we essentially get the Frobenius formula:

$$\left(\mathrm{Ind}_H^G \circ \mathrm{Res}_H^G (G/K)\right) \simeq G/H \otimes G/K$$

where a priori, this is a non-canonical isomorphism. This does in fact turn out to be canonical, but this is non-obvious. Now notice, that it follows from distributivity, that Res is a multiplicative homomorphism as well. So from a purely theoretical point of view, it is immediately clear that Res brings sums to sums, and products to product. But if we want to verify this explicitly using product formulas, we would get some highly non-obvious identity.

Remark 2.2. One of the things mathematics is famous for is identities. In fact, Yuri Manin once said, that the most profound way to prove identities, is to simply take something which is not on either side. This requires insight, and doesn't actually depend on the cleverness that is tested in solving puzzles or the like. Professor Wodzicki offered the following analogy. You can be the strongest

---

[2.5] On the left hand side, we do have have the data which is used to write the right hand side.

man in the world, and you could be capable of fighting off many tigers, but if you're in a dangerous jungle, you can still only make it maybe a few miles. But people like Grothendieck built highways and planes, and traveled hundreds of miles. This is a large misunderstanding about what math really is, since it's much easier to expose a child in kindergarten to puzzles than to De Rahm cohomology and derived functors. In any case, a good mathematician studies something very fundamental, and then when this thing is examined, it looks different from every side.

The Burnside theorem is in fact an example of when some fundamental object looks different from different sides. We can calculate the same thing multiple ways, and get non-trivial content out of this. In particular, it is highly non-obvious that stabilizers and fixed points are so closely related. Indeed it is even more interesting that they are related by this non-trivial matrix of marks.

$$\left|(G/K)^H\right| = \left|\{xK \mid H < {}^xK\}\right|$$

since $H < {}^xK$ iff $H <^G K$. So each of $N_G(H)/H$ divides $|G|$, because the order of G is the product of three numbers. So what we are driving at, is that this matrix M_G, the matrix of marks for fintie group G, is triangular, and its triangular elements are $m_{HH} = |N_G(H) : H|$. So we have

$$|G| = |G : N_G(H)|\,|N_G(H) : H|\,|H|$$

So the determinant of the matrix itself, which is integral valued, is

$$\det M_G = \prod_{H \in [\![\mathrm{Sgr}_G]\!]} |N_G(H) : H|$$

where each term is a natural number > 0. This shows that the sub-lattice of $\mathbb{Z}^{\mathrm{Sgr}_G}$ coinciding with the image of M_G, is the image of the Burnside ring $B(G)$ under the fixed points counting homomorphism.

If you apply a matrix from $\mathbb{Z}^N$ to $\mathbb{Z}^N$ for N some finite set, and we have a left matrix multiplication by an integral matrix L_M, then the image is a sub-lattice. Now we have thar $\det \neq 0$ iff the quotient is $\mathbb{Z}^N/M\mathbb{Z}^N$. These are simply the things in the image, so they are linear combinations, with integral coefficients. So they are the columns of that matrix. Now this is an abelian group, so if we tensor by $\mathbb{Q}$, we get:

$$\begin{tikzcd}\mathbb{Z}^N \arrow[r, "L_M"] & \mathbb{Z}^N \arrow[r, two heads] & \mathbb{Z}^N/M\mathbb{Z}^N\end{tikzcd}$$

$$\begin{tikzcd}\mathbb{Z}^N \otimes_{\mathbb{Z}} \mathbb{Q} \arrow[r, "L_M"] & \mathbb{Z}^N \otimes_{\mathbb{Z}} \mathbb{Q} \arrow[r, two heads] & \mathbb{Z}^N/M\mathbb{Z}^N \otimes_{\mathbb{Z}} \mathbb{Q}\end{tikzcd}$$

So this means the determinant is nonzero iff the quotient group is torsion. But if we take a free finitely generated abelian group divided by any subgroup, then this is always free. This is not a trivial fact at all. For a proof, see chapter 1 in [1]. This is in fact true for all Dedekind domains, and not only $\mathbb{Z}$.

In any case we get that the quotient is a finite group. We also know, that in order to invert the determinant, we need only to be able to invert the order of the group G. This means that actually, if we look at $B(G)$, and tensor over $\mathbb{Z}$:

$$B(G) \otimes_{\mathbb{Z}} \mathbb{Z}\left[|G|^{-1}\right] \xrightarrow{\sim} \mathbb{Z}\left[|G|^{-1}\right]^{\mathrm{Sgr}}$$

under the fixed points counting map. We are tensoring the product, but because the product is finite, from the Abelian point of view, this is the same as the direct sum. If this direct product was infinite, this would not be the case. This is of course not the case, because tensor products of modules commute with arbitrary direct sums.

Now notice that $\mathbb{Z}^{\mathrm{Sgr}_G}/B(G)$ is in fact finite (not only torsion) and in particular, we have the formula,

$$\det M_G = \left|\mathbb{Z}^{\mathrm{Sgr}_G}/B(G)\right|$$

because if we take a square matrix with integral coefficients, whose determinant is non-zero, then actually the quotient of the target by its image will be a group which has order being the covolume of one lattice in another, and this covolume is calculated in terms of the determinant. In other words, we are actually taking a fundamental domain of the image, and because it is sparser, it will be bigger. And, we will tile it, with the fundamental domain of the target. And we will find, that there are as many piece there, as the index of one group in another.

Chapter 3

Nilpotent groups

3.1 p-groups

3.1.1 Cauchy's theorem

Definition 3.1. We say that G is a π group, where π is a set of primes, iff the order of any element $g \in G$ is a product of powers of $p \in \pi$.

Example 3.1. For $\pi = \{p\}$, we call G a *p-group.*

One often writes π' as the complement of π. In particular, p' is the set of primes distinct from the prime p.

Remark 3.1. Often times a p group is defined to be a group which has order a power of a prime. This however doesn't make sense for an infinite group, so our definition is somewhat more robust. This might seem like a minimal consideration, but in fact infinite p-groups are very important in arithmetic algebraic geometry. For example, see [2, 3] written by Demazure, a student of Grothendieck.

We now offer a very basic observation:

Proposition 3.1. *Suppose that $|G| = p^n$ for some prime p. Let X be a finite G-set. Then*

$$|X| = \left|X^G\right| \pmod p$$

Proof. Let $|G| = p^n$ for some prime p.[3.1] Let X be a finite G-set. Then all such X can be written as the disjoint union $X = X^G \cup \left(X \setminus X^G\right)$, which means we can write $|X| = \left|X^G\right| + \left|X \setminus X^G\right|$. Note the fixed points correspond to points with stabilizers equal to G, so all of the other points have stabilizers which are proper subgroups $\operatorname{Stab}_G x < G$. Now we also have that

$$X \simeq \bigcup_{\mathcal{O} \in X_G \setminus X^G} \mathcal{O}$$

[3.1] Note that by Lagrange's theorem, this is a p group. Not in the reverse, a priori.

where each $\mathcal{O} \simeq G/\operatorname{Stab}_G x$ for any $x \in \mathcal{O}$. This means $|\mathcal{O}| = |G : \operatorname{Stab}_G x| > 1$ is divisible by p for every x such that $\operatorname{Stab}_G x < G$ properly. But we already saw that points in $X \setminus X^G$ are exactly the points where $\operatorname{Stab}_G x$ is a proper subgroup. This means we have the observation that

$$|X| = \left|X^G\right| \pmod{p}$$

This should be viewed as equality in $\mathbb{Z}/p\mathbb{Z}$. □

Fact 3.1 is one of the most commonly used facts in finite group theory. We can apply this in a novel way to obtain:

Theorem 3.1 (Cauchy)**.** *If p divides $|G|$, then there exists an element of order p in G.*

Proof. Apply proposition 3.1 to the set

$$X \coloneqq \{(g_1, \cdots, g_p) \in G^p \mid g_1 \cdots g_p = e\}$$

under the cyclic right shift action of the group $\mathbb{Z}/p\mathbb{Z}$ given by:

$$(g_1, \cdots, g_p) \xmapsto{1} (g_p, g_1, \cdots, g_{p-1})$$

Exercise 3.1.1. Verify that this action of $\mathbb{Z}/p\mathbb{Z}$ does indeed preserves the definition of X.

So from the proposition we have:

$$\left|X^{\mathbb{Z}/p\mathbb{Z}}\right| = |X| \pmod{p}$$

Notice any sequence of $p-1$ elements in G, can be completed in a unique way to an element of X. In other words, we have a map:

$$\begin{tikzcd}
G^{p-1} \arrow[r] & X \\
(g_1, \cdots, g_{p-1}) \arrow[r, mapsto] & \left(g_1, \cdots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1}\right) \\
(g_1, \cdots, g_{p-1}) & (g_1, \cdots, g_p) \arrow[l, mapsto]
\end{tikzcd}$$

which is in fact a bijection. So indeed, p divides $|X| \pmod{p} = p^{p-1}n$, and therefore $\left|X^{\mathbb{Z}/p\mathbb{Z}}\right| = 0 \pmod{p}$.

Now notice that the fixed points are exactly

$$X^{\mathbb{Z}/p\mathbb{Z}} = \{(g, \cdots, g) \in G^p \mid g^p = e\}$$

which is nonempty, since $(e, \cdots, e) \in X^{\mathbb{Z}/p\mathbb{Z}}$. So now we have a bijection

$$\{g \in G \mid p = |g|\} \cup \{e\} \leftrightarrow X^{\mathbb{Z}/p\mathbb{Z}}$$

by sending $g \mapsto (g, \cdots, g) \in G^p$. So since we know that $\left|X^{\mathbb{Z}/p\mathbb{Z}}\right|$ is divisible by p, the previously noted bijection gives us:

$$|\{g \in G \,|\, p = |g|\}| = -1 \pmod{p}$$

and we are done. □

Corollary 3.1. *Finite p groups are precisely groups of order a power of p.*

Corollary 3.2. *Let p divide the order of G. Then the number of subgroups of order p, $\mathrm{Sgr}_p\, G$, is congruent to 1 modulo p.*

Proof. Take an element of order $|g| = p$, and consider the powers

$$e = g^p, g, g^2, \cdots, g^{p-1}$$

which of course make up the cyclic group $\langle g \rangle$. But now notice that e is the only element with order one in $\langle g \rangle$. All of the other $p - 1$ elements have order p. Now take another element g' of order p. Two possibilities: Well $\langle g \rangle$ and $\langle g' \rangle$ are both cyclic, and their intersection is either trivial, or they coincide exactly. This follows directly from Lagrange's theorem.

So now we have the disjoint union:

$$\{g \in G \,|\, |g| = p\} = \bigcup_{C \in \mathrm{Sgr}_p\, G} C \setminus \mathrm{I} = \bigcup_{C \in \mathrm{Sgr}_p\, G} C^{\#}$$

where $C^{\#}$ denotes C without the identity element. Then since each C^* has $p-1$ elements, and this is a disjoint union, we have the following:

$$|\{g \in G \,|\, |g| = p\}| = (p-1)\left|\mathrm{Sgr}_p\, G\right| = (-1)\left|\mathrm{Sgr}_p\, G\right| \pmod{p}$$

So now we combine this with knowing that the number of elements of order p is actually equal to $-1 \pmod{p}$, to get that $\left|\mathrm{Sgr}_p\, G\right| = 1 \pmod{p}$ as desired. □

This means that in any finite group, we always have an odd number of elements of order 2, if the order of the group is even. If the order is odd, we don't have any at all.

Exercise 3.1.2. Consider the groups of order 12. This is of course a difficult task to tackle with bare hands. But even with these simple considerations, we know that every such group must have a subgroup of order 3, and in fact must have either 1, so it is normal, or 4 of them. Then in this second case, the obligatory element(s) of order 2 must form only a single group, which is therefore normal. So we can say quite a bit about this relatively complicated problem without much work.

3.1.2 Subnormal series

The following corollary gives one of the defining results used for the characterization of nilpotent groups.

Corollary 3.3. *If G is a finite p group, then any subgroup H is subnormal, which means there exists a finite subnormal series starting at H and terminating at G:*

$$H = H_0 \lhd H_1 \lhd \cdots \lhd H_m = G$$

Proof. Let G be any finite group where $|G| = p^n m$ where $n < 0$ and $p \not| m$. So $p|\,|G|$. Now let P be a p-subgroup of G. Suppose $|P| = p^l$ for some $l \in \mathbb{N}$. Then we have two possibilities. If $l < n$ then $p|\,|G/P|$. If $l = n$, then $p \not| \,|G/P|$. Now look at $(G/P)^P = \frac{N_G(P)}{P}$. We know that the number of elements here, is

$$\left|(G/P)^P\right| = \left|\frac{N_G(P)}{P}\right| = |G/P| \pmod p$$

so when $l < n$, this cardinality is zero. It is only non-zero when $l = n$.

So if P is a p-group of non-maximal order, then automatically, P is normalized by a larger group. Now consider the extension:

$$\begin{tikzcd}
\frac{N_g(P)}{P} & N_G(P) \arrow[l, two heads, "\pi"'] & P \arrow[l, tail]
\end{tikzcd}$$

So apply Cauchy's theorem to this quotient group. This shows there is a cyclic group C_p of order p within $N_G(P)/P$. In particular, if we take the pre-image $\pi^{-1}(C_p)$, the kernel is the same, so we get a sub-extension:

$$\begin{tikzcd}
C_p \arrow[d, hook] & P' \arrow[l, two heads] \arrow[d, hook] & P \arrow[l, tail] \arrow[d, equal] \\
\frac{N_g(P)}{P} & N_G(P) \arrow[l, two heads, "\pi"'] & P \arrow[l, tail]
\end{tikzcd}$$

Now, by Lagrange's theorem, we have that

$$|P'| = |C_P|\,|P| = pp^l = p^{l+1}$$

So we have shown that if P is a p subgroup, whose order is not maximal, then P in fact sits as a normal subgroup, in a group of order P^{l+1} So what this actually means, is we have the following:

$$P = P_l \lhd P' = P_{l+1} \lhd P_{l+2} \lhd \cdots \lhd P_n$$

so every p subgroup of every finite group, is the beginning of a subnormal series (or subnormal flag or subnormal chain). $\square$

Look at all of the possible subnormal chains starting with H. Then the smallest length m of such a subnormal chain will be called the class of subnormality. H is also said to be m-subnormal. Note that 1-subnormal means normal.

As it turns out, a group G is Nilpotent iff every subgroup is subnormal. In fact, finite Nilpotent groups are precisely products of p-groups. This is of course not the definition, and we have to wait a bit before we see that this is the case.

Remark 3.2. Quantum Abelian groups are precisely nilpotent groups.

It is important to notice that corollary 3.3 holds for arbitrary finite p-groups. For examples such as the so-called monster group and such, these incredibly complicated groups are guaranteed to have these subnormal flags, which are effectively incedence geometries. There is a sense in which we can realize some exotic groups, as symmetries of certain finite incedence geometries.

3.1.3 Sylow theorems

Corollary 3.4. *A maximal p subgroup in a group of order $p^n m$ where $(m, p) = 1$ has p^n elements. Such subgroups are called Sylow p-subgroups. So in other words, if p^n divides $|G|$ and p^{n+1} does not divide $|G|$, there exists some p-Sylow subgroup.*

Theorem 3.2. *Suppose $|G| = p^n m$ for $(m, p) = 1$. Then we have the following:*

1. *Any p-subgroup P of order p^l is contained in the increasing flag of p-subgroups:*
$$P = P_l < P_{l+1} < \cdots < P_n$$
where $|P_i| = p^i$.
2. *Given a p-subgroup P and a Sylow p subgroup P', then $P < {}^g P'$ for some $g \in G$.*
3. *Write $\left|\operatorname{Syl}_p G\right|$ for the number of Sylow p-subgroups. Then $\left|\operatorname{Syl}_p G\right|$ divides m, and $\left|\operatorname{Syl}_p G\right| \equiv 1 \pmod p$.*

Proof. (1): Cauchy's theorem guarantees, that if $|G| = p^n m$, then there are indeed p subgroups. But now from corollary 3.3 this implies there is a subnormal flag $\mathrm{I} < P_1 \lhd P_2 \lhd P_3 \cdots \lhd P_n$ such that each P_i has order $|P_i| = p^i$.

(2): Let P be a p-subgroup, and P' a Sylow p subgroup. Then consider $(G/P')^P$. Now we have

$$|\{gP' \mid P < {}^g P'\}| = |G/P'| \pmod p \neq 0 \pmod p$$

since P' is the maximal p-subgroup. This means we have shown even more than required of us. We have in fact shown that every p-subgroup $P <^G P'$.[3.2]

[3.2] This is a perfect example of a proof which takes advantage of our approach from the very beginning. Our considerations of categories of G-sets and such gave us motivation to consider these objects, which would have otherwise seemed arbitrary.

(3): Since all p-Sylow subgroups are conjugate, this means they form a single orbit under adjoint action. So now just have to calculate the number of elements in a single orbit. But we know this is just the index in G, of the stabilizer: $\left|\mathrm{Syl}_p G\right| = |G : N_G(P)|$ for any p-Sylow subgroup P. So we have that:

$$|G : N_G(P)|\,|N_G(P) : P| = |G : P| = m$$

and $n_p|m$ as desired. Now we have

$$(G/P)^P = \frac{N_G(P)}{P} \subset G/P$$

But now notice that

$$\left|\frac{N_G(P)}{P}\right| = \left|\frac{G}{P}\right| \pmod{p} = m \pmod{p}$$

which means we can divide by m in $\mathbb{Z}/p\mathbb{Z}$, since this is a field, and get that $\left|\mathrm{Syl}_p G\right| \equiv 1 \pmod{p}$. ☐

Corollary 3.5. *If P, P' are Sylow p-subgroups, then they are conjugate.*

Proof. This is the usual form of the second Sylow theorem. It follows directly from our formulation of the second Sylow theorem. ☐

Example 3.2. Theorem 3.2 is very useful for classification of finite groups. In particular, consider a finite group of order $p^e q$ such that $(p, q) = 1$. In particular, if q is prime, then we either have q p-Sylow subgroups, or exactly 1. But by the second Sylow theorem, if there is only one, this is a normal subgroup.

3.2 Exercises

Let G be a finite group, and let $|G| = p^e m$ for $e > 0$. Let $G^{\#} = G \setminus \mathrm{I}$. Consider orbital decomposition into conjugacy classes:

$$G^{\#} = \bigcup_{x \in [\![G^{\#}]\!]} G/C_G(x)$$

where $C_G(x)$ is the centralizer.

Now suppose $X \subset G$. We can build two different subgroups of G out of this, by considering $C_G(X)$ and $N_G(X)$ In particular, we have two maps $\mathcal{P}(G) \to \mathrm{Sgr}\, G$ which reverse the order. We can either $X \mapsto C_G(X)$ or $N_G(X)$. This is notable, because this is a homomorphism of lattices.

Recall that any subset of any group generates a subgroup, denoted by $\langle X \rangle$. This is defined as the intersection of all subgroups which contain X. Note that it is obvious that $C_G(X) = C_G(\langle X \rangle)$. On the other hand, we have $N_G(X) < N_G(\langle X \rangle)$.

Exercise 3.2.1. Show that there exists an element $x \neq e$ such that p divides $|C_G(x)|$.

Exercise 3.2.2. Prove that if p divides the order of some finite group G, there exists an element of order p.

Exercise 3.2.3. Show that if G is non-Abelian, then G/ZG is not cyclic.

3.3 Filtrations

Definition 3.2. The upper central series of a group G is an *increasing filtration* iff

$$\mathrm{I} = Z_0G < Z_1G < \cdots < Z_lG < Z_{l+1}G < \cdots < G$$

where

$$Z_l := \{g \in G \mid [G, g] \in Z_{l-1}\}$$

is called the l-center subgroup.

This characterization is equivalent to defining

$$Z_l = \{g \in G \mid [G, \cdots [G, g] \cdots] = \mathrm{I}\}$$

where the commutator is taken l times. In particular, $Z_1G = ZG$ is the center of the group. This is also equivalent to having the following diagram for each l:

$$\begin{tikzcd}
G/Z_lG & G \arrow[l, two heads] & Z_lG \arrow[l, tail] \\
Z\left(G/Z_lG\right) \arrow[u, hook] & Z_{l+1}G \arrow[l, two heads] \arrow[u, hook] & Z_lG \arrow[l, tail] \arrow[u, equal]
\end{tikzcd}$$

Definition 3.3. A subgroup is *characteristic* iff it is invariant under any automorphism α of G.

Proposition 3.2. *Each subgroup Z_lG is characteristic.*

Proof. We apply $\alpha(g)$ and verify this condition still holds:

$$[G, \cdots, [G, \alpha(g)] \cdots] = \alpha([G, \cdots [G, g] \cdots]) = \alpha(\mathrm{I}) = \mathrm{I}$$

since $G = \alpha(G)$. □

Proposition 3.3. *Characteristic subgroups are normal in G.*

Definition 3.4. Let $\Omega \subset \mathrm{Aut}(G)$ be a set of automorphisms of a group G. Then an Ω-series of subgroups is a series $\cdots < G_i < G_{i+1} < \cdots$ if each G_i is Ω invariant.

Example 3.3. Consider a filtration $\cdots \lhd G_i \lhd G_{i+1} \lhd \cdots$ such that every G_i is characteristic in G_{i+1}. Then if any G_j is characteristic in G, then all of the G_k for $k \leq j$ are characteristic in G. In other words, if the series begins at the trivial group, and extends to G, then it is actually stronger to be sub-characteristic than it is to be globally characteristic.

Now if we restrict our attention to inner automorphisms[3.3] then if we have a filtration of subgroups invariant under the inner automorphisms of the next one, then this is clearly a subnormal series, in the sense that each subgroup is normal in the next. But then in this case, even if this series begins at the trivial group and extends to G, it doesn't mean anything besides the final element is normal in G. This boils down to the fact that if we have three subgroup $A \lhd B \lhd C$, we don't necessarily have that $A \lhd C$.

Remark 3.3. The previous example brings to attention the difference between a normal series, where each subgroup is normal in the group, and a subnormal series, where each subgroup is normal in the next.

Definition 3.5. An increasing filtration

$$\cdots \subseteq X_l \subseteq X_{l+1} \subseteq \cdots X$$

of a set X for $l \in \mathbb{Z}$ is *co-complete* iff

$$\bigcup_{l \in \mathbb{Z}} X_l = X$$

It is said that an element $x \in X$ has finite filtration l, iff $x \in X_l$. It is *separable* iff

$$\bigcap_{l \in \mathbb{Z}} X_l = \emptyset$$

Warning 3.1. If we are defining a separable increasing filtration for $\mathbf{Set}_*$ (the category of sets with distinguished elements) we would define the intersection of the element to be the set containing the distinguished element. More generally we take the intersection to be the initial object. Note this is consistent with the previous definition, since $\emptyset$ is the initial object in **Set**.

Remark 3.4. We could also define the dual notion of a complete filtration.

3.4 Definition and application to p-groups

Definition 3.6. A group G is *nilpotent* iff there is n such that $Z_n G = G$. If $Z_n G = G$, but $Z_{n-1} G \neq G$, then we say that G is nilpotent of *class* n. It is also said that G is nilpotent of *level* n.

Proposition 3.4. *The center $ZG \neq I$ for any finite p-group.*

[3.3] This is the smallest group of automorphisms which contains conjugation.

Proof. Let G be a p-group. Since ZG is the set of fixed points with respect to the adjoint action of G, we have $|ZG| = |G| \pmod p$. But this is 0, so p divides $|ZG|$ and it therefore cannot be 1. ☐

Corollary 3.6. *Every finite p-group is nilpotent.*

Proof. By induction on the powers of p, this means that Z_2G is strictly bigger since $Z(G/ZG) \neq 1$ which is only the case when $ZG < Z_2G$ strictly. Therefore, we have a strictly increasing sequence of subgroups, which means we must terminate at G. ☐

Proposition 3.5. *Any subgroup of any finite p-group is actually the corresponding term of the complete flag which is a subnormal series.*

Proof. Recall we established that in a finite p-group G with $|G| = p^e$, for every subgroup $H < G$ with $|H| = p^l$ we have the subnormal series:

$$H = H_l \triangleleft H_{l+1} \triangleleft H_{l+2} \triangleleft \cdots \triangleleft G$$

where H_{l+1} has order p^{l+1}. Now $ZH \neq \mathrm{I}$ is a p-group, so by Cauchy's theorem this contains some cyclic group C_p of order p. Now call $H_1 = C_p$, and apply this argument to $H = G$. ☐

Proposition 3.6. *For every proper subgroup $H < G$ of a finite p-group, the normalizer $N_G(H)$ contains H as a strict normal subgroup.*

Proof. We know that $\left|(G/H)^H\right| = |G/H| = 0 \pmod p$. This is of course

$$(G/H)^H = \frac{N_G(H)}{H}$$

if $H \neq \mathrm{I}$. But if H is trivial, obviously $(G/H)^H = G$. ☐

Corollary 3.7. *Suppose we have two finite p-groups $H < H'$ such that H is the maximal proper subgroup of H'. Then $N_{H'}(H) = H'$.*

Proof. So if we have two finite p-groups $H < H'$ such that H is maximal, then we know $|H : H'| = p$. Now we know the normalizer satisfies:

$$H < N_{H'}(H) \leq H'$$

So now we have that

$$p = |H' : H| = |H : N_{H'}(H)|\, |N_{H'}(H) : H|$$

but we know $|N_{H'}(H) : H| \neq 1$, so $H' = N_{H'}(H)$. ☐

In other words, every maximal subgroup has order p and is normal. Now this means, if we consider the action of a finite p-group G on the set of all subgroups, this means the maximal subgroups are fixed points of this action.

3.5 Subgroups of nilpotent groups

Proposition 3.7. *The product of two nilpotent groups is nilpotent.*

This means any positive integer is the order of some nilpotent group, since all p-groups are nilpotent, and all positive integers can be expressed as a product of primes.

Proposition 3.8. *Every proper subgroup of every finite nilpotent group is normalized by some larger group. In other words, it is a proper subgroup of its normalizer.*

Proof. Let H be any such proper subgroup, and write $Z = ZG$. We have that $H \triangleleft HZ$ trivially. So now we have two possibilities. If $HZ > H$ properly, then we are done. But if not, then $H = HZ$ and then we have that $H/(Z \cap H) = HZ/Z < G/Z$ properly. Now what is important, is that G/Z is nilpotent of class $n-1$ where G is nilpotent of class n.[3.4] Now we take this normal subgroup, and consider its pre-image. In general, if we have $N \subset H$, where $N \triangleleft G$, then if $K < G/N$ normalizes H/N, the pre-image of K in G normalizes H. This is because if an element in the quotient G/N normalizes H/N, then since N is normal, its pre-image in G clearly normalizes H. So now by induction on the nilpotency class, we have the result. ☐

The following statement might be called a “fourth Sylow theorem.”

Proposition 3.9. *For all $|G| < \infty$, and P Sylow, then*

$$N_G(N_G(P)) = N_G(P)$$

which means if P is not a normal subgroup of G, then G is not nilpotent.

Proof. This is equivalent to showing that a group G is not nilpotent if there exists a non-normal Sylow p-subgroup. But saying this is not-normal, means there is more than 1, since a Sylow p-subgroup is normal iff it is unique.

Now if we consider P as a Sylow p-subgroup of the normalizer as well, then it is normal in this group, and therefore unique. But this means that every element of the normalizer of the normalizer fixes P, and therefore normalizes P. Therefore we have equality. ☐

So now we have shown that if we have one non-normal Sylow p-subgroup, then the group is not nilpotent. We now consider the opposite, to get the following remarkable fact:

Proposition 3.10. *Every finite Nilpotent group is canonically isomorphic to the product of its Sylow p-subgroups.*

[3.4] Note for $n = 1$ they are Abelian. In particular, every proper subgroup of an Abelian group is normalized by the whole group.

Proof. We know in general that I $= [H, K] \subseteq K \cap H$ iff H,K normalize one another. So now do this for groups $P_1, \cdots, P_l$ where these are our unique normal Sylow p-subgroups for all primes. So saying they are normal in each other, is saying their commutators are contained in their intersections. But the intersections are simultaneously p, q groups for two different primes p, q meaning this is just the trivial group. Therefore two groups which normalize each other with relatively prime orders must commute. In general, if we have a bunch of subgroups H_i such that elements of H_i commute with H_j for $i \neq j$, then we have a map from the product into G. This is a homomorphism of groups, with trivial kernel, since the orders are relatively prime. This means the map is injective, so now if these guys are Sylow p-subgroups, then the order of this is the product of these primes, which is the order of G. So we get an inclusion of the product to a group of the same order as G, so this is an isomorphism. □

All together we have shown that a finite group is nilpotent iff every of its Sylow p-subgroups is normal, and in this case, the group is the product of such Sylow p-subgroups. So the theory of finite Nilpotent groups is just the theory of finite p-groups. This is of course not the case for infinite groups.

3.6 Commutator calculus

For $x, y \in G$, define

$$[x, y] \coloneqq xy\,(yx)^{-1} = xyx^{-1}y^{-1}$$

This is a function $G, G \to G$. Note this is not exactly a homomorphism, since it is sort of twisted in the sense that it is not "additive" in the left argument.

Proposition 3.11. *The commutator is skew symmetric.*

Proof. Clearly $[y, x] = [x, y]^{-1}$. □

For any $H, K < G$, we define

$$[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle$$

This is perhaps the more tempting choice which we denote by the following notation:

$$[X, Y]_n = \{[x_1, y_1] \cdots [x_n, y_n] \mid x_i \in X, y_i \in Y\}$$

This is however not in general a subgroup.

Notice that $[X, X]_1$ is closed with respect to taking inverses, but is not closed under multiplication. This is independent of X being closed under inverses, this is only a consequence of skew symmetry. Of course if X has the identity element, then we have the filtration

$$[X, X]_1 \subseteq [X, X]_2 \subseteq \cdots [X, X] = \bigcup_{n \geq 1} [X, X]_n$$

In fact, if $H, K < G$, then this still applies. We even have

$$[H, K] = [K, H]$$

This is a non-trivial fact with follows from some basic identities.

Definition 3.7. A group G is *perfect* iff $G = [G, G]$.

Definition 3.8. A group G is *quasi-perfect* iff the commutator subgroup $[G, G]$ is perfect.

Now recall that an extension of a group G is the following:

$$G \twoheadleftarrow G' \hookleftarrow K$$

One might say G' is an extension of a group G means there is a short exact sequence in **Grp** as above. This sequence itself it also referred to as an extension. We also say G' is an extension of G by K.

As it turns out, extensions of a group G form a category. To see this, take two extensions:

$$G \twoheadleftarrow G' \leftarrowtail K$$

$$H \twoheadleftarrow H' \leftarrowtail L$$

then a morphism in this category is given by compatible maps $G \leftrightarrow H$, $G' \leftrightarrow H'$, and $K \leftrightarrow L$. Now notice this compatibility is given by a notion of kernel and cokernel. The issue is of course, that the category **Grp** is non-Abelian, and we aren't guaranteed to have kernels and cokernels. We do however have the 0 object, so we can come up with an abstract notion of kernel and cokernel.

To see why this is a relevant discussion, suppose we have a non-normal $K < G'$. What is the cokernel of the homomorphism $K \hookrightarrow G'$? As it turns out, every homomorphism from any group to another group has a cokernel. This is really given by a universal property, where K maps to any other object trivially. We work out the details in the exercises.

Definition 3.9. A monomorphism κ in a category **C** is said to be *effective* or *regular* iff κ is the kernel of some morphism. We say an epimorphism is *effective* or *regular* iff it is the cokernel of some morphism.

Exercise 3.6.1. If κ has a cokernel π, then κ is effective iff κ is a kernel of its own cokernel π. Also show π is effective iff π is a cokernel of its own kernel κ.

There is in fact a notion of extension in any category with zero object. If we have the following:

$$a'' \xleftarrow[\pi]{} a \xleftarrow[\iota]{} a'$$

then we have two conditions for this to be an extension. Even though they overlap, we need both of them:

1. ι is the kernel of π

2. π is the cokernel of ι

In the category of vector spaces, or category of modules, we offer what these conditions mean. In fact, this discussion will hold in any additive category. In such categories extensions are given by exact sequences. So in fact, the first condition guarantees exactness at a and a', and the second condition guarantees exactness at a and a''. So as we mentioned earlier, even though these conditions overlap, they are certainly both necessary for the definition.

Proposition 3.12. *In Abelian categories every monomorphism is effective and every epimorphism is effective.*

Example 3.4. The previous proposition does not hold in **Grp**. In **Grp** every epimorphism is effective, but not every monomorphism is. To see this, let $H < G$ such that G is the smallest normal subgroup containing H. Then this means that every homomorphism from G to any other group which vanishes on H, is actually trivial. In fact this example exhibited what is called a simple group.

Definition 3.10. A group G is simple iff G and 1 are the only normal subgroups.

So simple groups are very complex groups, for which homomorphisms give us nothing, since they are all trivial, except for the embedding.

So if we take any subgroup which is not normal, then cokernel is the quotient by the normal closure.

Definition 3.11. An extension $G \twoheadleftarrow G' \hookleftarrow K$ is central iff $K \subset ZG'$.

Recall that we can restrict to the study of the extensions of some group G to get a category. Now we know by the definition of an extension, that specifying one morphism $G' \to H'$ is enough to specify the full morphism between the two extensions. But now let us consider only central extensions. This category may or may not have an initial object. This object is referred to as a universal central extension.

Theorem 3.3. *A group G has a universal central extension iff G is perfect.*

3.7 Exercises

Exercise 3.7.1. Prove the following identities:

$$[xy, z] = \left({}^{x}[y, z]\right)[x, z] \qquad\qquad [x, yz] = [x, y]\left({}^{y}[x, z]\right)$$

Exercise 3.7.2. Show that $[H, K] \subseteq H$ iff $K \subseteq N_G(H)$.

Exercise 3.7.3. Show that $[H, K] \triangleleft H$ and of course, also by symmetry, in K.

Exercise 3.7.4. Suppose $G = \langle H, K\rangle$, so every element in G, can be written as a finite product of elements of H and K. Show that $[H, K]\, H = \langle {}^{g}H \mid g \in G\rangle$.

Exercise 3.7.5. Suppose $H, K, L \lhd G$. Show that $[HK, L] = [H, L]\,[K, L]$ and $[H, KL] = [H, K]\,[H, L]$.

Exercise 3.7.6. Consider any diagram of group homomorphisms,

$$\begin{tikzcd}
G \arrow[d, "h"] & H \arrow[l, "f"'] \arrow[dl, "\text{trivial}"] \\
K &
\end{tikzcd}$$

i.e. $f(H) \subseteq \ker g$. Now define $H' := f(H)$. Then as we have seen, $\langle {}^{g}H' \mid g \in G \rangle$ is the smallest normal subgroup of G containing H'. Now define π to be the quotient homomorphism by this subgroup. Show that we have the following factorization:

$$\begin{tikzcd}
G' \arrow[dr, dashed, "\exists! h'"'] & G \arrow[l, two heads, "\pi"'] \arrow[d, "h"] & H \arrow[l, "f"'] \arrow[dl, "\text{trivial}"] \\
& K &
\end{tikzcd}$$

So we need to show two things. First we need to show that we have this unique map h'. Then we need to show that $\pi \circ f$ is trivial.

3.8 Consequences of the exercises

Recall from the first exercise, we have $[xy, z] = \left({}^{x}[y, z]\right)[x, z]$. The following is a consequence of this identity:

Corollary 3.8. *For any $a, b \in G$,*

$$[a^n, b] = \left({}^{a^{n-1}}[a, b]\right)\left({}^{a^{n-2}}[a, b]\right)\cdots\left({}^{a}[a, b]\right)[a, b]$$

with exactly n terms.[3.5]

We now have some consequences of this formula:

Corollary 3.9. *If $[a, [a, b]] = e$, then*

$$[a^n, b] = [a, b]^n$$

Corollary 3.10. *If $x, y \in G$ and $[x, y]$ commuted with x and y, then*

$$[x^m, y^n] = [x, y]^{mn}$$

for $m, n \in \mathbb{Z}$.

Corollary 3.11. *If $a \in Z_2G$, which is equivalent to $[a, g] \in ZG$ for all $g \in G$, then $[a^n, g] = [a, g]^n$.*

[3.5] Note that since conjugation does not change the degree of an element of a group, so since each term has degree one, this equation is consistent in this sense.

Definition 3.12. For any group G, the set of elements in G of finite order, $\operatorname{Tors} G$, is called the *torsion subgroup*. A group is called *torsion free* if $\operatorname{Tors} G$ is trivial.

Note that trivially, the quotient group $G/\operatorname{Tors} G$ is torsion free.

Proposition 3.13. *For any group G, $\operatorname{Tors} G$ is a characteristic subgroup.*

This gives us a canonical extension:

$$G/\operatorname{Tors} G \twoheadleftarrow G \hookleftarrow \operatorname{Tors} G$$

so every group is an extension of a torsion-free group by a torsion group.

In **Grp**, we have two sub-categories consisting of torsion groups, $\mathbf{Grp}_t$, and torsion free, $\mathbf{Grp}_{tf}$. The intersection consists only of trivial objects. It is important to note these are zero objects. We say these two categories are separated.

Proposition 3.14. *Let T be a torsion group and F be torsion free. Then $\operatorname{Hom}_{\mathbf{Grp}}(T, F)$ consists only of the zero morphism.*

Note that we have trivial embeddings of $\mathbf{Grp}_t \hookrightarrow \mathbf{Grp}$ and $\mathbf{Grp}_{tf} \hookrightarrow \mathbf{Grp}$. We also have functors

$$\begin{array}{ccc} \mathbf{Grp} \longrightarrow \mathbf{Grp}_t & \qquad & \mathbf{Grp} \longrightarrow \mathbf{Grp}_{tf} \\ \\ G \longmapsto \operatorname{Tors} G & \qquad & G \longmapsto G/\operatorname{Tors} G \end{array}$$

Exercise 3.8.1. What are the adjunctions here?

In general, take three categories $(\mathbf{C}, \mathbf{T}, \mathbf{F})$ separated, so $\mathbf{T} \cap \mathbf{F}$ consists of initial objects. Then there exists two functors TF and T, where $TF : \mathbf{C} \to \mathbf{F}$ and $T : \mathbf{C} \to \mathbf{T}$. Then we have an extension of functors:

$$\widetilde{TF} \twoheadleftarrow \mathrm{id}_{\mathbf{C}} \hookleftarrow \widetilde{T}$$

where $\widetilde{T}$ is T composed with inclusion.

Example 3.5. $TF(G) := G/\operatorname{Tors} G$ then $TF \circ TF \simeq TF$.

Now back to the corollaries of the exercises:

Corollary 3.12. *Suppose that $x \in Z_2G$. Let ZG be a torsion group annihilated by some $n \in \mathbb{Z}$. Then $x^n \in ZG$. Equivalently, $Z(G/ZG) = Z_2G/ZG$ is annihilated by n.*

Proof. Since $z \in Z_2G$, for every $y \in G$, $[x, y]$ commutes with x. Therefore we can apply the above corollary to get that $x^n \in ZG$. $\square$

In general, by induction on l, one obtains that $Z_l G$ is a torsion group annihilated by n^l.

Corollary 3.13. *If G is nilpotent of class l, and the center of G is annihilated by n, then every element in G is annihilated by n^l.*

Warning 3.2. A priori, if we have a group generated by a certain set of a certain cardinality, this doesn't mean anything about the generation of subgroups. In particular, if a group is finitely generated, it doesn't follow that a subgroup, or even the center, is finitely generated.

Suppose $z_1, \cdots, z_m$ generate G. Then if $[x, z_i] \in ZG$ and there exists n_i such that $[x, z_i]^{n_i} = e$ then taking $n := \operatorname{lcm}(n_i)$ gives us that x^n commutes with all the z_i. From this it follows trivially that it commutes with any element of any group generated by these elements.

Proposition 3.15. *If G is a finitely generated nilpotent group such that ZG is a torsion group, then G is a torsion group.*

We now note a special case of this proposition:

Proposition 3.16. *A finitely generated nilpotent group is finite iff its center is finite.*

The statement of the next result looks like abstract nonsense. The importance is explained through the proof.

Proposition 3.17 (Witt identity)**.** *For $x, y, z \in G$,*

$$\left({}^{x}\left[z,\left[x^{-1},y\right]\right]\right)\cdot\left({}^{y}\left[x,\left[y^{-1},z\right]\right]\right)\cdot\left({}^{z}\left[y,\left[z^{-1},x\right]\right]\right)=e$$

Proof. First, we introduce some non-standard notation. For three group elements $a, b, c \in G$ we write:

$$a \cdot_b c := cac^{-1}bc$$

Now, take $x, y, z \in G$. We desire to show some motivation as to how one might find this identity out, and why one might care about this. First note that

$$[z,[x,y]] = z\left(xyx^{-1}y^{-1}\right)z^{-1}yxy^{-1}x^{-1}$$

so taking the inverse of x,

$$\left[z,\left[x^{-1},y\right]\right] = z\left(x^{-1}yxy^{-1}\right)z^{-1}yx^{-1}y^{-1}x$$

and now conjugating by x, we can write:

$$\begin{aligned}{}^{x}\left[z,\left[x^{-1},y\right]\right] &= xz\left(x^{-1}yxy^{-1}\right)z^{-1}yx^{-1}y^{-1}xx^{-1}\\ &= \left(xzx^{-1}yx\right)\left(y^{-1}z^{-1}yx^{-1}y^{-1}\right)\\ &= \left(z\cdot_x y\right)\left(z^{-1}\cdot_{y^{-1}}x^{-1}\right) = \left(z\cdot_x y\right)\left(x\cdot_y z\right)^{-1}\end{aligned}$$

so now permuting the role of x,y, and z we can write three expressions:

$$\begin{aligned} {}^{x}\left[z,\left[x^{-1},y\right]\right] &= \left(z\cdot_{x} y\right)\left(x\cdot_{y} z\right)^{-1} \\ {}^{y}\left[x,\left[y^{-1},z\right]\right] &= \left(x\cdot_{y} z\right)\left(y\cdot_{z} x\right)^{-1} \\ {}^{z}\left[y,\left[z^{-1},x\right]\right] &= \left(y\cdot_{z} x\right)\left(z\cdot_{x} y\right)^{-1} \end{aligned}$$

The result follows directly. □

Corollary 3.14. *Suppose* $H, K, L \lhd G$. *Then*

$$[H,[K,L]] \lhd [K,[L,H]]\,[L,[H,K]]$$

Exercise 3.8.2. Express $\left[x^{-1},y^{-1}\right]$ in terms of $\left[x,y^{-1}\right]$. Then express this in terms of $[x,y]$.

Corollary 3.15 (Three subgroups theorem)**.** *Let* $X, Y, Z < G$, *and* $N \lhd G$. *If* $[[X,Y],Z] \subseteq N$ *and* $[[Y,Z],X] \subseteq N$, *automatically* $[[Z,X],Y] \subseteq N$.

3.9 Decreasing filtrations

Definition 3.13. The upper central series of decreasing characteristic subgroups:

$$G = L^1G > L^2G > L^3G > \cdots$$

is a decreasing filtration iff

$$L^{i+1}G := \left[G, L^iG\right]$$

Equivalently we can define:

$$L^{i+1}G = \langle [g_1,[g_2,\cdots[g_i,g_{i+1}]\cdots]] \mid g_1,\cdots,g_{i+1} \in G\rangle$$

We will often take the notation $L^i = L^iG$. We now apply the three subgroup theorem in this setting. What we get is

$$\left[L^1, L^i\right] = L^{1+i}$$

Theorem 3.4. $\left[L^j, L^i\right] \subseteq L^{j+i}$

Proof. Proceed by induction on j. For $j = 1$ we have equality by definition. For L^2,

$$\begin{aligned} \left[L^2, L^i\right] = \left[L^i,\left[L^1,L^1\right]\right] &\subseteq \left[L^1,\left[L^i,L^1\right]\right]\left[L^1,\left[L^1,L^i\right]\right] \\ &= L^{i+2}L^{i+2} = L^{i+2} \end{aligned}$$

Now assume for all $i \in \mathbb{Z}^+$, and for all $j < m$,

$$\begin{aligned} \left[L^m, L^i\right] &= \left[\left[L^{m-1},L^1\right],L^i\right] \subseteq \left[L^1,\left[L^i,L^{m-1}\right]\right]\left[L^{m-1},\left[L^1,L^i\right]\right] \\ &= \left[L^1,\left[L^i,L^{m-1}\right]\right] \subset \left[L^1, L^{i+m-1}\right] = L^{i+m} \end{aligned}$$

$$\left[L^{m-1}, L^{1+i}\right] \subset L^{m+1}$$

So we proved that

$$\left[L^{i}, L^{j}\right] \subset L^{i+j}$$

□

3.10 Lie algebras

We now present a corollary of the theorem which gave us that $\left[L^{j}G, L^{i}G\right] \subseteq L^{j+i}G$.

Corollary 3.16.

$$\bigoplus_{i>0} L^{i}G/L^{i+1}G$$

is a $\mathbb{Z}^{+}$ *graded Abelian group, and in fact a Lie algebra under the Lie bracket operation:*

$$\left[\bar{g}, \bar{h}\right] = [g, h] \bmod L^{i+j+1}$$

for $\bar{g} \in L^{i}/L^{i+1}$ *and* $\bar{h} \in L^{j}/L^{j+1}$.

Proof. From the theorem,

$$\left[L^{i}, L^{i}\right] \subset L^{2i}$$

The Witt identity shows us directly that this does indeed satisfy the Jacobi identity in **Lie**G. □

In fact, this shows us we have a Lie ring functor:

$$\textbf{Grp} \xrightarrow{\textbf{Lie}} \mathbb{Z}_{+}\text{-graded Lie rings}$$

where these rings are of the form: $\mathfrak{g} = (g_i)_{i\in\mathbb{Z}_+}$ where $\mathfrak{g}$ is equipped with biadditive pairings given by the Lie bracket $[\,]$

$$g_i, g_j \to g_{i+j}$$

for $i, j \in \mathbb{Z}^{+}$. This pairing satisfies the following:

1. Bilinearity: for all $g_1, g_2, g_3 \in \mathfrak{g}$,

   $$[ag_1 + bg_2, g_3] = a\,[g_1, g_3] + b\,[g_2, g_3] \quad [g_1, ag_2 + bg_3] = a\,[g_1, g_2] + b\,[g_1, g_3]$$

2. Alternativity: for all $g \in \mathfrak{g}$.

   $$[g, g] = 0$$

3. Jacobi identity: For all g_1, g_2, g_3:

   $$g_1\,(g_2g_3) + g_2\,(g_3g_1) + g_3\,(g_1g_2) = 0$$

   In bracket notation this is written:

   $$[g_1, [g_2, g_3]] + [g_2, [g_3, g_1]] + [g_3, [g_1, g_2]] = 0$$

Proposition 3.18. *For all $g, h \in \mathfrak{g}$ we have:*

$$[g,h] = -[h,g]$$

And if we are not working in characteristic 2*, this is equivalent to alternativity.*

Proof. Bilinearity and alternativity imply that

$$[x+y, x+y] = [x,y] + [y,x] = 0$$

so we are done. ☐

Suppose we are given a $\mathbb{Z}$ graded k-algebra for k any commutative unital ring, called the ground ring, then we write this

$$A = (A_i)_{i\in\mathbb{Z}} \qquad\qquad A_i, A_j \to A_{i+j}$$

So we have defined Lie rings, and Lie rings that are $\mathbb{Z}^+$ graded. We also have a super Lie algebra, which is like a $\mathbb{Z}/2\mathbb{Z}$ graded Lie algebra, with a super skew-symmetry condition, and super Jacobi identity. We will see more about these.

We can also define a graded-commutator

$$[a,b] = ab - (-1)^{\tilde{a}\tilde{b}}\, ba$$

where $\tilde{a} \coloneqq$ degree of a modulo 2. Note this is not a commutator which is somehow graded, this is a graded-commutator. In the case that this is a super algebra, this is the parity of a.[3.6] We call a super-commutator the graded-commutator when the grading it $\mathbb{Z}/2\mathbb{Z}$.

1. graded-Lie algebra: has graded-Jacobi identity
2. graded Lie algebra: has Jacobi identity
3. super Lie algebras: has grading given by $\mathbb{Z}/2$ with super-commutator. Note this is different from $\mathbb{Z}/2$-graded lie algebras. However $\mathbb{Z}/2$-graded-Lie algebras are precisely super Lie algebras.

Note that graded-commutative means super commutator $[a,b] = 0$ for all a, b.

3.10.1 Campbell-Hausdorff formula

Proposition 3.19. *If the upper-central series of a group G stabilizes, so $L^iG = L^{i+1}G$ for some i, then* **Lie**G *is nilpotent, and $\mathbb{Z}^+$ graded.*

[3.6] Even parity are called bosons, and odd are called fermions.

Let $\mathfrak{g}$ be a $\mathbb{Z}^+$ graded Lie algebra:

$$\mathfrak{g} = (g_i)_{i \in \mathbb{Z}^+} \in \prod_{i \in \mathbb{Z}^+} g_i$$

convolution multiplication. We can define the formal sums:

$$g = \sum_{i \in \mathbb{Z}^+} g_i \qquad\qquad g' = \sum_{j \in \mathbb{Z}^+} g'_j$$

then we can just take

$$h_m = \sum_{i+j=m} g_i g'_j \qquad\qquad gg' := \sum_{m \in \mathbb{Z}^+} h_m$$

This allows us to formally define a map:

$$g \mapsto e^g := \sum_{n=0}^{\infty} \frac{1}{n!} g^n$$

Theorem 3.5 (Campbell-Hausdorff)**.**

$$e^g e^{g'} = e^{g * g'}$$

where

$$g * g' := g + g' + \frac{1}{2}\left[g_1, g_2\right] + \frac{1}{12}\left[g_1, \left[g_1, g_2\right]\right] + \frac{1}{12}\left[g_2, \left[g_2, g_1\right]\right] \\ - \frac{1}{24}\left[g_2, \left[g_1, \left[g_1, g_2\right]\right]\right] + \cdots$$

3.11 Exercises

Exercise 3.11.1. Given the Jacobi identity, derive and explain the analogous identity for a Lie superalgebra.

Exercise 3.11.2. Given $H < G$ and $P \in \operatorname{Syl}_p G$, show that $P \cap H \in \operatorname{Syl}_p H$.

Exercise 3.11.3. Given $H \triangleleft G$ and $Q \in \operatorname{Syl}_p H$, show that $G = HN_G(Q)$.

Exercise 3.11.4. Given $P \in \operatorname{Syl}_p G$, show that the $N_G(N_G(P)) = N_G(P)$. In other words, if P is not normal, it is impossible to build a normal flag starting at P and terminating at G.

Exercise 3.11.5. Suppose $|G| = p^e m$ where p is prime, and greater than m. Show that G has a normal p-subgroup. That is, G is an extension of a group G'' of order m, and a p-group:

$$G'' \twoheadleftarrow G \hookleftarrow P$$

where $|P| = p^e$ and $|G''| = m$.

Exercise 3.11.6. Suppose $|G| = p^2q$ for p,q prime. Prove that one of the following holds:

1. $p > q$ and G has a normal Sylow p-subgroup
2. $q > p$ and G has a normal Sylow q-subgroup
3. $|G| = 12$ and G has normal 2-subgroup.

3.12 Important functors

We offer a recap of some important functors we have seen in this chapter:

$$\begin{tikzcd}
\mathbf{Grp} \arrow[r, "\mathbf{Lie}"] & \text{Lie rings that are } \mathbb{Z}_+\text{-graded} \arrow[dddl, bend left] \\
\mathbf{Grp}_{\mathrm{ucsf}} \arrow[u, hook] \arrow[r, "\mathbf{Lie}"] & \text{nilpotent } \mathbb{Z}_+\text{-graded Lie rings} \\
\mathbf{Grp}_{\mathrm{nil}} \arrow[u, hook] \arrow[ur] & \\
\mathbf{Grp}_{\mathrm{nil,div}} \arrow[u, hook] &
\end{tikzcd}$$

where $\mathbf{Grp}_{\mathrm{ucsf}}$ denotes the category of groups with an upper central series of finite length. In particular this means we have:

$$G = L^1G \triangleright L^2G \triangleright \cdots \triangleright L^mG$$

of finite length.

Warning 3.3. Just because this flag is finite, doesn't mean it terminates at 1. This is of course the case when G is nilpotent.

We introduce the following definition:

Definition 3.14. A ring R is a *power associative* iff $xx^2 = x^2x$ and $x^2x^2 = \left(x^2x\right)x$ for all $x \in R$.

Then we have the following construction for all power associative rings R:

$$\mu_\infty(R) = \{r \in R \,|\, \exists n \geq 1 \text{ s.t. } r^n = 1\}$$

Example 3.6. A particular example of this is:

$$\mu_\infty(\mathbb{C}) = \{\zeta \in \mathbb{C} \,|\, \exists n \geq 1 \text{ s.t. } \zeta^n = 1\}$$

Example 3.7. This μ_∞ construction is very useful in algebraic number theory. It is often applied to rings of integers.

In general this defines the following for us:

$$\begin{tikzcd}
\mathbf{Grp} & \mathbf{Rng}_{\text{pow-ass}} \arrow[l, "\mu_\infty"']
\end{tikzcd}$$

$$\begin{tikzcd}
\mu_\infty\left(R\right) & R \arrow[l, mapsto]
\end{tikzcd}$$

In fact this forms an injective abelian group, which means for every abelian group A, a subgroup A', and homomorphism $f : A' \to \mu_\infty$, we have the following commutative diagram:

$$\begin{tikzcd}
 & \mu_\infty \\
A \arrow[ur, dashed, "\tilde{f}"] & A' \arrow[l, tail] \arrow[u, "f"]
\end{tikzcd}$$

In fact, μ_∞ is what is called a cogenerator of $\mathbf{Grp}_{\mathbf{Ab}}$. We have to introduce some preliminary concepts to actually define this.

Definition 3.15. An object $g \in \operatorname{Obj}\left(\mathbf{C}\right)$ is a *generator* iff for any pair of morphisms $\alpha, \beta : a \to b$ these are not equal iff there exists morphisms

$$\begin{tikzcd}
g \arrow[r, "\varphi"] \arrow[rr, bend left, "\alpha\circ\varphi"] \arrow[rr, bend right, "\beta\circ\varphi"'] & a \arrow[r, shift left, "\alpha"] \arrow[r, shift right, "\beta"'] & b
\end{tikzcd}$$

such that $\alpha \circ \varphi \neq \beta \circ \varphi$.

Proposition 3.20. *If* $\mathbf{C}$ *has arbitrary coproducts, then* g *is a generator iff for all* $a \in \operatorname{Obj}\left(\mathbf{C}\right)$*, there is an epimorphism:*

$$\coprod_X g \twoheadrightarrow a$$

Example 3.8. In the category $\mathbf{Grp}$, the group $\mathbb{Z}$ is a generator. So by this proposition we have that the free group generated by X:

$$\text{Free}\left(X\right) = \coprod_X \mathbb{Z}$$

satisfies the following:

$$\begin{tikzcd}
\text{Free}\left(X\right) \arrow[dr] & \\
X \arrow[u, hook] \arrow[r, hook] & G
\end{tikzcd}$$

Finally we have that a cogenerator is defined to be the dual of the generator, so we have the following:

Proposition 3.21. *If* $\mathbf{C}$ *has arbitrary products, then* c *is a cogenerator iff for all* $a \in \operatorname{Obj}(\mathbf{C})$ *there exists a monomorphism:*

$$a \hookrightarrow \prod_X c$$

Example 3.9. This proposition means every abelian group is a subgroup of an infinite product of torsion groups.

Theorem 3.6 (Baer)**.** *An abelian group* I *is injective iff* I *is divisible.*

This means in $\mathbf{Grp_{Ab}}$ the torsion free divisible groups are the same as $\mathbb{Q}$ vector spaces.

Definition 3.16. F is *flat* iff $\otimes F$ preserves exactness.

Proposition 3.22. F *is flat iff* F *is torsion free.*

Definition 3.17. A projective object is the dual object to an injective object.

Proposition 3.23. *A free abelian group is called* projective *iff it is a projective* $\mathbb{Z}$ *module.*

Definition 3.18. A category is an *additive category* iff there is an abelian group structure on the set of morphisms between any two objects such that the composition is biadditive. We also have that finite products exist.

Proposition 3.24. *The dual of an additive category is again additive.*

Definition 3.19. A category is an *exact category* iff it is written as a pair (A, E) where A is an additive category, and E is a class of sequences called exact which satisfies the following:

1. The class E is closed under isomorphisms and contains all split extensions. For any exact sequence the deflation is the cokernel of inflation and the inflation is the kernel of the deflation.

2. The class of deflations is closed under composition and base change by arbitrary maps. The class of inflations is closed under compositions and cobase change by arbitrary maps.

3. If a morphism $M \to M'$ having a kernel can factor a deflation $N \to M'$ as $N \to M \to M'$, then it is a deflation. If a morphism $I \to I'$ having a cokernel can factor as inflation $I \to J$ as $I \to I' \to J$ then it is also an inflation.

This is effectively just an additive category with some additional structure to allow for the notion of an exact sequence. This of course includes all Abelian categories. This notion was introduce by Quillen, and therefore they are often called Quillen-exact or exact in the sense of Quillen. It was later discovered by Deligne, that this is precisely the sort of category where the notion of a derived category exists.

Definition 3.20. An inflation is also called an admissable monomorphism, and a deflation is also called an admissable epimorphism. An extension is *admissable* iff it consists of admissable monomorphism and epimorphism.

Given an exact sequence $A'' \twoheadleftarrow A \hookleftarrow A'$, a basechange is given by the top line, and a cobasechange is given by the bottom line of the following diagram:

$$\begin{tikzcd}
B \arrow[d] & ? \arrow[l] \arrow[d] & A' \arrow[l] \arrow[d, equal] \\
A'' \arrow[d, equal] & A \arrow[l, two heads] \arrow[d] & A' \arrow[l, tail] \arrow[d] \\
A'' & ? \arrow[l] & C \arrow[l]
\end{tikzcd}$$

Chapter 4

Affine groups and Hopf algebras

4.1 Bimodules

Definition 4.1. Let A be a k-bimodule. In this text, when we say this is equipped with a k-bilinear map, we mean

$$\mu : A, A \to A$$

is additive in each argument, and k-balanced. This balancedness splits into the following three conditions:

$$\begin{aligned} \mu\left(ca_1, a_2\right) &= c\mu\left(a_1, a_2\right) \\ \mu\left(a_1 c, a_2\right) &= \mu\left(a_1, ca_2\right) \\ \mu\left(a_1, a_2 c\right) &= \mu\left(a_1, a_2\right) c \end{aligned}$$

Warning 4.1. For us, a k-bilinear map is not a bimodule map in each argument.

Now consider $A \in R$-**Mod**-S, $B \in S$-**Mod**-T. Then a k-bilinear map $\mu : A, B \to C \in R$-**Mod**-T satisfies:

$$\begin{tikzcd}
& A \otimes_S B \arrow[dr, dashed] & \\
A, B \arrow[ur] \arrow[rr, "\mu"] & & C
\end{tikzcd}$$

so even though a tensor product is often referred to as just the object, it should be thought of as a bifunctor from the categories of bimodules to the category of bilinear maps. In other words, the tensor product is an initial object in the category of bilinear maps. Note we can also extend this notion of linearity to n-products of such bimodules.

We have introduced the tensor product here as something which replaces multilinear maps with linear maps, which is indeed its main purpose. It is however usually introduces by the following:

$$\mathrm{Hom}_{R\text{-}\mathbf{Mod}\text{-}T}\left(A \otimes_S B, C\right) = \mathrm{Hom}_{R\text{-}\mathbf{Mod}\text{-}S}\left({}_RA_S, \mathrm{Hom}_{\mathbf{Mod}\text{-}T}\left({}_SB_T, {}_RC_T\right)\right)$$

which is in fact in the category R-**Mod**-S.

Warning 4.2. There is some ambiguity in considering $\mathrm{Hom}_{\mathbf{Mod}\text{-}T}\left({}_SB_T, {}_RC_T\right)$ since we have to take the forgetful functor such that we can consider B and C as objects in **Mod**-T in order to consider this Hom set. But then we need to recall that we didn't use these two left actions by S and R. Now we need to take the Hom set and equip this with a bimodule structure. Now if these rings are commutative this Hom set has this structure naturally, but this is not true over noncommutative rings.

4.2 Algebras

Definition 4.2. An associative k-algebra A with identity is a k-bimodule together with a pair of k-bilinear maps:

$$\mu : A \otimes A \to A \qquad\qquad \eta : k \to A$$

such that:

1. (associativity) the following diagram commutes:

$$\begin{tikzcd} A \otimes A \otimes A \arrow[r, "\mathrm{id} \otimes \mu"] \arrow[d, "\mu \otimes \mathrm{id}"] & A \otimes A \arrow[d, "\mu"] \\ A \otimes A \arrow[r, "\mu"] & A \end{tikzcd}$$

2. (identity) both of the following compositions comprise the identity:

$$A \simeq k \otimes A \xrightarrow{\eta \otimes \mathrm{id}} A \otimes A \xrightarrow{\mu} A$$

$$A \simeq A \otimes k \xrightarrow{\mathrm{id} \otimes \eta} A \otimes A \xrightarrow{\mu} A$$

4.3 Coalgebras

Let k be a fixed associative unital ring. We will refer to this as the ground ring. There is a functor:

$$\mathbf{Set} \to k\text{-}\mathbf{Coalg}_{\mathrm{com,un}}$$

first we define a coalgebra.

Definition 4.3. A k-coalgebra C is a k-bimodule equipped with a k-bimodule map from

$$\Delta : C \to C \otimes_k C$$

called comultiplication.

Definition 4.4. Coassociativity, cocommutativity, coidentity for comultiplication, and a unary operation providing the inverse for comultiplication are given by reversing the arrows for these constructions in the case of multiplication:

$$M \otimes_k M \to M$$

More concretely, a coassociative, counital k-coalgebra is a k-bimodule equipped with a comultiplication $\Delta : C \to C \otimes C$ and a counit $\epsilon : C \to k$ such that the following two diagrams commute:

$$\begin{tikzcd} C \arrow[r, "\Delta"] \arrow[d, "\Delta"] & C \otimes C \arrow[d, "\mathrm{id} \otimes \Delta"] \\ C \otimes C \arrow[r, "\Delta \otimes \mathrm{id}"] & C \otimes C \otimes C \end{tikzcd} \qquad \begin{tikzcd} C \arrow[rr, "\Delta"] \arrow[d, "\Delta"] \arrow[dr, "\mathrm{id}"] & & C \otimes C \arrow[d, "\mathrm{id} \otimes \epsilon"] & \\ C \otimes C \arrow[r, "\epsilon \otimes \mathrm{id}"] & k \otimes C \arrow[r, phantom, "\cong"] & C \arrow[r, phantom, "\cong"] & C \otimes k \end{tikzcd} \tag{4.1}$$

A cocommutative coalgebra means that we get a flip called τ which comes from a bilinear balanced map taking

$$\tau : c_1, c_2 \mapsto c_2 \otimes c_1$$

such that

$$\Delta^{\mathrm{op}} := \tau \circ \Delta = \Delta$$

Example 4.1. We now consider the universal property of tensor product of k-algebras. Let us have A, B, C and $f : A \to C$ and $g : B \to C$ such that $[f(A), g(B)] = 0$ in the category of unital binary k algebras then we have the following:

$$\begin{tikzcd} A \arrow[r, "\varphi_1"] \arrow[dr, "f"'] & A \otimes_k B \arrow[d, dashed] & B \arrow[l, "\varphi_2"'] \arrow[dl, "g"] \\ & C & \end{tikzcd}$$

Note that

$$\varphi_1 : a \mapsto a \otimes 1_A \qquad \qquad \varphi_2 : b \mapsto 1_A \otimes b$$

Remark 4.1. If k is unital, saying we have a k bimodule is equivalent to saying there is a left $k \otimes_{\mathbb{Z}} k^{\mathrm{op}}$ module. So if we have this bimodule M, to produce a k-bimodule we require

$$cm := (c \otimes 1)\, m \qquad \qquad mc' := \left(1 \otimes (c')^{\mathrm{op}}\right) m$$

For example this gives us:

$$\left(c \otimes (c')^{\mathrm{op}}\right) m := c\,(mc') = (cm)\, c'$$

For from a bimodule, we get a left module over $k \otimes_{\mathbb{Z}} k^{\mathrm{op}}$. In the reverse we cannot do this. This algebra is sometimes referred to as the enveloping algebra of k.

4.4 Bialgebras

Definition 4.5. A bialgebra A is a k-bimodule paired with $(A, \mu, \eta, \Delta, \epsilon)$

$$A \xrightarrow{\Delta} A \otimes_k A \xrightarrow{\mu} A$$

satisfying the following properties:

1. (A, μ, η) is a unital associative algebra.
2. (A, Δ, ϵ) is a counital coassociative coalgebra.
3. The following commutative diagrams giving compatibility:

$$\begin{tikzcd}
 & & A \arrow[drr, "\Delta"] & & \\
A^{\otimes 2} \arrow[urr, "\mu"] \arrow[dr, "\Delta^{\otimes 2}"'] \arrow[drrr, dashed, "\Delta_{A^{\otimes 2}}"] & & & & A^{\otimes 2} \\
 & A^{\otimes 4} \arrow[rr, "\mathrm{id}\otimes\tau\otimes\mathrm{id}"'] \arrow[urrr, dashed, "\mu_{A^{\otimes 2}}"] & & A^{\otimes 4} \arrow[ur, "\mu^{\otimes 2}"'] &
\end{tikzcd} \tag{4.2}$$

$$\begin{tikzcd}
A \otimes A \arrow[rr, "\mu"] \arrow[dr, "\epsilon\otimes\epsilon"'] & & A \arrow[dl, "\epsilon"] \\
 & k \otimes k \simeq k &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & k \otimes k \simeq k \arrow[dl, "\eta\otimes\eta"'] \arrow[dr, "\eta"] & \\
A \otimes A & & A \arrow[ll, "\Delta"]
\end{tikzcd}$$

$$\begin{tikzcd}
k \arrow[dr, "\eta"] \arrow[dd, "\mathrm{id}"] & \\
 & A \arrow[dl, "\epsilon"] \\
K &
\end{tikzcd}$$

Remark 4.2. Note in eq. (4.2) the map $\Delta_{A^{\otimes 2}}$ is comultiplication of $A^{\otimes 2}$ not $\Delta^{\otimes 2}$. Similarly $\mu_{A^{\otimes 2}}$ is multiplication of $A^{\otimes 2}$, not $\mu^{\otimes 2}$.

Note that if we consider k as a k-algebra over itself[4.1] then our conditions on $\eta : k \to A$ translate to η being a homomorphism of bialgebras. Similarly so for $\epsilon : A \to k$.

Definition 4.6. An augmented algebra is a pairing (A, μ, η, ϵ) where η is an augmentation An augmented coalgebra is a pairing $(A, \Delta, \eta, \epsilon)$ where η is a coaugmentation.

So unital and counital bialgebras, are precisely bialgebras which are simultaneously augmented and coaugmented.

[4.1] Note this can happen in many different ways. In algebraic number theory one often works with k as a k-algebra over itself in multiple different "twisted" ways.

Definition 4.7. A bialgebra is said to be *commutative*, *finitely generated*, *finitely presented*, etc. iff its underlying algebra has this property.

Definition 4.8. Let A be a bialgebra. An inversion (or antipodal map or antipode), is a k-bimodule map $S : A \to A$ such that

1. The following diagram commutes:

$$\begin{tikzcd}
 & A \otimes A \arrow[rr, "S \otimes \mathrm{id}"] & & A \otimes A \arrow[dr, "\mu"] & \\
A \arrow[ur, "\Delta"] \arrow[dr, "\Delta"'] \arrow[rr, "\epsilon"] & & k \arrow[rr, "\eta"] & & A \\
 & A \otimes A \arrow[rr, "\mathrm{id} \otimes S"] & & A \otimes A \arrow[ur, "\mu"'] &
\end{tikzcd}$$

2. For all $a, b \in A$ we have $S(ab) = S(b) S(a)$ and $S(1) = 1$.

Proposition 4.1. *Every bialgebra admits at most one inversion.*

So we can speak of this as *the* antipode.

Definition 4.9. A bialgebra $(H, \Delta, \mu, \epsilon, \eta, S)$ is a *Hopf k-algebra* iff H is associative, coassociative, unital, counital, and S is the antipode.

Warning 4.3. Hopf algebras do not need to be (co)-associative but we will only be interested in this case, so we take this as part of the definition. However for the sake of completeness we offer some discussion of these alternative classifications. It is said that a Quasiassociative Hopf algebra is such that we do not assume associativity of multiplication but we do assume associativity of comultiplication. We then have the natural notion of a quasi-coassociative Hopf algebra, for which we take the multiplication to be associative but do not take the comultiplication to be associative.

We now consider C to be a coaugmented k-coalgebra. Recall this means there is a homomorphism of coalgebras $\eta : k \to C$. Denote $\eta(1_k)$ by 1.[4.2]

Definition 4.10. We say $c \in C$ is primitive iff $\Delta(c) = c \otimes 1 + 1 \otimes c$. We say $c \in C$ is group-like iff $\Delta(c) = c \otimes c$.

We write the group-like elements as $G(C)$ and the primitive elements as $P(C)$.

Example 4.2. $G(k) = k$

[4.2] Note there is no multiplication assumed here, yet we have an "identity."

4.5 Functors

Consider the category $\mathbf{Bialg}_{k,\eta}$ of unital bialgebras. Then there is a functor P given by taking primitive elements which brings $\mathbf{Bialg}_{k,\eta}$ into the category of unital algebras: $\mathbf{Alg}_k$. We also have a functor G, given by taking group-like elements which brings $\mathbf{Bialg}_{k,\eta}$ to the category of unitary binary structures.

If we instead take the category $\mathbf{Bialg}^{\text{ass}}_{k,\eta}$ of associative unital bialgebras, P brings this category to $\mathbf{Lie}_k$, and G brings this category to the category $\mathbf{Mon}$ of monoids. Note that in this case the left adjoint of P is given by $\mathfrak{g} \mapsto U_k\mathfrak{g}$. The proof of this is left as an exercise. We also have that the left adjoint of G is given by $G \mapsto kG$.

$$\begin{tikzcd}
 & \mathbf{Bialg}^{\text{ass}}_{k,\eta} \arrow[dl, "P"] \arrow[dr, "G"] & \\
\mathbf{Lie}_k \arrow[ur, bend left, "U_k\cdot"] & & \mathbf{Mon} \arrow[ul, bend right, "k\cdot"']
\end{tikzcd}$$

We might just take the definition of these two functors giving kG and $U_k\mathfrak{g}$ as left adjoints of the functors G and P respectively, but there are explicit constructions which are often useful. The object $U_k\mathfrak{g}$ is called the universal enveloping algebra, and is given by:

$$U_k\mathfrak{g} = T_k\mathfrak{g}/I \qquad\qquad T_k\mathfrak{g} \coloneqq \bigoplus_{n\geq 0} \mathfrak{g}^{\otimes_k n}$$

where I is the ideal generated by elements of the form:

$$[g_1, g_2]_{T\mathfrak{g}} - [g_1, g_2]_{\mathfrak{g}}$$

note that the first term is in $T^2\mathfrak{g}$ and the second is in $T^1\mathfrak{g}$. In particular, this commutator is defined as:

$$[g_1, g_2]_{T\mathfrak{g}} \coloneqq g_1 \otimes g_2 - g_2 \otimes g_1$$

Notice that if the Lie algebra has trivial bracket, then we get a graded algebra. So the symmetric algebra of k-module V is $U_k(V)$ with zero bracket. Also note that the exterior algebra will be the enveloping algebra of a super Lie-algebra which is abelian, but has only fermionic elements. Note that we have the following diagram:

$$\begin{tikzcd}
\mathbf{Hopf}_k \arrow[r, hook] \arrow[d, "G"] & \mathbf{Bialg}^{\text{ass}}_{k,\eta} \\
\mathbf{Grp} \arrow[r, hook] & \mathbf{Mon}
\end{tikzcd}$$

Let X be any set. Then take $X \mapsto kX$ where kX is the free k-module with basis X. This is a co-commutative, coassociative, and counital k-coalgebra. Recall the basic fact from linear algebra:

Proposition 4.2. *If we have a linear transformation from a vector space with basis X into any vector space, by restricting this map to the basis, we get a function, and any such function can be uniquely extended to a unique transformation.*

Note that in the present situation these aren't just vector spaces, these are vector spaces with comultiplication. In particular, this is the god-given functorial mapping $\Delta : X \to X \times X$. which induces a map:

$$kX \to k\left(X \times X\right) = kX \otimes kX$$

which means in general, $kX^n = kX^{\otimes n}$. So this is actually a tensor category, since it takes the tensor product in the category **Set**, namely Cartesian product, and brings it to the tensor product of k-modules. So kG is counital, because for every set, there is a unique function from this set to the set with a single element. In particular the mapping:

$$X \to X^0 \coloneqq \{\varphi \,|\, \varphi : \emptyset \to X\}$$

4.6 Exercises

Exercise 4.6.1. Formulate the universal property of the tensor product of k-coalgebras.

Exercise 4.6.2. Show that if A is a unital bialgebra, then the set $P\left(A\right)$ of primitive elements is closed under commutator operation $[\cdot, \cdot]$

$$[a, b] = ab - ba$$

Show that that the set $G\left(A\right)$ of group-like elements is closed under multiplication.

Exercise 4.6.3. Let H be a Hopf algebra. Show that $G\left(H\right)$ is a group, even if comultiplication is not associative. [Hint: The antipode allows us to invert every element.]

Exercise 4.6.4. Show that $\mathfrak{g} \mapsto U_k\mathfrak{g}$ is a left adjoint functor to the functor P.

Exercise 4.6.5. Let G be a group. Show that multiplication $G \times G \to G$ equips kG with the structure of a Hopf algebra. Additionally show that the functor from **Grp** to Hopf k-algebras is left adjoint to the group functor $G\left(\cdot\right)$.

Chapter 5

Representation theory of groups

A good reference for this chapter is [4].

5.1 Definitions and examples

We will always assume G is a finite group.

Definition 5.1. A *linear representation* of a group G is a pair (π_V, V) where V is a vector space over a field[5.1] k, and π_V is a group homomorphism:

$$\pi_V : G \to \mathrm{Aut}\,(V)$$

A representation of G is also sometimes called a G-module.

Remark 5.1. Note that $\mathrm{Aut}\,(V) = \mathrm{GL}\,(V)$. For $V \simeq \mathbb{C}^n$ we have $\mathrm{GL}\,(V) \simeq \mathrm{GL}_n\,(\mathbb{C})$ is the group of $n \times n$ complex valued invertible matrices. Note also that

$$\mathrm{SL}_n\,(\mathbb{C}) = \mathrm{GL}_n\,(\mathbb{C})\,/\,\{\det = 1\}$$

Example 5.1. Consider the symmetric group of permutations of n objects: S_n. This will be our standard example of a group. Permutations can simply be viewed as bijective mappings between two copies of these n objects. Then the multiplication for this group is given by composition. We clearly have inverses and an identity. We can represent these maps geometrically by drawing a path from an element of the domain to its image in the codomain. Clearly it is the case that the element of the group does not depend on the nature with which we draw this path. We could, for example, make it cross over or under the other paths. This seems trivial, but will become relevant under the consideration of the next example.

[5.1] For us $k = \mathbb{C}$ will be sufficient.

Figure 5.1: The "slide" Reidemeister move.

Example 5.2. We now consider the braid group, which is a discrete infinite group. Call the configuration space the space of all n-tuples of points

$$C_n = \left\{ (x_1, \cdots, x_n) \mid x_i \in \mathbb{R}^2, x_i \neq x_j \right\}$$

So this is a certain topological space for which we can define the pure braid group $\pi_1(C_n)$. Roughly speaking this is the group consisting of equivalence classes of paths determined by continuous deformations. Then we can take the quotient C_n/S_n where S_n acts by permuting points. Now the Braid group B_n is taken to be

$$B_n \coloneqq \pi_1(C_n/S_n)$$

which consists of the paths in C_n which connect $(x_1, \cdots, x_n)$ to $(x_{\sigma 1}, \cdots, x_{\sigma n})$ for $\sigma \in S_n$. So the difference between the braid group and the symmetric group is simply that in B_n it matters how we braid, but in the symmetric group it matters only how we permute the elements, and not how we got there.

There are multiple ways to choose generators for B_n. We present one of them. We can consider the standard braids consisting only of braids corresponding to the elementary permutations. Changing i with $i+1$, we call this element s_i. So then

$$B_n = \langle s_1, \cdots, s_{n-1} \mid s_i s_j = s_j s_i, i \neq j \pm 1; s_i s_{i\pm 1} s_i = s_{i\pm 1} s_i s_{i\pm 1} \rangle$$

The nontrivial part of this statement isn't that this holds, but that this is sufficient to determine every element of B_n. Note that this relates to what is referred to as the *Reidemeister moves.* The one of interest to us is in fig. 5.1.

As noted before, there is a sense in which B_n contains S_n along with additional elements. We can guess that B_n is somehow an extension of S_n. In particular, we can write:

$$S_n = B_n / \left\langle s_i^2 = 1 \right\rangle$$

Example 5.3. Take $\mathrm{SL}_n(\mathbb{F}_p)$ for a finite field $\mathbb{F}_p$.

We now present some actual examples of representations.

Example 5.4. Take the group $\mathbb{C}^n$. This has a standard basis $e_1, \cdots, e_n$. So take $\sigma e_i = e_{\sigma i}$ for $\sigma \in S_n$. Then a nonzero invariant vector is given by the sum of the basis vectors:

$$\sigma(e_1 + \cdots + e_n) = e_1 + \cdots + e_n$$

So we have this action of S_n on $\mathbb{C}^n$, with invariant subspace given by $L = \mathbb{C}\left(e_1 + \cdots + e_n\right)$. Now taking this quotient, we again have the action

$$S_n : \mathbb{C}^n / L \circlearrowright$$

on this $n-1$ dimensional space. Also note that we can split $\mathbb{C}^n \simeq L \oplus \mathbb{C}^n/L$. So now we have three representations:

$$\begin{aligned} \pi &: S_n \to \operatorname{Aut}\left(\mathbb{C}^n\right) \\ \pi_1 &: S_n \to L \\ \pi_2 &: S_n \to \mathbb{C}^n/L \end{aligned}$$

This is an example of a sub-representation and a quotient representation.

Definition 5.2. Let $\left(\pi_V, V\right), \left(\pi_W, W\right)$ be G-modules such that

$$\varphi : W \hookrightarrow V$$

so if φ commutes with the G-action:

$$\varphi \circ \pi_W\left(g\right) = \pi_V\left(g\right) \circ \varphi$$

then W is called a subrepresentation of V.

Example 5.5. Clearly the example before fits the above definition for $V = \mathbb{C}^n$, $W = L$.

Proposition 5.1. *If $W \subset V$ is a subrepresentation, then G acts naturally on the quotient space V/W, and $\left(\pi_{V/W}, V/W\right)$ is called a* quotient representation.

Definition 5.3. It is said that V *splits* into $V_1 \oplus V_2$ iff both V_1 and V_2 are subrepresentations of V, and of course the sum is isomorphic to V as vector spaces.

Proposition 5.2. *Note that if V splits as $V = V_1 \oplus V_2$ we have that $V/V_1 \simeq V_2$ and $V/V_2 \simeq V_1$.*

Definition 5.4. Let $\left(\pi_V, W\right)$ and $\left(\pi_W, W\right)$ be G-modules. Then a homomorphism of vector spaces $f : V \to W$ is a homomorphism of G-modules iff $f \circ \pi_V\left(g\right) = \pi_W\left(g\right) \circ f$.

Definition 5.5. Two representations are isomorphic:

$$\left(\pi_W, W\right) \simeq \left(\pi_V, V\right)$$

iff there exists a G-module homomorphism $f : V \to W$ which is a linear isomorphism.

Warning 5.1. This is more rigid than an isomorphism as vector spaces.

Definition 5.6. A representation $\left(\pi_V, V\right)$ is irreducible iff it has no nonzero subrepresentations.

Example 5.6. We have seen that $S_n : \mathbb{C}^n \circlearrowright$ is reducible because of the subspace L from the previous example. However, $S_n : L \circlearrowright$ is irreducible.

Exercise 5.1.1. Prove that $S_n : \mathbb{C}^n/L \circlearrowright$ is irreducible.

5.2 Operations on representations

Suppose we have two representations (π_V, V) and (π_W, W) of the same group. We want to consider some operations on these two representations.

Definition 5.7. The tensor product of these two representations is a linear representation $(\pi_{V\otimes W}, V \otimes W)$ such that

$$(\pi_V \otimes \pi_W)(g)(x \otimes y) \coloneqq \pi_V(g)\, x \otimes \pi_W(g)\, y$$

Definition 5.8. The direct sum of these representations is given by:

$$\pi_{V\oplus V}(g) \coloneqq \pi_V(g) \oplus \pi_W(g)$$

acting on $V \oplus W$.

Definition 5.9. The dual of any G-module (π_V, V) is given by:

$$(\pi, V)^* \coloneqq (\pi_{V^\vee}, V^\vee)$$

Recall

$$V^\vee = \operatorname{Hom}(V, \mathbb{C})$$

then take

$$\langle \pi_{V^\vee}(g)\, l, x\rangle \coloneqq \left\langle l, \pi_V\left(g^{-1}x\right)\right\rangle$$

for $l \in V^\vee$ and $x \in V$. Then the dual linear map is given by:

$$\pi_{V^\vee}(g) = \pi\left(g^{-1}\right)^*$$

We also note that there is always the concept of a trivial representation of G. This is just taking $\pi_V(g) \coloneqq 1$ for all $g \in G$, so every element of the group acts as the trivial automorphism on V.

5.3 Categories of representations

Definition 5.10. We write G-**Mod** as the category of finite dimensional G-modules. In particular, the objects are given by pairs (π_V, V) and the morphisms are given by:

$$\operatorname{Mor}((\pi_V, V), (\pi_W, W)) \coloneqq \{f_i : V \to W \mid f\pi_V(g) = \pi_W(g)\, f, \forall g \in G\}$$

Proposition 5.3. *G-**Mod** is an Abelian $\mathbb{C}$-linear category.*

Proposition 5.4. *If $f : V \to W$ is a morphism of modules, then $\ker(f) \subset V$ is a subrepresentation of V, and $\operatorname{im}(f) \subset W$ is a subrepresentation of w.*

Corollary 5.1. *If $V \subset W$ is a subrepresentation of W, then W/V is also naturally a representation of G.*

Corollary 5.2. *If $V \subset W$ is a subrepresentation, then $W \simeq V \oplus W/V$ as a linear space, but not necessarily as a module.*

This means $\pi_w(g)$ has the following form:

$$\pi_W(g) = \begin{pmatrix} \pi_{W/V}(g) & * \\ 0 & \pi_V(g) \end{pmatrix}$$

if it splits as a G-module then $* = 0$ so this matrix is diagonal.

In general:

$$0 \to W \hookrightarrow W \to W/V \to 0$$

is an exact sequence of G-modules and this is all we can say. This is what it means for G-**Mod** to be an abelian category.

So we have seen that G-**Mod** is an abelian category. But what if we replace G by some other algebraic set? Say an associative algebra $A/\mathbb{C}$? Then A-**Mod** consists of finite dimensional A-modules. But now notice that A-**Mod** is also an abelian category, since we never actually used the particular characteristic of a group in the above when showing G-**Mod** is an abelian group. So why is the category G-**Mod** of interest to us at all? Where is the importance of the group structure? There should be some more restrictive sort of category which contains G-**Mod** and not A-**Mod**. to see what this might be, we consider the constructions we have made which do rely on on the group structure:

1. Recall that from a representation (π_V, V) we constructed the dual representation:
$$(\pi_V, V)^* = (\pi_{V^\vee}, V^\vee)$$
and then we used the group structure to define:
$$\pi_{V^V}(g) \coloneqq \left(\pi_V\left(g^{-1}\right)\right)^*$$
2. We used the existence of the identity to show the existence of a trivial representation.
3. Recall we defined the tensor product of two representations. There is no such notion for a generic associative algebra.
4. We established a natural isomorphism between $(\pi_V, V) \otimes (\pi_W, W)$ and $(\pi_W, W) \otimes (\pi_V, V)$ given by
$$c_{VW}(x \otimes y) = y \otimes x$$

Theorem 5.1. *G-**Mod** is a(n)*

1. *abelian $\mathbb{C}$-linear category*

2. *monoidal category with* $\otimes$

$$\begin{tikzcd}C \times C \times C \arrow[r, "\otimes \times \mathrm{id}"] \arrow[d, "\mathrm{id} \times \otimes"] & C \times C \arrow[d, "\otimes"] \\ C \times C \arrow[r, "\otimes"] & C\end{tikzcd}$$

Note than in general monoidal categories this won't be commutative. And object $I \in \mathrm{Obj}\,(G\text{-}\mathbf{Mod})$ *such that*

$$I \otimes V \simeq V \simeq V \otimes I$$

3. *rigid monoidal category: For any* V*, there exists a right dual* $V^{\vee}$ *and left dual* ${}^{\vee}V$ *paired with evaluation and coevaluation maps*

$$e_V : V^{\vee} \otimes V \to I \qquad\qquad i_V : I \to V \otimes V^{V}$$

and such that:

$$\left({}^{\vee}V\right)^{\vee} = {}^{\vee}\left(V^{\vee}\right)$$

4. *braided category: on any monoidal category a braided structure is an isomorphism:*

$$c_{VW} : V \otimes W \xrightarrow{\sim} W \otimes V$$

$$\begin{tikzcd}C \otimes C \arrow[r, bend left, "\otimes"] \arrow[r, bend right, "\otimes^{op}"'] \arrow[r, phantom, "\Uparrow c"] & C\end{tikzcd}$$

5.4 G-colored tangles

We now present a graphical way to think about G-modules. We first introduce the category $\mathcal{T}\,(G)$ of G-colored tangles, then we introduce a functor from this category to the category G-**Mod**.

Define the objects of this category to be:

$$\mathrm{Obj}\,(\mathcal{T}\,(G)) \coloneqq \{(\epsilon_1, V_1)\,, \cdots, (\epsilon_n, V_n) \mid \epsilon_i = \pm 1, V_i \in G\text{-}\mathbf{Mod}\}$$

and the morphisms to be:

$$\mathrm{Mor}\,((\epsilon, V)\,, (\sigma, W)) = \{G\text{-colored tangles }\}$$

Example 5.7. A pictorial example of an object in $\mathcal{T}\,(G)$ can be found in fig. 5.2.

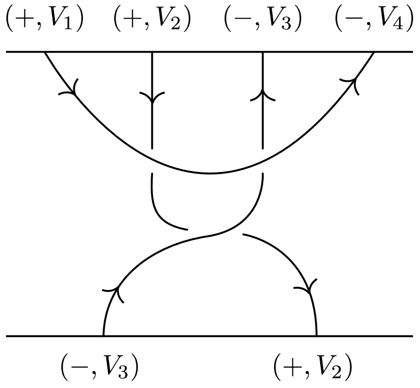

Figure 5.2: Example of a G-colored tangle.

We get a monoidal structure on $\mathcal{T}(G)$ from:

$$(\epsilon, V) \otimes (\sigma, W) = ((\epsilon, V), (\sigma, W))$$

we get a dual construction from:

$$^\vee((\epsilon_1, V_1), \cdots, (\epsilon_n, V_n)) = ((-\epsilon_n, V_n), \cdots, (-\epsilon_1, V_1))$$

evaluation map from:

$$(\epsilon, V)^V \otimes (\epsilon, V) \to \mathrm{I}$$

and a braiding:

$$c_{V,W} : V \otimes W \to W \otimes V$$

This can be visualized in fig. 5.3

So we have seen this category $\mathcal{T}(G)$ shares these special properties with G-**Mod**. This inspires us to construct a covariant functor $F : \mathcal{T}(G) \to G$-**Mod**. First we define F on objects:

$$F((\epsilon_1, V_1), \cdots, (\epsilon_n, V_n)) = V_1^{\epsilon_1} \otimes \cdots \otimes V_n^{\epsilon_n}$$

where $V^+ = V$ and $V^- = V^\vee$. Then we want to see the effect of the functor on morphisms. We first define F on some simple morphisms in $\mathcal{T}(G)$. For a single strand running from V to itself we define F to take this to id_V viewed as a morphism in G-**Mod**. For a cup strand $(+, V)$ to $(-, V)$, we define F to bring this to the map $i_V : \mathbb{C} \to V \otimes V^\vee$. Similarly, we take the cap from $(-, V)$ to $(+, V)$ under F to the map $e_V : V^\vee \otimes V \to \mathrm{I}$. Then two paths crossing between nodes V and W are mapped to c_{VW}. In addition to this we insist that:

$$F(t_1 \circ t_2) = F(t_1) F(t_2) \qquad F(t_1 \otimes t_2) = F(t_1) \otimes F(t_2)$$

for any two tangles t_2,t_2. This allows us to build any possible tangle, and we therefore have a well defined functor. In fact even more is true:

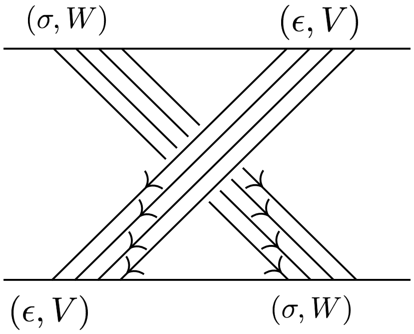

Figure 5.3: Pictorial representation of the braided structure of the category $\mathcal{T}(G)$.

Theorem 5.2. *There exists a unique functor F as constructed above.*

Now suppose we have a picture

$$F(t) : V_1^{\epsilon_1} \otimes \cdots \otimes V_n^{\epsilon_n} \to W_!^{\sigma_1} \otimes \cdots W_n^{\sigma_n}$$

for every tangle t, this is a G-linear map. Then we might wonder if the following:

$$\mathrm{Hom}\left(V_1^{\epsilon_1} \otimes \cdots \otimes V_n^{\epsilon_n}, W_1^{\sigma_1} \otimes \cdots \otimes W_k^{\sigma_k}\right)$$

is generated by $F(t)$.

Let's consider a particular case: $\mathbb{C}^n \otimes \cdots \otimes \mathbb{C}^n = (\mathbb{C}^n)^{\otimes N}$. Then the group GL_n acts diagonally:

$$g(v_1 \otimes \cdots v_n) = gv_1 \otimes \cdots \otimes gv_n$$

and S_n acts by permutations. Then we have the following:

Theorem 5.3. *The centralizer*[5.2] *$Z(\mathrm{GL}_n)$ in $(\mathbb{C}^n)^{\otimes N}$ is isomorphic to the group algebra $\mathbb{C}[S_n]$.*

Corollary 5.3. *This action $\mathrm{GL}_n \times S_n$ acts on $(\mathbb{C}^n)^{\otimes N}$ multiplicity free.*

5.5 Morita equivalence

Theorem 5.4 (Morita)**.** *Every additive equivalence of categories of unitary modules, over units k-algebras A, B is provided by a Morita context.*

So in this context, we have the following theorem:

Theorem 5.5. *If Γk does not divide $|G|$, then kG is a product of matrix algebras Morita equivalent to $k \times \cdots \times k$.*

[5.2] Note that here, these are just all of the linear maps commuting with GL_n

Chapter 6

Solvable groups and extensions

The main goal of this chapter is to prove the Schur-Zassenhaus theorem. This can be formulated a few different ways; we will prove a few of them. First we review the notion of an extension and consider some preliminary group cohomology. We use these tools to prove a simplified version of the Schur-Zassenhaus theorem. This simplified form will also act as a lemma for proving the stronger forms of the theorem.

6.1 Group extensions

Definition 6.1. A composable pair of group homomorphisms π and ι:

$$\begin{tikzcd} \mathcal{E}:\ G & H \arrow[l, two heads, "\pi"] & K \arrow[l, tail, "\iota"] \end{tikzcd}$$

is said to be an extension (of G by K) iff $\ker \pi = \iota(K)$ if π is an epimorphism and ι is a monomorphism.

Definition 6.2. We say that an extension $\mathcal{E}$ splits, or is a split extension iff there exists a right inverse $\sigma : G \to H$ to π. That is, $\pi \circ \sigma = \mathrm{id}_G$. In this case, such a right inverse is called a *splitting* of $\mathcal{E}$. We write $\operatorname{Split}\mathcal{E}$ for the set of splittings of the extension $\mathcal{E}$.

Proposition 6.1. $\operatorname{Split}\mathcal{E}$ *is nonempty iff* $\mathcal{E}$ *is split.*

For any two splittings σ and σ', $\sigma' = \chi\sigma$ where $\chi : G \to K$ is a map such that

$$\chi(g_1 g_2) = \sigma'(g_1)\,\sigma'(g_2)\,\sigma(g_2)^{-1}\,\sigma(g_1)^{-1}$$

Now of course we have

$$\chi(g_1)\,\chi(g_2) = \sigma'(g_1)\,\sigma(g_1)^{-1}\,\sigma'(g_2)\,\sigma(g_2)^{-1}$$

so we can see how far χ is from being a homomorphism by calculating:

$$\begin{aligned}\chi\left(g_1\right)\chi\left(g_2\right)\chi\left(g_1g_2\right)^{-1} &= \sigma'\left(g_1\right)\sigma\left(g_1\right)^{-1}\sigma'\left(g_2\right)\sigma\left(g_2\right)^{-1} \\ &\qquad \left(\sigma'\left(g_1\right)\sigma'\left(g_2\right)\sigma\left(g_2\right)^{-1}\sigma\left(g_1\right)^{-1}\right)^{-1} \\ &= \sigma'\left(g_1\right)\sigma\left(g_1\right)^{-1}\sigma'\left(g_2\right)\sigma\left(g_2\right)^{-1} \\ &\qquad \sigma\left(g_1\right)\sigma\left(g_2\right)\sigma'\left(g_2\right)^{-1}\sigma'\left(g_1\right)^{-1}\end{aligned}$$

Exercise 6.1.1. Determine

$$\chi\left(g_1\right)\chi\left(g_2\right)\chi\left(g_1g_2\right)^{-1}$$

in the case where K is abelian.

6.2 Curvature

Our main goal is to describe, up to restricted isomorphism, all extensions of a group G by an abelian group K. This is a very difficult task, but by doing this, we will be able to prove many important and deep theorems.

Given a general extension, it is not necessarily split. But we know every surjective map as viewed in **Set** has a splitting. That is, consider a map $s : G \to H$ which is just a function such that $\pi \circ s = \mathrm{id}_G$. So s is an inverse of π in **Set**. This is what we we will call a section, or a set theoretic splitting.

Warning 6.1. A set theoretic splitting is not necessarily a group homomorphism. This is the difference between a proper split extension and an extension with a chosen section.

Definition 6.3. For any function between groups $s : G \to H$, let ρ_s be a function of two variables $\rho_s : G, G \to K$ defined by

$$\rho_s\left(g_1, g_2\right) = s\left(g_1\right)s\left(g_2\right)s\left(g_1g_2\right)^{-1}$$

Equivalently,

$$s\left(g_1\right)s\left(g_2\right) = \rho_s\left(g_1, g_2\right)s\left(g_1g_2\right)$$

This is called the left curvature of s.

Example 6.1. We offer a silly example of curvature. Take either of the extensions:

$$\begin{tikzcd}\mathbb{Z}/10\mathbb{Z} & \mathbb{Z}/100 \arrow[l, two heads] & \mathbb{Z}/10 \arrow[l, two heads, "\times 10"']\end{tikzcd}$$

$$\begin{tikzcd}\mathbb{Z}/10\mathbb{Z} & \mathbb{Z} \arrow[l, two heads] & \mathbb{Z} \arrow[l, two heads, "\times 10"']\end{tikzcd}$$

then the following definition for ρ trivially satisfies the definition:

$$\rho\left(i, j\right) \coloneqq \begin{cases}1 & i + j \geq 10 \\ 0 & i + j < 10\end{cases}$$

So this is the process of “carrying the one” from elementary school addition.

In our case, the condition that $\pi \circ s = \mathrm{id}_G$ implies that the curvature is a function $\rho_s : G, G \to K$ since s is a right inverse. In any case, we can write the following:

$$\begin{aligned} s(g_1)\, s(g_2 g_3) &= \rho(g_1, g_2 g_3)\, s(g_1 g_2 g_3) \\ s(g_1 g_2)\, s(g_3) &= \rho(g_1 g_2, g_3)\, s(g_1 g_2 g_3) \end{aligned}$$

Now we can rewrite the second expression as follows:

$$\begin{aligned} \rho(g_1, g_2)\, s(g_1 g_2)\, s(g_3) &= \rho(g_1, g_2)\, \rho(g_1 g_2, g_3)\, s(g_1 g_2 g_3) \\ &= s(g_1)\, s(g_2)\, s(g_3) \\ &= s(g_1)\, \rho(g_2, g_3)\, s(g_2 g_3) \\ &= {}^{s(g_1)}\rho(g_2, g_3)\, s(g_1)\, s(g_2 g_3) \end{aligned}$$

so substituting the first expression into this gives us:

$$^{s(g_1)}\rho(g_2, g_3)\, \rho(g_1, g_2 g_3)\, s(g_1 g_2 g_3) = \rho(g_1, g_2)\, \rho(g_1 g_2, g_3)\, s(g_1 g_3 g_3)$$

which gives us the 2-cocycle[6.1] identity:

$$\boxed{^{s(g_1)}\rho(g_2, g_3)\, \rho(g_1, g_2 g_3) = \rho(g_1, g_2)\, \rho(g_1 g_2, g_3)}$$

This is also written:

$$\boxed{\delta\rho = {}^{s(g_1)}\rho(g_2, g_3)\, \rho(g_1, g_2 g_3)\, \rho(g_1 g_2, g_3)^{-1}\, \rho(g_1, g_2)^{-1} = 1}$$

which is called the non-abelian co-boundary of ρ. But there is a problem here, because this still depends on s. That is, $\delta\rho$ is a function of three arguments, and is a constant function.

Note that we can write this in the additive form as well.

$$\boxed{1 = g_1\rho(g_2, g_3) - \rho(g_1 g_2, g_3) + \rho(g_1, g_2 g_3) - \rho(g_1, g_2)} \tag{6.1}$$

Remark 6.1. We are implicitly treating K as some sort of "bi-group" in the sense that we are equipping it with a certain group-theoretic action on the left and on the right. We know we have a left action of H on K in a canonical way, but we really want a left action of G on K. The problem is, that we can't necessarily do this in a canonical way since we need to choose a section s. We will see in the next proposition, that if K is abelian, which is the case we will be primarily interested in, we actually do have such a canonical action of G on K. In any case, we equip K with a left action of conjugation by elements of H, and a left action given by the trivial action of elements of G. In the last term in (6.1) we really wanted an action of g_3 on the right as before. In fact we do have this, but since right action is trivial here, this can be omitted from the notation.

[6.1] Recall a cocycle is a closed cochain.

Proposition 6.2. *If K is abelian, then for every extension*

$$\begin{tikzcd} \mathcal{E}:\ G & H \arrow[l, two heads, "\pi"'] & K \arrow[l, tail, "\iota"'] \end{tikzcd}$$

G acts canonically on K as follows:

$$^{g}K := {}^{\tilde{g}}K$$

where $\tilde{g} \in H$ such that $\pi\left(\tilde{g}\right) = g$.

Note that if $\tilde{g}'$ is another element such that $\pi\left(\tilde{g}'\right) = g$, then $\tilde{g}' = k'\tilde{g}$ for some $k' \in K$. But k' acts trivially on K, since it is Abelian. Note that picking a splitting s is just doing this lifting process for all $g \in G$. This is effectively the same as this whole transversal business. In particular, the image under any set-theoretic section s is precisely a transversal of the G-set of cosets of K in H. In any case, this is incredibly important, because this means when K is abelian, $\delta\rho$ from before doesn't actually depend on s.

In other words we have given the group K the structure of a G-module. That is, this provides a homomorphism $G \to \operatorname{Aut} K$ which sends g to the conjugation by any element $g' \in H$ which maps to g under π.

So this says, that $\delta\rho$ is the coboundary of the 2-cocycle ρ of G with coefficients in K where K is viewed as a representation of G. That is, if K is abelian, for every s, we write

$$\rho_s \in Z^2\left(G, K\right) \qquad\qquad \delta\rho_s \in B^2\left(G, K\right)$$

where K is a $G\mathbb{Z}$ module (or equivalently a $\mathbb{Z}G$ module).

6.3 General cohomological theory

Let k be commutative unital ground ring and V be a k-module.[6.2] The standard cochain complex of a group with coefficients in a representation V is given by:

$$C^n\left(G; V\right) := \left\{ \underbrace{G, \cdots, G}_{n} \to V \right\} \simeq \operatorname{Hom}_{k\text{-}\mathbf{Mod}}\left(kG^{\otimes_k n}, V\right)$$

Note this is trivially a k-module. We now construct what are called coboundary maps. These are k-linear maps:

$$C^n\left(G; V\right) \xrightarrow{\delta} C^{n+1}\left(G; V\right)$$

$$f \longmapsto \delta f$$

So f is a function of n variables and δf is a function $n+1$ variables, but we have to build it from f. So suppose we have $g_1, \cdots, g_{n+1}$, then we will use all

---

[6.2] Our $\mathbb{Z}$-module K from before has become V here where our ground right was implicitly just $\mathbb{Z}$.

of the potential contractions to a list of length n to construct this δ function. We can remove the first element, the last element, or take any two neighbours and replace them with their product. Now we apply the function f to the new list of objects of length n to get an element in the target. But notice that if we remove the first or last elements completely, these do not affect the behavior of this term in our definition for δf. As such, we take this image in the target and twist it by this element. So if we have removed the first one, we twist by a left action, and if we remove the last one, we twist by the right action. So the target of these functions should be a sort of "G-bimodule" where the right action is trivial.

Remark 6.2. Recall the category kG-**Mod** is actually isomorphic to the category of k-linear representations of G. That is, homomorphisms:

$$G \to \mathrm{GL}\left(V\right) := \mathrm{Aut}_{k\text{-}\mathbf{Mod}} V$$

So in this sense, bi-actions of groups are the same as bimodules.

Consider a trivial action of G and some element:

$$\gamma = \sum_{g \in G} c_g g$$

where $c_g \neq 0$ for finitely many $g \in G$. Then γ acts as:

$$\gamma v = \sum c_g g v = \left(\sum c_g\right) v = \int v$$

So there is a homomorphism from kG to k, which is precisely given by:

$$\gamma \mapsto \int \gamma = \sum c_g$$

Notice this is not only a homomorphism of algebras, but in fact a homomorphism of Hopf algebras, since k is the image of the trivial group, and from every group there exists a homomorphism to the trivial group. This is what is called augmentation, and the kernel is denoted by $I_k G$ or $J_k G$. This ideal is called an augmentation ideal. Note that this is a nonunital algebra. This is a standard fact of homological algebra:

Proposition 6.3. *The bicohomology of the augmentation ideal $I_k G$ is precisely the group cohomology of G.*

Returning to our list of $n-1$ elements, we are producing a function:

$$\begin{aligned} g_1, \cdots, g_{n+1} \longmapsto\; & g_1 f\left(g_2, \cdots, g_{n+1}\right) \\ & + \sum_{i=1}^{n} \left(-1\right)^i f\left(g_1, \cdots, g_i g_{i+1}, \cdots, g_{n+1}\right) \\ & + \left(-1\right)^{n+1} f\left(g_1, \cdots, g_n\right) \end{aligned} \tag{6.2}$$

Remark 6.3. Note that in (6.2), as noted above, we have a right action of g_{n+1}, but since the action is trivial, we omit this from the expression.

Now with this understanding of the coboundary function δ, we can define the nth cohomology to be:

$$H^n(G;V) = Z^n(G;V)/B^n(G;V)$$

where the

$$Z^n(G;V) \coloneqq \ker \delta^n \qquad\qquad B^n(G;V) \coloneqq \operatorname{im} \delta^{n-1}$$

are called the group/module of n-cocycles of G with coefficients in V and the group/module of n-coboundaries.

6.4 Chain homotopy

So we have seen that given a set theoretic section for π, we obtain a 2-cocycle of G with coefficients in a $\mathbb{Z}$-module K.

Definition 6.4. Given two cochain-complexes (C^*, δ_C^*) and (D^*, δ_D^*) consider map h from C to D of degree -1 and morphisms $\varphi, \psi : C \to D$ as in the following diagram:

$$\begin{tikzcd}
C^* \arrow[loop right, "\delta_C"] \arrow[d, shift right, "\varphi"'] \arrow[d, shift left, "\psi"] \arrow[d, bend right=60, "h"'] \\
D^* \arrow[loop right, "\delta_D"]
\end{tikzcd}$$

Note that these are really the collections $\varphi = (\varphi_n)$ where each $\varphi_n : C^n \to D^n$ and $\psi = (\psi_n)$ where each $\psi_n : C^n \to D^n$. So φ, ψ preserve degree, h is of degree -1, and the coboundaries δ_C and δ_D are of degree $+1$. Then h is a *homotopy* from φ to ψ iff the following supercommutator condition is satisfied:

$$\psi - \varphi = [h, \delta] = h\delta_C + \delta_D h$$

This is often denoted $\varphi \sim_h \psi$.

The map φ is said to be *null homotopic* if ψ is 0 and vice versa. So this means φ is representable as the supercommutator of some graded map of degree -1 with the corresponding coboundaries. In this case h is also called a *contracting homotopy.*

If ψ is the identity on any given complex, it is then said that the complex is *contractible.*

Proposition 6.4. *Let G be a finite group. Multiplication by the order $|G|$ is chain-homotopic to* 0*, equivalently it is null-homotopic. That is we have the diagram*

$$\begin{tikzcd}
C^*(G;V) \arrow[loop left, "\delta"] \arrow[loop right, "h"]
\end{tikzcd}$$

and the expression:

$$[h, \delta] = |G| \operatorname{id}_{C^*(G;V)}$$

Explicitly the homotopy is given by:

$$(h\alpha)(g_1, \cdots, g_{n-1}) = (-1)^{n-1} \sum_{x \in G} \alpha(g_1, \cdots, g_{n-1}, x)$$

Remark 6.4. The intuition behind this form of the homotopy is that we are fixing this argument to be x for every $x \in G$ and computing some sort of average.

Corollary 6.1. *If k is a field or characteristic* 0*, then cohomology is identically* 0*.*

Proof. So now suppose k is a field of characteristic 0. Then these modules are k-vector spaces, so there is no torsion. So by proposition 6.4, the cohomology must be 0. ☐

The following comes directly from the definitions:

Proposition 6.5. *If φ and ψ are homotopic, then $\varphi - \psi$ is null homotopic.*

Now we have the following fundamental fact:

Proposition 6.6. *If φ and ψ are homotopic, then they induce the same map on the cohomology group.*

Now suppose $\gamma \in Z^n C$ is an n-cocycle in C. If ψ is null homotopic, then

$$\psi\gamma = h\delta\gamma + \delta(h\gamma) = \delta(h\gamma)$$

so we have that $\psi\gamma$ is explicitly represented as the coboundary of some chain, which is manufactured using the contracting homotopy h. This is the standard use of a contracting homotopy h. The presence of a contracting homotopy is very powerful. The following is essential in homological algebra:

Proposition 6.7. *If we apply an additive functor to a (co)chain complex, it will take any contracting homotopy to a contracting homotopy.*

Proof. This essentially follows from the fact that all of the characterizing aspects of a contracting homotopy are additive, and are therefore obviously preserved by any additive functor. ☐

Definition 6.5. A cyclic complex is a complex with zero (co)homology.

Cyclic complexes are very rarely preserved by functors. In fact, functors which preserve cyclic complexes are called exact functors.

Example 6.2. Suppose we have the category of k-representations of G. Then take two functors: invariants and coinvariants.

$$\begin{tikzcd} V \arrow[r, mapsto] & V^G \end{tikzcd}$$

$$\begin{tikzcd} kG\text{-}\mathbf{Mod} \arrow[r, shift left, "\text{inv}"] \arrow[r, shift right, "\text{coinv}"'] & k\text{-}\mathbf{Mod} \end{tikzcd}$$

$$\begin{tikzcd} V \arrow[r, mapsto] & V_G \end{tikzcd}$$

Recall that V^G is the largest set of V such that G acts trivially. That is it is the largest trivial subrepresentation of G. Of course V_G is the largest trivial quotient representation.

Then we have that inv is left exact but not right exact, and coinv is right exact but not left exact. For each additive functor, you have left derived and right derived functors, and we can apply them to every functor.

Warning 6.2. It is a common misunderstanding that right derived functors only exist for left exact functors, and left derived functors only exist for right exact functors. This is not true. It is simply the case that right derived functors for left exact functors behave nicely in the sense that they are balanced etc.

As it turns out, cohomology groups such as the ones we are calculating, are precisely the right derived functors of the invariants functor.

We saw essentially this same picture with G-sets, only this category was semi-simple. This category of representations of is not necessarily semi-simple, so we don't get the same results. For certain particular cases, however, there will be convenient results.

Example 6.3. Let G be a finite group such that $(|G|, \operatorname{char} k) = 1$, that is $|G|$ is invertible in k. Then the category kG-**Mod** modules is semi-simple, and the functor inv is exact. This is because multiplication by $|G|$ is invertible in kG.

Example 6.4. Let G be a finite group. If $\operatorname{char} k = p$ where p divides $|G|$ then this is significantly different. This leads into a profoundly beautiful theory. For more on this see the third part of Serre's representation theory of finite groups [5]. This is fundamental in homotopy theory, algebraic K-theory, and algebraic number theory.

6.5 Exercises

Exercise 6.5.1. Develop the corresponding 2-cocycle identity for the right curvature $\rho^r(g_1, g_2)$ which has the property:

$$s(g_1, g_2)\,\rho^r(g_1, g_2) = s(g_1)\,s(g_2)$$

and for the middle curvature which has the property:

$$s(g_1)^{-1}\,s(g_1 g_2)\,s(g_2)^{-1} =: \rho^m(g_1, g_2)$$

Exercise 6.5.2. Show that $\delta \circ \delta = 0$.

Exercise 6.5.3. Prove proposition 6.4.

6.6 Isomorphism classes of extensions

So what if we have two splittings s and s':

$$\begin{tikzcd}
G \arrow[r, bend left, tail, "s"] \arrow[r, bend right, tail, "s'"'] & H \arrow[l, two heads] & K \arrow[l, tail]
\end{tikzcd}$$

for abelian K. Of course this means there is a certain factor $\tau(g)$ such that $s'(g) = \tau(g)\, s(g)$. So $\tau : G \to K$. Now for both s and s', we get that their curvatures are both cocycles: $\rho_{s'}, \rho_s \in Z^n(G; K)$. Then it turns out to be the case that:

$$\rho_{s'} \rho_s^{-1} = \delta\tau$$

Conversely, we can take any $\tau : G \to K$ and from some splitting s, this will of course give us a new splitting $s' := \tau s$. All set theoretic splittings arise this way.

So starting from an extension, we get a cocycle by choosing a splitting. But if we were to choose a different splitting, then we would end up with a different cocycle. However, the cohomology class of this cocycle is canonically defined by this extension. This means that a certain isomorphism class of extensions are the same as connected components of this category. So the connected components of this category form a group. This is the second cohomology group of G with coefficients in K. Where we mean two extensions H and H' of G by K are isomorphic iff

$$\begin{tikzcd}
G & H \arrow[l, two heads] \arrow[d, "\sim"] & K \arrow[l, tail] \\
G & H' \arrow[l, two heads] & K \arrow[l, tail]
\end{tikzcd}$$

So now we have addition on these isomorphism classes. In particular, we start with the exact sequence $G \times G \twoheadleftarrow H \times H' \hookleftarrow K \times K$. Then we take a pullback, followed by a pushout to get:

$$\begin{tikzcd}
& & G \times G & H \times H' \arrow[l, two heads] & K \times K \arrow[l, tail] \\
& G \arrow[ur, tail, "\Delta"] & & & \\
G \arrow[ur, equal] & & \tilde{H} \arrow[ul, dashed, two heads] \arrow[ur, dashed, tail, bend right] \arrow[dl, dashed, two heads] & & \\
& H'' \arrow[ul, two heads] & & K \times K \arrow[ul, tail] \arrow[dl, two heads, "+"] & \\
& & K \arrow[ul, tail] & &
\end{tikzcd}$$

We have implicitly used the fact that the pullback of a monomorphism is a monomorphism. This is true in every category. We have also used the fact that a pullback of an epimorphism is an epimorphism. This is not true in every category, but it is here. So starting with two arbitrary extensions of G by K, we end up with a new extension H'' of G by K.

So each of these initial extensions have a corresponding second cohomology class. So when we pull in the quotient, and push in the kernel we are sort of adding these classes to get a new cohomology class.

So by this argument, we can form a sum of any two curvature cocycles to form a curvature cocycle. But now we can ask the general question of whether every cocycle, or at least every cohomology class, is produced this way. As it turns out, every cohomology class, produces an extension, for which it is the curvature cocycle. In particular, this is:

$$G \twoheadleftarrow K \rtimes_\rho G \hookleftarrow K$$

where of course G acts on K and ρ is of course a 2-cocycle of G with coefficients in K, being a representation of G. Then the definition of this is very simple. Just take $K \times G$ and then define twisted multiplication:

$$(k_1, g_1) \cdot_\rho (k_2, g_2) := \left(k_1 {}^{g_1}k_2 \rho\left(g_1, g_2\right), g_1 g_2\right)$$

Now we can write this for any function of two variables ρ.

Exercise 6.6.1. Show this is associative iff ρ is a 2-cocycle of G with coefficients in a G-module K.

Note that if $\rho = 1$, this is simply the semidirect product. This $\rho = 1$ represents the trivial element in this group of isomorphism classes of extensions. So the general procedure is to start with an extension and consider the curvature. Then look at the corresponding cocycle, and then we might be able to find that for whatever reason, this is actually a coboundary. If this is the case, then it is the coboundary of some function of one variable. Then we can multiply this on the left to modify the original choice of splitting, and now for this new splitting, we can show that the curvature is simply the identity. This is of course the whole meaning of a coboundary. This is often used in the sense that we might start with an extension, consider some splitting, and show this must be a coboundary which means this is a split extension.

6.7 Abelian case of Schur-Zassenhaus theorem

As mentioned in the introduction to this chapter, the main goal, and one of the highlights of the course, is proving the Schur-Zassenhaus theorem in full generality. For now prove a simplified case using the tools we have since developed:

Theorem 6.1 (Schur-Zassenhaus(abelian))**.** *Consider an extension:*

$$\begin{tikzcd}\mathcal{E}: G & H \arrow[l, two heads, "\pi"'] & K \arrow[l, tail, "\iota"']\end{tikzcd}$$

where K is abelian and $(|G|, |K|) = 1$. Then this extension splits.

Proof. This will effectively follow from the fact that multiplication by $|G|$ on $C^* (G; V)$ is null homotopic under the homotopy from proposition 6.4. Recall this means we have the expression:

$$[h, \delta] = |G| \operatorname{id}_{C^*(G;V)}$$

where the homotopy can be written explicitly as:

$$(h\alpha) (g_1, \cdots, g_{n-1}) = (-1)^{n-1} \sum_{x \in G} \alpha (g_1, \cdots, g_{n-1}, x)$$

In other words, multiplication by $|G|$ is 0. That is, every element in the cohomology of a finite group is torsion of order dividing $|G|$.

So now if $(|G|, |K|) = 1$ then $|G|$ is invertible in K, but it is also 0. So every curvature is cohomologous to some cocycle which is divisible by the order of G. But that cocycle is, by the formula above, null-homotopic. So because it is a cocycle it is the coboundary of some 1-cochain, which means that the original section, for which we chose our curvature, can actually be modified by that function $G \to K$ making it a homomorphism, meaning the extension is split. ☐

6.8 Basic properties of solvable groups

We now state the standard definition of a solvable group via the derived series. First consider the commutator functor, which is a subfunctor of the identity functor on **Grp**. This takes any group to its commutator subgroup:

$$G \to [G, G] = \{[g_1, g_2] \cdots [g_{2n-1}, g_{2n}] \mid g_1, \cdots, g_{2n} \in G\}$$

Recall this is not just a normal subgroup, but in fact a characteristic subgroup which we write as: $[G, G] \lhd\!\!| \, G$.

Proposition 6.8. *When we have $G'' \twoheadleftarrow G$, this implies $[G'', G''] \twoheadleftarrow [G, G]$. Similarly, When we have $G \hookleftarrow G'$, this implies $[G, G] \hookleftarrow [G', G']$.*

First take $G^{(0)} = G$. Then inductively define:

$$G^{(n+1)} = \left[G^{(n)}, G^{(n)}\right]$$

so we have

$$G^{(0)} \; |\!\!\rhd G^{(1)} \; |\!\!\rhd \cdots$$

Definition 6.6. If $G^{(n+1)} = 1$, we say G is *solvable* of degree n. In particular, G is *solvable* for finite n. For a given group G, let $\operatorname{Solv} G$ denote the set of solvable subgroups.

Solvable groups comprise the smallest subcategory of **Grp** which contains all Abelian groups, and which is closed under extensions. A solvable group of degree i is obtained from i extensions.

Example 6.5. Abelian groups are solvable of degree 0, and metabelian[6.3] are solvable of degree 1.

Now we have some observations:

Proposition 6.9. *Let G be solvable of degree n. For any quotient group G'' and any subgroup G', we have*

$$(G'')^{(i)} \twoheadleftarrow G^{(i)} \hookleftarrow G'^{(i)}$$

In addition, G'' and G' are solvable of degree $\leq n$.

Proposition 6.10. *Suppose G is an extension of G'' by G' where G'' is solvable of degree m and G' is solvable of degree n. Then G is solvable of degree $m+n+1$.*

Proof. We know that

$$1 = (G'')^{(m+1)} \twoheadleftarrow G^{(m+1)}$$

which implies $G^{(m+1)} < G'$ so

$$G^{(m+n+2)} < (G')^{n+1} = 1$$

thus G is solvable of degree $m+n+1$. ☐

The previous proposition shows us the category $\mathbf{Grp}_{\text{solv}}$ of solvable groups is hereditary, cohereditary, and closed under extensions. We also see that this category contains the category **Ab** of abelian groups. In fact it even contains the closure of this category under extensions, written $\mathbf{Ab}_{ext\,\text{cl}}$. But by the definition of $\mathbf{Grp}_{\text{solv}}$, this is also contained in $\mathbf{Ab}_{ext\,\text{cl}}$ since if $G^{(n+1)}$ is trivial, then $G^{(n)}$ is abelian, meaning G is an extension of $G/G^{(n)}$, which is abelian, which is solvable of degree $n-1$. So by induction, solvable groups of degree n are obtained by applying n extensions by abelian (co)kernels. In any case, solvable groups are exactly the closure of **Ab** under taking extensions.

6.9 Complements

We introduce the following basic notion:

Definition 6.7. For a subgroup $K < H$, a subgroup $J < H$ is said to be a complement of K iff $H = JK$ and $J \cap K = 1$

Proposition 6.11. *Splitting of an extension with normal kernel is exactly equivalent to the kernel having a complement.*

[6.3] Recall metabelian groups are all of the groups which can be expressed as extensions of abelian groups.

In particular, we have

$$\begin{tikzcd}
\sigma(G) \arrow[r, hook] & H \arrow[dl, bend left, "\pi", "\sim"'] \\
G &
\end{tikzcd}$$

and since π restricted to H is an isomorphism,

$$G \cap K = 1 \qquad\qquad H = GK = KG$$

6.10 Solvable case of Schur-Zassenhaus theorem

We can now prove a more general version of the Schur-Zassenhaus theorem using these basic facts about extensions of solvable groups and the fact that we know the weaker case in theorem 6.1.

Theorem 6.2 (Schur-Zassenhaus (solvable)). *If $(|G|, |K|) = 1$, and K is solvable, then the extension splits.*

Proof. If K is abelian we are done. So suppose K is solvable but not abelian and that this is the smallest counterexample. Let M be a minimal nontrivial normal subgroup of H contained in K. Since K is solvable this M surely exists. Now we know $[M, M] \triangleleft M$ is normal as well. Since M is solvable, this is always proper unless M is trivial, but we chose M such that it was nontrivial and minimal, so $[M, M] = 1$. This is a general fact that such minimal nontrivial normal subgroups are abelian.

Now take such a subgroup M, and take quotients of H and K to get:

$$\begin{tikzcd}
 & M \arrow[r, equal] \arrow[d, tail] & M \arrow[d, tail] \\
G \arrow[d, equal] & H \arrow[l, two heads, "\pi"] \arrow[d, two heads, "\pi''"] & K \arrow[l, tail] \arrow[d, two heads] \\
G \arrow[r, bend right, hook, "\sigma'"'] & H/M \arrow[l, two heads, "\pi'"'] & K/M \arrow[l, tail]
\end{tikzcd}$$

It is a basic fact in homological algebra that the induced map between the quotients on the left is an isomorphism. But since this extension was the smallest counterexample, the bottom line splits. So we have some splitting σ' which is a monomorphism, so $\pi' \circ \sigma' = \mathrm{id}_G$. Now we have the diagram:

$$\begin{tikzcd}
M \arrow[r, equal] \arrow[d, tail] & M \arrow[d, tail] \\
H' \arrow[r, tail, dashed, "\overline{\sigma}'"] \arrow[d, two heads, dashed, "\overline{\pi}''"] & H \arrow[d, two heads, "\pi''"] \\
G \arrow[u, bend left, "\sigma''"] \arrow[r, tail, "\sigma'"] & H/M
\end{tikzcd}$$

The map $\overline{\pi}''$ is the pullback of π'' and the map $\overline{\sigma}'$ is the pullback of σ'. The left column here is the pullback of the right column by σ'. This is also called a base-change. Explicitly this pullback is:

$$H' = \{(g,h) \in G \times H \mid \sigma'(g) = \pi''(h)\}$$

So it is the largest subset of the cartesian product such that the image agreed in H/M. Now we are done, because we haven't changed the condition on the kernel. The kernel is abelian, normal, and its order is a divisor of the order of K. Even for large $|K|$ this is already relatively prime to G, so therefore the order of M is relatively prime to G, which means we can apply the abelian form of the theorem to this new extension. See exercises for the rest of this proof. $\square$

6.11 Exercises

Exercise 6.11.1. Complete the proof of theorem 6.2. That is, show that $\pi \circ \bar{\sigma}' \circ \sigma'' = \mathrm{id}_G$. Equivalently, $\sigma := \overline{\sigma}' \circ \sigma''$ is a splitting of $\mathcal{E}$ which means contradiction with the assumption that this was a counterexample.

Exercise 6.11.2. Suppose $H' \rhd K'$

$$\begin{tikzcd}
G' \arrow[d, dashed, "f"] & H' \arrow[l, two heads, "\pi'"] \arrow[d, hook] & K' \arrow[l, tail] \arrow[d, hook] \\
G & H \arrow[l, two heads, "\pi"] & K \arrow[l, tail]
\end{tikzcd}$$

Show that f is injective iff $K' = H' \cap K$

Exercise 6.11.3. Show that f is surjective iff $H = H'K = KH'$.

Exercise 6.11.4. Show that the center $Z(N)$ of a normal subgroup of a group H is normal in H.

6.12 Frattini's argument

The following theorem is a famous, though simple, Corollary of the Sylow theorems which we introduce now for use in the forthcoming arguments.

Theorem 6.3 (Frattini). *Suppose K is a normal subgroup of a finite group H, and P is a Sylow p-subgroup of K. So $H \rhd K >_{\mathrm{Syl}} P$. Then we have:*

$$H = N_H(P)\,K$$

Proof. We know that for any $h \in H$,

$${}^{h}P < {}^{h}K = K$$

hence by the second Sylow theorem, there exists $k \in K$ such that ${}^{h}P = {}^{k}P$. In other words ${}^{k^{-1}h}P = P$ so $k^{-1}h \in N_H(P)$ so $h \in KN_H(P)$. $\square$

Note that there is a more general version of Frattini's argument which we saw before. In particular, suppose $K \triangleleft H$ and H acts on a set X such that $\mathrm{Res}_K^H X$ is transitive. Then $H = KH_x$ where H_x is a stabilizer of any element $x \in X$. If we additionally suppose that H acts freely, this means that K_x is trivial for any x. In other words, x is a K torsor. In this case, $K_x = H_x \cap K$, so we get a complement. So if you have any abelian normal subgroup in any finite group, we can always find a set on which the whole group acts, which is a torsor over the subgroup. In addition, all of the complements of this subgroup in the group, are stabilizers. That is, they necessarily fix at least one element.

Example 6.6. Start with a set where there is no chance of anything acting transitively. In particular, consider the set of all set-theoretic sections of H. Then suppose that we already know that there are sections which are complements of K in H. Then notice, that every element from any such complement, fixes the section which corresponds to the complement since it will simply take this subset to itself since a subgroup is closed. In particular, the elements that fix it are precisely elements from that group. So clearly every complement fixes something.

But as we noticed initially, there is no chance that even H, much less K, would act transitively. So now consider the gauge group to be the set of all functions from G to K which clearly acts transitively. Note that K is identified with the constant function. Now consider charge on these sections. Any two sections, over every point of G, differ by an element of K. But if K is abelian, we can multiply these differences by K in any order. For two sections s and s' we call this difference the quotient of s by s'. This is a gauge transformation. So this gauge transformation is a function from G to K. So then we are effectively taking a Feynman integral. The corresponding integration is over our group G. So say $s = ks'$, then we are just taking the product over all g of k and we get an element in K. So this is like an operation on sections, with values in K. We can do this for any Torsor. So now we can say that $s/s' = 1$ is an equivalence relation, and now we can verify that the action of K or G on these equivalence classes, is something.

6.13 Final form of Schur-Zassenhaus theorem

So we have seen the Schur-Zassenhaus theorem in both theorem 6.1 and theorem 6.2 as giving conditions for an extension to split. In this section we meet the most general form of the Schur-Zassenhaus theorem in two parts. The first part relaxes the condition even more to only require relatively prime orders. The second part asserts that all of the resulting complements of K in H are in fact conjugate.

6.13.1 Part 1

Theorem 6.4 (Schur-Zassenhaus (part 1))**.** *If* $(|G|, |K|) = 1$*, then any extension of* G *by* K *splits.*

Proof. From Frattini's argument and the exercises in the previous section, we have the following pair of extensions:

$$\begin{tikzcd}
G \arrow[d, equal] & N_H(P) \arrow[l, two heads, "\pi'"'] \arrow[d, hook] & N_K(P) = N_H(P) \cap K \arrow[l, tail] \arrow[d, hook] \\
G & H \arrow[l, two heads, "\pi"] & K \arrow[l, tail]
\end{tikzcd}$$

Then since $(|G|, |K|) = 1$, and since p divides the order of K, p does not divide the order of G. This means any Sylow p-subgroup of K, is always a Sylow p-subgroup of H. Now if P is not normal in H, $N_H(P)$ is strictly smaller, so by the induction hypothesis, there exists a complement $Q \subset N_H(P)$ of $N_K(P)$. This means π' takes Q isomorphically to G. In particular, this means Q is a complement of K in H as well.

So now the only remaining case is if any such P is normal in H. But if P is normal in H, then it is normal in K, and this means K is nilpotent, and therefore solvable. Therefore we are done. ☐

Notice that we didn't even need that argument. We can give the following proof:

Proof. Suppose for a given prime, the Sylow p-subgroup P is normal. So we have $P \triangleleft K \triangleleft H$, and $P \triangleleft H$. Since P is a p-group, it has nontrivial center. From the exercise in the previous section, we know the center $Z(P)$ is also normal since P is normal. So we have the following:

$$\begin{tikzcd}
 & Z(P) \arrow[r, equal] \arrow[d, tail] & Z(P) \arrow[d, tail] \\
G \arrow[d, equal] & H \arrow[l, two heads] \arrow[d, two heads] & K \arrow[l, tail] \arrow[d, two heads] \\
G \arrow[r, bend right, "\sigma'"] & H/Z(P) \arrow[l, two heads] & K/Z(P) \arrow[l, tail]
\end{tikzcd}$$

So here, $Z(P)$ replaces the minimal normal solvable subgroup of K that we have seen. Since we have a strictly smaller order on the bottom line, we have the splitting σ' by the inductive hypothesis. As before, we use σ' to take a pullback of this extension to get the extension G' of $Z(P)$ by G. Now we can use the abelian kernel version of Schur-Zassenhaus to get another splitting σ''.

$$\begin{tikzcd}
Z(P) \arrow[r, equal] \arrow[d, tail] & Z(P) \arrow[d, tail] \\
G' \arrow[r, dashed, "\overline{\sigma}'"] \arrow[d, dashed] & H \arrow[d, two heads, "\pi''"] \\
G \arrow[u, bend left, "\sigma''"] \arrow[ur] \arrow[r, "\sigma'"] & H/Z(P)
\end{tikzcd}$$

Now as we saw in the first exercise, the composition $\overline{\sigma}' \circ \sigma''$ is a splitting and we are done. ☐

Remark 6.5. The only advantage of the second proof we gave here is that we don't have to actively invoke the structure of solvable groups.

6.13.2 Part 2

As mentioned earlier, the second part of the Schur-Zassenhaus theorem asserts that the complements of K in H are in fact conjugate.

Example 6.7. Note that such complements are not conjugate in general. We provide a counterexample for when this coprime cardinality condition is not met. Let G and K be vector spaces. Then $H := G \times K$ is an abelian group, and in particular a split extension of G by K, where π projects onto G. Now it is clear that all of the complements of K are just vector subspaces intersecting one of these vector spaces at 0 which together span the whole space. But there's no way for these to be conjugate to one another since the group is abelian.

It is clear that from the abelian form of Schur-Zassenhaus theorem 6.1 we have shown the existence of complements in the abelian case. We now show that these complements are in fact conjugate:

Lemma 6.1 (Schur-Zassenhaus (part two, abelian))**.** *If* $(|G|, |K|) = 1$ *and* K *is abelian, the complements of* K *in* H *are conjugate.*

Proof. If we have a subgroup $K < H$ then consider the set of set theoretic sections

$$\mathcal{S} := \mathrm{Sect}\left(\; H/K \xleftarrow[\pi]{} H \; \right)$$

and the group

$$\mathcal{K} := \{H/K \to K\}$$

This can be thought of as a gauge group. Now note that $\mathcal{S}$ is an $(H, \mathcal{K})$ biset, where H acts on the left in the obvious manner, and $\mathcal{K}$ acts on the right. Then we want to investigate this action. It is very important that $\mathcal{S}$ is a $\mathcal{K}$-torsor. This means that $\mathcal{K}$ acts freely with a single orbit. So this is a very big set, acted on by a very big group.

Now we define charge, and we will define what it means for two sections to have the same charge. Then under this coprime condition the result will follow. We need to develop some more formalism before we can complete this proof, so we will return to this. ☐

We now prove the second part of the theorem in full generality:

Theorem 6.5 (Schur-Zassenhaus (part two))**.** *Under hypothesis that either* G *or* K *are solvable, all complements of* K *in* H *are* K *conjugate.*

Remark 6.6. This additional hypothesis is redundant by a difficult theorem of Feit and Thompson which states that every finite group of odd order is solvable.

Remark 6.7. It might initially seem that this theorem is stronger than saying that all complements of K are H conjugate rather than K conjugate. But in fact they are equivalent, because for a given complement Q of K in H, we have $h = kq$ for $q \in Q$.

Proof. Proceed by induction on the size of H. First assume K is solvable. In fact we don't even need full solvability. We only really need that K contains an abelian subgroup which is normal in H. Then we have:

$$\begin{tikzcd}
& M \arrow[d, tail] & M \arrow[d, tail] \\
G \arrow[d, equal] & H \arrow[l, two heads, "\pi"] \arrow[d, "\pi''"] & K \arrow[l, tail] \arrow[d] \\
G & H/M \arrow[l, two heads, "\pi'"] & K/M \arrow[l, tail]
\end{tikzcd}$$

With the first part of the theorem, we have already shown the existence of complements. So suppose Q and Q' are complements of K in H. Then $\pi''(Q')$ and $\pi''(Q)$ are subgroups of H/M. In particular they are complements of K/M in H/M since $Q \cap M \subset Q \cap K = 1$ and $Q' \cap M \subset Q' \cap K = 1$ and $\pi' \circ \pi'' = \pi$, so the images of Q and Q' under π'' still map to G under π'.

Now by the inductive hypothesis, there exists $k \in K$ such that ${}^{k}Q \subset Q'M$ but $Q' \cap M = 1$ and is abelian. In other words, the group $Q'M$ is an extension of Q' by M:

$$\begin{tikzcd}
Q' & Q'M \arrow[l, two heads] & M \arrow[l, tail]
\end{tikzcd}$$

Therefore there exists $m \in M$ such that ${}^{m}Q = Q'$ and ${}^{mk}Q = Q'$.

Now assume the group G is solvable. Again, we can relax this slightly. We assume G is such that the abelianization $G^{\mathbf{Ab}}$ is nontrivial. Let p divide the order of G. Of course this means $p \not| \, |K|$. Then suppose there exists an epimorphism $G \to C_p$ where C_p is the cyclic group with p-elements. Denote the kernel of this map by $\overline{G}$. Notice that there is also a map $\rho : H \to C_p$ given by composition of $\pi : H \to G$ and our map $G \to C_p$. Denote the kernel of ρ by $\overline{H}$. That is we have the following diagram:

$$\begin{tikzcd}
\overline{G} \arrow[d, tail] & \overline{H} \arrow[l] \arrow[d, tail] & K \arrow[l, tail] \arrow[d, equal] \\
G \arrow[d, two heads] & H \arrow[l, two heads, "\pi"] \arrow[d, "\rho"] & K \arrow[l, tail] \\
C_p \arrow[r, equal] & C_p &
\end{tikzcd}$$

Now let Q and Q' be two complements of K in H. Then we have the following claim:

Claim 6.1. $\overline{H} \cap Q$ and $\overline{H} \cap Q'$ are complements of K in $\overline{H}$

Exercise 6.13.1. Prove this.

By the inductive hypothesis, this means that there exists $k \in K$ such that

$$^{k}\left(\overline{H} \cap Q\right) = \overline{H} \cap Q'$$

So we have reduced this to the case where we can assume Q and Q' have the same intersection with $\overline{H}$. Now let P be a Sylow p-subgroup in Q and P' a Sylow p-subgroup in Q'. Notice that $\overline{H} \cap P$ is a Sylow p-subgroup in $\overline{H}$.

Now taking $\overline{Q} \coloneqq Q \cap \overline{H}$, since $Q \twoheadrightarrow C_p$, we have the extension:

$$\begin{tikzcd} C_p & Q \arrow[l, two heads] & \overline{Q} \arrow[l, tail] \end{tikzcd}$$

Note $P \cap \overline{Q}$ is precisely a Sylow p-subgroup of $\overline{Q}$. Furthermore, if p^l is the highest power of p dividing $|G|$, p^{l-1} must be the highest power of p dividing Q. This means there are elements in P which are not in $\overline{Q}$, which means they must map nontrivially to C_p. And since C_p has no nontrivial subgroups, we have $Q = P\overline{Q}$ and similarly $Q' = P'\overline{Q}$.

Now consider the group $\langle Q, Q' \rangle \subset H$. Notice that $\overline{Q}$ is normalized by Q and by Q' since $\overline{Q}$ is simultaneously the intersection of Q with a normal subgroup, and Q' with a normal subgroup. Therefore the group $\langle Q, Q' \rangle$ normalizes $\overline{Q}$ as well. This means P and P' are Sylow p-subgroups of $\langle Q, Q' \rangle$ since they have maximal possible order. Then we know that there is $h \in \langle Q, Q' \rangle$ such that $^{h}P = P'$, so

$$^{h}Q = {}^{h}P\,{}^{h}\overline{Q} = {}^{h}P\overline{Q} = P'\overline{Q} = Q'$$

and we are finished by the remark that the complements are H conjugate iff they are K conjugate. ☐

6.14 Hall subgroups

Let X be a G-torsor. Let $K \lhd G$. Then the set of K-orbits X_K, that is the set of orbits of this action restricted to K, is equipped with the induced structure of a G/K-set.

Exercise 6.14.1. Show that X_K is a G/K-torsor.

Definition 6.8. $(|G : H|\,, |H|) = 1$ iff $H < G$ is a *Hall* subgroup.

Let $H < G$ be a Hall subgroup. This is equivalent to saying that if

$$|G| = \prod_{\pi(G)} p^{e_p(G)}$$

where $\pi(G)$ denotes a finite set of primes dividing the order[6.4] of G then this implies

$$|H| = \prod_{\pi \subset \pi(G)} p^{e_p(G)}$$

[6.4] This is empty for trivial G.

for some subset $\pi \subset \pi(G)$. This leads to:

$$|G : H| = \prod_{\pi(G)\setminus\pi} p^{e_p(G)}$$

Definition 6.9. For any set of primes π, we say that G is a π-group iff $\pi(G) \subset \pi$.

The complement to π in $\pi(G)$ is denoted π'. And in particular, for any prime p, we write $p' := \{p\}'$. In addition to this, for any $n \in \mathbb{Z}^+$, write $|n|_\pi$ for the largest π divisor of n. The following follows directly from the definition:

Proposition 6.12. *For all n, $(|n|_\pi, |n|_{\pi'}) = 1$.*

Hall π-subgroups of a given group G are the maximal π-subgroups of G and moreover, $|H| = |G|_\pi$.

Theorem 6.6. *Any π-subgroup is contained in some Hall π-subgroup.*

Theorem 6.7. *Any two Hall π-subgroups are conjugate.*

We will prove these later...

Remark 6.8. The previous two theorems should be compared to the first two Sylow theorems. In particular, if π consists of a single prime, these are exactly them. In fact, these two theorems will also turn out to be equivalent to the Schur-Zassenhaus we have spent so much time with.

Theorem 6.8 (Burnside)**.** *If $\pi(G) = \{p, q\}$ then G must be solvable.*

Example 6.8. The smallest non-abelian simple group is A_5. It follows from this that every group of order less than 60 is solvable. Indeed $\pi(A_5) = \{2, 3, 5\}$.

Example 6.9. If $\pi(G) = \{p, q\}$ has only two elements, then every Sylow p-subgroup has every Sylow q-subgroup as a complement. So $G = PQ$ where P is any Sylow p-subgroup, and Q is any q-subgroup. Note that neither of these have to be normal.

Exercise 6.14.2. Consider $G = A_5$, so $\pi(G) = \{2, 3, 5\}$. For which subsets of 2-primes of $\{2, 3, 5\}$ does there exist a Hall π-subgroup?

Schur-Zassenhaus can then be reformulated as a statement about normal Hall-subgroups:

Theorem 6.9 (Schur-Zassenhaus (Hall subgroups (part 1)))**.** *If H is a normal Hall π-subgroup of a group G, then it has a complement, say K, which is necessarily a Hall π'-subgroup. That is,*

$$G = H_\pi H_{\pi'}$$

where H_π is normal and $H_{\pi'}$ may not be.[6.5] *In terms of extensions, we have:*

$$\begin{tikzcd}
 & K \arrow[dl, "\sim"'] \arrow[dr, hook] & & \\
G/H & & G \arrow[ll, two heads] & H \arrow[l, tail] \\
\pi' - group \arrow[u] & & &
\end{tikzcd}$$

Theorem 6.10 (Schur-Zassenhaus (Hall subgroups (part 2)))**.** *By part one, a normal Hall π-subgroup of G exists, which implies that a Hall π'-subgroup exists. Now if additionally, either a solvable Hall π, or π'-subgroup exists, then all Hall π'-subgroups are conjugate. In particular, they are conjugate by an element of H.*[6.6]

[6.5] If it is normal, this is a trivial extension.

[6.6] It is said that that they are fused.

Chapter 7

Transfer and fusion

7.1 Gauge groups

In any category, for any arrow α, one can consider the set of right sections, that is the right inverses of α. These are arrows σ such that $\alpha \circ \sigma = \mathrm{id}$ is the identity on the target of α. We say that α is a *split epimorphism* iff the set defined above is non-empty. We can also consider the set of left inverses of α, and if this is non-empty, α is a *split monomorphism*.

Example 7.1. One often considers this in a concrete category, so the objects are just sets with some algebraic structure. Then we can forget about this structure and just consider sections in **Set**.

Warning 7.1. Epimorphisms of sets with multiple algebraic operations are not necessarily surjective maps of the underlying sets.

Proposition 7.1. *Every monomorphism and every epimorphism in* **Set** *is split.*

Proof. It is a trivial fact that every monomorphism in **Set** is split. The fact that every epimorphism splits follows directly from the axiom of choice. □

Remark 7.1. Thanks to Gödel, we know that this is consistent, yet independent of the axioms (say ZF) of set theory.

Consider a group G and a subgroup $H < G$. Then we have the canonical quotient map

$$H\backslash G = \{Hg \mid g \in G\} \xleftarrow[\pi]{} G$$

The function π is not necessarily a group homomorphism, but it is certainly a homomorphism of G-sets. Now define the following set of all sections:

$$\begin{aligned}\Gamma_{H\backslash G} = \Gamma_\pi &= \left\{s : H\backslash G \to G \mid \pi \circ s = \mathrm{id}_{H\backslash G}\right\} \\ &= \{s : H\backslash G \to G \mid s(C) \in C\} \subset \mathrm{Map}(H\backslash G, G)\end{aligned}$$

Define the gauge group to be:

$$\mathcal{H} := \mathrm{Map}\,(H\backslash G, H)$$

We have a left action of this on $\Gamma_{H\backslash G}$ given by:

$$\chi, s \mapsto \chi s \qquad\qquad (\chi s)\,(C) = \chi\,(C)\,s\,(C)$$

for $s \in \Gamma_{H\backslash G}$ and $\chi \in \mathcal{H}$. We want to consider other actions on $\Gamma_{H\backslash G}$, and in order to consider these we define the set of transversals:

$$\mathcal{T}_{H\backslash G} = \{T \subset G \,|\, \pi|_T : H\backslash G \leftrightarrow T\}$$

In particular notice that there is a canonical identification between the set of sections Γ and the set of transversals. In one direction we can take a section and then its image is a corresponding transversal. In the reverse, we take a transversal T, and associate to it some section s_T such that $s_T\,(C)$ is the unique member of $T \cap C$.

This canonical identification means that for any group action we define on one, we get a corresponding action on the other. In particular, we have an obvious left action of the gauge group $\mathcal{H}$ on $\mathcal{T}_{H\backslash G}$. We also have a right regular action of G on itself, which induces an action on $\mathcal{T}_{H\backslash G}$, since the set of transversals is right G-invariant subset of $\mathcal{P}\,(G)$.

Exercise 7.1.1. Show that the set of transversals $\mathcal{T}_{H\backslash G}$ is a right G-invariant subset of $\mathcal{P}\,(G)$ and therefore the right regular action of G on itself induces an action on $\mathcal{T}_{H\backslash G}$.

Exercise 7.1.2. Write down explicitly the induced right action of G on the set of sections $\Gamma_{H\backslash G}$.

Denote this right action by $s, g \mapsto s * g$. It is important that we write this with the $*$ notation because $\mathrm{Map}\,(H\backslash G, G)$ clearly has a right regular action on G. We can simply multiply a G-valued function on any set on the left and on the right by an element of G, but this is not the same as $s * g$. The following follows directly from the definitions:

Proposition 7.2.

$$(s * g)\,(H\backslash G) = s\,(H\backslash G)\,g$$

Exercise 7.1.3. Verify that the left $\mathcal{H}$-action on $\Gamma_{H\backslash G}$ commutes with the right G-action.

Now let $N = N_G\,(H)$. Then for every $n \in N$, $n\,(Hg) = Hng$. In particular, N acts on the left on the right cosets of H in G. So now we have two left actions. In addition, this left action commutes with the right action by elements of G. In other words, right cosets of H in G are permuted by the left action of the normalizer. Next we will develop when H has a complement in its normalizer.

The left N action commutes with the right G-action, and together with the left action of $\mathcal{H}$, it provides a left action of the semidirect product:

$$N_G\,(H) \ltimes \mathcal{H}$$

7.2 Semidirect product

We now offer a brief review of the semidirect product. Consider two groups N, K where N acts on K, that is we have some homomorphism $\alpha : N \to \operatorname{Aut}(K)$. Then we take $S = N \ltimes_\alpha K$ to have the Cartesian product as the underlying set. Note that we have

$$\begin{tikzcd}
N \arrow[r, bend left, "\sigma"] & S \arrow[l, two heads, "\pi"] & K \arrow[l, tail]
\end{tikzcd}$$

so this contains a copy of both, but only K is normal. Now if $K \triangleleft N$, then we can take α to simply be conjugation, and we want this product to be something of the form $nn'\left(k^{n'}\right)k'$. This leads us to generalize to:

$$(n, k)(n', k') := (nn', \alpha(n')(k)k')$$

But if this is a right semidirect product, α must be an antihomomorphism from N. If α is a homomorphism we would have the factor in the second component is $\alpha(n)^{-1}(k)$ instead. We can more cleanly do this the other way:

$$K \rtimes_\alpha N \qquad\qquad (k, n)(k', n') = (k({}^{n}k'), nn')$$

Example 7.2. Take $N = \operatorname{Aut} K$ and $\alpha = \mathrm{id}$. Then we have the canonical extension:

$$\begin{tikzcd}
\operatorname{Aut} K \arrow[r, bend left, "\mathrm{id}"] & K \rtimes \operatorname{Aut} K \arrow[l, two heads] & K \arrow[l, tail]
\end{tikzcd}$$

This is what is often called the holomorph of the group, $\operatorname{Hol}(K)$. This is a group which somehow contains both the group and the set of automorphisms. So we have seen this is canonically a semidirect product.

Then we can take a pullback by any action given by a homomorphism $N \to \operatorname{Aut} K$ to get another extension

$$\begin{tikzcd}
\operatorname{Aut} K \arrow[r, bend left, "\mathrm{id}"] & K \rtimes \operatorname{Aut} K \arrow[l, two heads] & K \arrow[l, tail] \\
N \arrow[u] & ? \arrow[l] \arrow[u] & K \arrow[l] \arrow[u, equal]
\end{tikzcd}$$

But since this is a pullback of a split extension, this extension splits as well. So our original extension is somehow universally terminal.

7.3 Transfer

7.3.1 Preliminary setup

So we have seen that the set of transversals and the set of sections are the same. This set is a left $N_G(H) \ltimes \mathcal{H}$-set and a right G-set. In particular, we have that

$\Gamma_{H\backslash G}$ is a left $\mathcal{H}$-torsor. Now suppose α is a homomorphism from H to some abelian group. We now define a pairing from $\Gamma, \Gamma \to \mathcal{H}$ given by division. This is well defined precisely because Γ is a torsor over $\mathcal{H}$. Now we can follow this pairing with the application of α fiberwise, and then take this so-called integral. Together we write this composition as $//_\alpha$ as in the following diagram:

$$\begin{tikzcd}
\Gamma_{H\backslash G}, \Gamma_{H\backslash G} \arrow[r, "/"] \arrow[rrr, bend left, "//_\alpha"] & \mathcal{H} \arrow[r, "\alpha\circ()"] & \mathrm{Map}\left(H\backslash G, A\right) \arrow[r, "\int_{H\backslash G}"'] & A \\
s', s \arrow[r, mapsto] & s'/s & &
\end{tikzcd}$$

Example 7.3. If H is abelian, we can take $\alpha = \mathrm{id}$ and then we just have:

$$\begin{tikzcd}
\Gamma_{H\backslash G}, \Gamma_{H\backslash G} \arrow[rr, "//"] \arrow[dr, "/"] & & H \\
& \mathcal{H} \arrow[ur, "\int_{H\backslash G}"] &
\end{tikzcd}$$

so we are just sending:

$$s', s \mapsto \prod_{c \in H\backslash G} \left(s'/s\right)(c)$$

Then $\sim$ is a congruence for the left action of $N_G(H)$. So now if we consider $\Gamma_{H\backslash G}/\sim$, we can notice that this is an $N_G(H)$-set.

We can make the following preliminary observations:

$$\begin{aligned}
s//_\alpha s &= e \in A \\
\left(s''//_\alpha s'\right)\left(s'//_\alpha s\right) &= s''//_\alpha s \\
s//_\alpha s' &= \left(s'//_\alpha s\right)^{-1}
\end{aligned}$$

This directly shows that we have the following equivalence relation[7.1] on Γ. We declare $s' \sim_\alpha s$ iff $s'//_\alpha s = e$.

Now take any two transversals T and T'. We know there exists a unique $\chi \in \mathcal{H}$ such that $T' = \chi T$. Therefore

$$T'g/Tg = \chi Tg/Tg = \chi$$

Now if H is abelian we of course still know there is unique $\chi \in \mathcal{H}$ such that $T' = \chi T$, but now for any $\nu \in N_G(H) \ltimes \mathcal{H}$ we have:

$$\nu T'/\nu T = \nu\chi T/\nu T = \nu\chi\nu^{-1}\nu T/\nu T = {}^{\nu}\chi$$

[7.1] This is sometimes referred to as being equi-charged.

But the real question is whether we have this same expression for this $//_\alpha$ operation. In general, we have

$$\nu T'//_\alpha \nu T = {}^\nu \left(T//_\alpha T\right)$$

if $\ker \alpha$ is invariant under conjugation by elements of $N_G(H)$. That is, if $\ker \alpha \triangleleft N_G(H)$. This is certainly the case if H is abelian.

So now assuming $H \triangleleft G$ is abelian, we can set $\alpha = \mathrm{id}$ and define

$$X \coloneqq \Gamma_{H\backslash G}/\sim_{\mathrm{id}_H}$$

Let $H \subset \mathcal{H}$ consist of constant gauges. Then each element $h \in H$ acts on X as multiplication by $h^{|G:H|}$. The interpretation here is that we are integrating the "constant" function h.

Now consider $\chi \in \mathcal{H}$ such that $\int_{H\backslash G} \chi = e$. Denote the collection of such χ by $\mathcal{H}_0$. Then we have that $\mathcal{H}/\mathcal{H}_0 \simeq H$ so this is just the integral map:

$$\int_{H\backslash G} : \mathcal{H} \to H$$

The whole point is:

$$x \in \mathcal{H}_0 \iff \chi s \sim s$$

Now let $[S] \in X$ be the class of S. Then the action is

$$\left(\int_{H\backslash G} \chi\right)[S] \coloneqq \chi\,[S] \coloneqq [\chi S]$$

so for a general h, the action is $h\,[S] \coloneqq [\chi S]$ where $\int \chi = h$.

7.3.2 Schur-Zassenhaus theorem

Now under the relatively prime assumption, the map multiplication by $|G:H|$ from $H \to H$ is an isomorphism. At this point we observe:

Proposition 7.3. *If $H \triangleleft G$, then G acts on X, with H acting as a subgroup via $\mathcal{H}$ action.*

So if $g \in G$ also belongs to H, then g acts on $[S] \in X$ by $h^{|G:H|}$. Now $h^{|G:H|}[S] = [S]$ iff $h\,[S] = [S]$ since $|G:H|$ is relatively prime to $|H|$. In particular, there exists j which is inverse to $|G:H| \bmod |H|$.

Also, for any $k \in H$, there exists $h \in H$ such that $h^{|G:H|} = k$. So if I want for example $k\,[S]$ then there is h such that $h^{|G:H|}[S]$. So this is a free, transitive action.

Exercise 7.3.1. Let X be a G-set such that any subgroup $H < G$ is a transitive H-set. Show that $G = G_x H$ where G_x is the stabilizer of any $x \in X$.

Solution. Frattini

Corollary 7.1. *If X is an H-torsor, then $1 = H_x = H \cap G_x$ since H acts freely. Hence G_x is a complement to H.*

So we find that all the stabilizers which intersect trivially with H are complements. Now suppose K is a complement to H which is normal and abelian. Then K gives us a class $[K]$ which is the transversal. And of course elements of K act trivially on it, that is for every $k \in K$, $kK = K$. So the equivalence class stays put.

7.3.3 Alternative description

We offer a slightly less constructive discussion of transfer. So we have seen that we have two left actions and one right action on the set $\Gamma_{H\backslash G} \simeq \mathcal{T}_{H\backslash G}$. Moreover, this is clearly an $\mathcal{H}$ torsor. These actions have no relation a priori. However they will turn out to be related, since we have the inclusion, $H \hookrightarrow \underline{\underline{H}}$ where $\underline{\underline{H}}$ denotes the collection of constant gauges. In fact, when we restrict this left regular action of the normalizer to H, we actually get the action of the subgroup of constant gauges. Also notice that $N_G(H)$ acts on $\operatorname{Map}(H\backslash G, H)$. This is an action by conjugation on the value space.

Proposition 7.4. *The action of $N_G(H)$ normalizes the action of $\mathcal{H}$.*

Proof. We want to show that for every $\chi \in \mathcal{H}$, there is some χ' such that $n\chi$ acts as χ'. Take any transversal T, multiply it by any $\chi \in \mathcal{H}$, then act by multiplying by $n \in N_G(H)$. This is the same as $\left(n\chi n^{-1}\right) nT$ which gives

$$n\chi T = {}^{n}\chi nT$$

and ${}^{n}\chi \in \mathcal{H}$. So we have explicitly found such a χ'. ☐

Remark 7.2. Suppose two groups A and B act on a set X. That is, we have

$$\lambda : A \to \operatorname{Aut}_{\mathbf{Set}}(X) \qquad\qquad \mu : B \to \operatorname{Aut}_{\mathbf{Set}}(X)$$

Then saying the action of A normalizes the action of B just means $\lambda(A)$ normalizes $\mu(B)$. Recall $a \in A$ normalizes B iff $[a, B] \subseteq B$

Now assume H is abelian. Then we have a canonical extension

$$\begin{tikzcd}
H & \mathcal{H} \arrow[l, two heads, "\int_{H\backslash G}"'] & \mathcal{H}_1 \arrow[l, tail] \\
\prod_{C \in H\backslash G} \chi(C) & \chi \arrow[l, mapsto] &
\end{tikzcd}$$

Now as a consequence of the previous proposition we have the following:

Corollary 7.2. *$\mathcal{H}_1$ is G-invariant subgroup under the action of $N_G(H)$.*

Now take X to be the set of orbits of the group of gauges with charge 1: $X \coloneqq \left(\mathcal{T}_{H\backslash G}\right)_{\mathcal{H}_1}$. Therefore the action of the normalizer $N_G(H)$ induces an action on X. Now due to the above exercise, X is an $H \simeq \mathcal{H}/\mathcal{H}_1$-torsor. What we find here now, is that $H \subset N_G(H) \simeq \underline{\underline{H}} \subseteq \mathcal{H}$. The diagram here is:

$$\begin{tikzcd}
N_G(H) & & \\
H \arrow[u, hook] \arrow[r] \arrow[drr, "\cdot|G:H|"'] & \underline{\underline{H}} \arrow[r, hook] & \mathcal{H} \arrow[d, two heads] \\
 & & H \simeq \mathcal{H}/\mathcal{H}_1
\end{tikzcd}$$

7.3.4 Schur-Zassenhaus theorem

We now assume $(|G:H|, |H|) = 1$ as in the statement of the Schur-Zassenhaus theorem. Note that this means $H \simeq \underline{\underline{H}}$. In fact, if we now consider the more general setting:

$$G' \xrightarrow{\alpha} G \xrightarrow{\lambda} \Sigma_X$$

Suppose that α is an epimorphism. Then G acts transitively iff G' acts transitively. Now suppose α is a monomorphism. Then if G acts freely, this implies G' acts freely. Therefore if α is an isomorphism, then X is G-torsor iff X is a G'-torsor. Now in the case at hand, G and G' are the same, but α is indeed a nontrivial epimorphism. This ultimately means there is a complement to H in $N_G(H)$. These are all conjugate because when $G = N_G(H)$, so when H is normal, then indeed each complement gives us a transversal, and therefore every complement will fix an actual transversal corresponding to the group. So in particular, the orbit containing that complement is fixed by that complement. So every complement appears as the stabilizer of some orbit, and because all orbits form a torsor, we are done. This is a beautiful tautological argument.

7.4 Extensions and complements

If $H \lhd G$ has a complement K in G we write $H \lhd_K G$.

Lemma 7.1. *Suppose $A < G$ is an abelian normal subgroup of some group G with complement K. That is, $A \lhd_K G$ is abelian. Then any maximal subgroup $M < G$ containing K does not contain A.*

Proof. Let M be any maximal subgroup of G containing K. Since $G = AK < AM$, we know $M \lneqq AM = G$ so $A \nsubseteq M$ as desired. ☐

Lemma 7.2. *Let $A < G$ be an abelian normal subgroup of some group G with complement K. That is, $A \lhd_K G$ is abelian. Suppose there is some maximal subgroup M containing K which also does not contain A. Then $AM = G$.*

Proof. Let M be a maximal subgroup of A containing K which does not contain A. Then since A is normal, $AM < G$. We also have $M \lneq AM$, and since M is maximal, $AM = G$. ☐

Lemma 7.3. *If we have an abelian subgroup $A \triangleleft G$, and $K < G$ such that $G = AK$, then $A \cap K \triangleleft G$.*

Proof. Let $g \in G$. Then there exists some $a \in A$ and $k \in K$ such that $g = ak$. Now we know a centralizes $A \cap K$ since this is a subset of abelian A. Therefore $a \in N_G(A \cap K)$. In addition, k normalizes A since it is abelian, and of course also normalizes K, so

$$^k(A \cap K) \subseteq {}^kA \cap {}^kK = A \cap K$$

and therefore $^g(A \cap K) = A \cap K$ so we are done. ☐

Corollary 7.3. *Let $A \triangleleft G$ be a minimal abelian subgroup, and $K \lneq G$ be such that $AK = G$. Then $A \cap K = 1$.*

Proof. Suppose abelian $A \triangleleft G$ is minimal, and $K \lneq G$ satisfies $G = AK$. These imply that $A \not\subseteq K$, so $A \cap K \lneq A$ is normal in G. But since A was minimal, $A \cap K = 1$. ☐

Corollary 7.4. *For any minimal abelian normal subgroup $A \triangleleft G$, and any maximal subgroup $M <_{\max} G$, either $A < M$, or $A \cap M = 1$.*

7.5 Frattini subgroup

Definition 7.1. For a group G we define the Frattini subgroup of G to be:

$$\varphi(G) := \bigcap_{M <_{\max} G} M$$

We will eventually see that $\varphi(G)$ is always a characteristic subgroup. Now using the preceding lemmata and corollaries we have:

Proposition 7.5. *Let A be a minimal abelian normal subgroup of G. Then TFAE:*

1. *A is complemented.*
2. *A is complemented by a maximal subgroup.*
3. *We have $A \not\subseteq \varphi(G)$.*
4. *$A \cap \varphi(G) = 1$*

Additionally, under any of these conditions, the complement to A must be maximal, and all maximal subgroups M such that $A \not\subseteq M$ are isomorphic.

7.5.1 Main result regarding the Frattini subgroup

The main theorem is the following:

Theorem 7.1. *If $A \triangleleft G$ is abelian and $A \cap \varphi(G) = 1$, then*

1. *$A = A_1 \cdots A_n$ is a product of mutually disjoint minimal abelian normal subgroups.*
2. *There exist maximal subgroups $M_1, \cdots, M_n$ such that $A_i \triangleleft_{M_i} G$.*
3. *$A \triangleleft_{M_1 \cap \ldots \cap M_n} G$*

Before proving this, we make some preliminary considerations.

Warning 7.2. This theorem is not to say that if a normal abelian subgroup has nontrivial intersection with $\varphi(G)$ that is cannot have a complement.

Example 7.4. If a normal abelian subgroup is a Hall π-subgroup, then by Schur-Zassenhaus there is a complement even though we don't necessarily have this trivial intersection with the Frattini subgroup.

Consider any $H \lneq G$. Then take $\overline{H}$ to be the intersection of all subgroups which are maximal with respect to containing H. Note this is always a non-empty collection. We call this the maximal closure of H. This is however not necessarily equal to H itself. So we have $H < M < G$.

Example 7.5. The maximal closure of the trivial group is the Frattini group $\varphi(G)$.

Example 7.6. A cyclic p-group has a single maximal subgroup. In particular if we have a group of order p^n, then the maximal subgroup consists of the elements of order p. So this is a subgroup of order p^{n-1}. As such, the Frattini group $\varphi(G)$ is nontrivial in this case.

Let $X, Y, Z \subset G$ be three subsets of G. Then under certain conditions, we have the following inclusions:

$$\begin{tikzcd}
& (XY)\cap Z & \\
& (XY)\cap Z^2 \arrow[u, hook, "Z^2\subseteq Z \implies"] & \\
X\left(Z\cap Y\right) \arrow[ur, hook, "X\subseteq Z \implies"] & & \left(X\cap Z\right)Y \arrow[ul, hook, "Y\subseteq Z \implies"] \\
X\left(Z^{-1}Z\cap Y\right) \arrow[u, hook, "Z<G \implies"] & & \left(X\cap ZZ^{-1}\right)Y \arrow[u, hook, "Z<G \implies"] \\
X\left(X^{-1}Z\cap Y\right) \arrow[u, hook, "X\subseteq Z \implies"] & & \left(X\cap ZY^{-1}\right)Y \arrow[u, hook, "Y\subseteq Z \implies"] \\
& (XY)\cap Z \arrow[ul, hook] \arrow[ur, hook] &
\end{tikzcd}$$

Upon further consideration, in order for the left chain to hold we really just need $X \subseteq Z < G$. Similarly, in order for the right chain to hold we need only $Y \subseteq Z < G$. We now offer some corollaries to the preceding considerations:

Corollary 7.5. *If $X \subseteq Z < G$ then*

$$(XY)\cap Z = X\left(Z\cap Y\right)$$

If $Y \subseteq Z < G$, then

$$(XY)\cap Z = \left(X\cap Z\right)Y$$

Note these both equal $\left(X\cap Z\right)\left(Y\cap Z\right)$ so intersection with subgroup distributes over multiplication of subsets under the assumption that Z dominates at least one factor.

Corollary 7.6. *If we have $Z < G$ and $X \subseteq Z \subseteq XY$, then this implies:*

$$Z = X\left(Z\cap Y\right)$$

Similarly, if we have: $Y \subseteq Z \subseteq XY$ and $Z < G$ then this implies:

$$Z = \left(X\cap Z\right)Y$$

Corollary 7.7. *Suppose $XY = G$, and $X\cap Y = 1$. If we also have a subgroup $Z < G$ such that $X \subseteq Z$, then we get that $Z = X\left(Z\cap Y\right)$, and of course $X\cap Z\cap Y = 1$.*

Then this gives us relative complements.

Corollary 7.8. *If $H \triangleleft_K G$, and L is such that $H < L < G$, then $H\cap L \triangleleft L$ which has $L\cap K$ as a complement in L.*

Lemma 7.4 (n-complements)**.** *Suppose we have normal subgroups $\{H_i\}_{i=1}^n$ with corresponding complements $\{K_i\}_{i=1}^n$. Assume that $H_{i+1} < K_1 \cap \cdots \cap K_i$ for $1 \leq i < n$. Then*

$$H_1 \cdots H_n \lhd_{K_1 \cap \ldots \cap K_n} G$$

Exercise 7.5.1. Prove the 2-complements lemma. That is, prove the base case $n = 2$ for the proof of the n-complements lemma.

Exercise 7.5.2. Derive the n-complements lemma from the 2-complements lemma by induction.

Lemma 7.5. *If two normal subgroups H_1, H_2 avoid each other, then they commute.*

Proof. Consider the set $[H_1, H_2]$. This is contained in H_1 iff H_1 is normalized by H_2, which is certainly the case if they are both normal. Therefore, $[H_1, H_2] < H_1 \cap H_2$. ☐

Finally we can prove the following theorem:

Theorem 7.2. *Let $A \lhd G$ be abelian such that $A \cap \varphi(G) = 1$. Then there exists $K < G$ such that $A \lhd_K G$. More specifically, A is necessarily a product $A_1 \cdots A_n$ where each factor is a minimal abelian normal subgroup, complemented by some maximal subgroup $M_i < G$, and $A_{i+1} \subset M_1 \cap \cdots \cap M_i$. And finally, $M_1 \cap \cdots \cap M_n$ is a complement of A.*

Proof. Let A_1 be any minimal abelian normal subgroup of G, contained in A. Such A_1 exists, because if not, then A itself must be minimal. Let M_1 be a maximal subgroup that avoids A. Now consider $A \cap M_1$. We know this is abelian and normal because $AM_1 \supseteq A_1M_1 = G$, which means $AM_1 = G$, so $A \cap M_1 \lhd G$, which is abelian as well since it is also a normal subgroup of A. Also notice that $A \cap M_1$ is a (normal) complement to A_1 in A.

Now we have two possibilities. If $A \cap M_1$ is trivial, then we are done. If not, let A_2 be a minimal normal subgroup of $A \cap M_1$. Otherwise, we essentially construct an algorithm. The input for the ith iteration is as follows: a sequence of subgroups $A_1, \cdots, A_i < A$ and a sequence of maximal subgroups $M_1, \cdots, M_i < A$ complementing the A_i, such that $M_1 \cap \cdots \cap M_i$ is a complement of $A_1 \cdots A_i$. If $A \cap M_1 \cap \cdots \cap M_n$ is nontrivial then take A_{i+1} to be a minimal abelian normal subgroup of this nontrivial intersection and proceed to the next iteration. If $A \cap M_1 \cap \cdots \cap M_n$ is trivial, then we just need to show A is equal to the appropriate product. We know:

$$A \subset A_1 \cdots A_n \left(M_1 \cap \cdots \cap M_n\right)$$

Now if a group is a subgroup of a product of two groups, and it avoids one, then it is contained in the other, so we are done. ☐

7.6 Exercises

Definition 7.2. An element $x \in G$ is said to be a *non-generator* iff for any subset $Y \subset G$, we have that $\langle \{x\} \cup Y \rangle = G$ implies $\langle Y \rangle = G$.

Prove the following statements:

Exercise 7.6.1. Every element of $\varphi(G)$ is a non-generator.

Exercise 7.6.2. If x is a non-generator, then $x \in \varphi(G)$.

Exercise 7.6.3. Suppose $X \subseteq \varphi(G)$ is any subset. Show that for any subset $Y \subseteq G$, we have that if $\langle X \cup Y \rangle = G$, then this implies $\langle Y \rangle = G$.

7.7 Nilpotency

Corollary 7.9. *For any subgroup $K < G$, $K\varphi(G) = G$ iff $K = G$.*

Lemma 7.6. *$\varphi(G)$ is characteristic.*

Proof. Indeed, if $\alpha \in \mathrm{Aut}(G)$, $M <_{\max} G$ implies $\alpha(M) <_{\max} G$. ☐

Proposition 7.6. *$\varphi(G)$ is nilpotent.*

Proof. Let $S <_{\mathrm{Syl}_p} \varphi(G)$. Then since $\varphi(G)$ is characteristic, it is normal, so by theorem 6.3, $G = \varphi(G) N_G(S)$. Now from the corollary, this means $N_G(P) = G$, so $S \triangleleft G$, and therefore $S \triangleleft \varphi(G)$. ☐

Remark 7.3. We have actually shown that such a Sylow subgroup is normal in the entire group. This leads us to the following:

Lemma 7.7. *Sylow subgroups of normal nilpotent subgroups of G are normal in G.*

Proof. Due to their uniqueness, a Sylow subgroup $S < N \triangleleft G$ of nilpotent normal subgroup N, is characteristic in N. In particular, it is normalized by G, since $G = N_G(S)$. ☐

We now have the following lemma:

Lemma 7.8. *If $M \triangleleft_{\max} G$, then G/M is cyclic of prime order.*

Proof. For any subgroup $H < G/M$, we have the following pullback:

$$\begin{tikzcd}
G/M & G \arrow[l, two heads, "\pi"] & M \arrow[l, tail] \\
H \arrow[u, hook] & \pi^{-1}H \arrow[l, two heads] \arrow[u, hook] & M \arrow[l, tail] \arrow[u, equal]
\end{tikzcd}$$

In particular:

$$\pi^{-1}H \gneq M \iff H \neq 1 \qquad G/M \gneq \pi^{-1}H \iff H \neq G$$

In other words, if we take the quotient by any normal subgroup, and this quotient has at least one nontrivial subgroup, this normal subgroup is not maximal. This is because any proper subgroup of the quotient, has a preimage which would contain it. This shows that if M is a normal maximal subgroup, then the quotient by it must be a group which doesnt have any nontrivial subgroups. But in every group, we can take any element, and generate a cyclic group with this element. So if we take a nontrivial element, this is a group which satisfies this. So for M to be maximal, G/M must be generated by that element, so the group is cyclic. But the only cyclic group for which every nontriviel element is a generator, is a cyclic group of prime order. $\square$

Recall we have already seen the following lemma in our proof of the fact that any Sylow subgroup of a nilpotent group is normal.

Lemma 7.9. *In a nilpotent group N, any proper subgroup $H \lneq N$ is properly contained in its normalizer.*

We now consider the intersection

$$\bigcap_{M \lhd_{\max} G} M$$

assuming there is at least one such M. Then we have the following extension:

$$\begin{tikzcd} \prod_{M \lhd_{\max} G} G/M & G \arrow[l, two heads] & \bigcap_{M \lhd_{\max} G} M \arrow[l, tail] \end{tikzcd}$$

So in light of the above lemma, we have that the product:

$$\prod_{H \lhd_{\max} G} G/M$$

is an elementary abelian group, i.e. a product of cyclic groups of prime order. So every group with at least one maximal normal subgroup, is an extension of an elementary abelian group E, by the intersection of all such maximal normal subgroups.

We now have the following theorem:

Theorem 7.3. *A group is nilpotent iff every maximal subgroup is normal.*

Proof. If G is nilpotent, by the preceding lemma, we have that every proper subgroup is contained in its normalizer, which means for any maximal subgroup $M <_{\max} G$, we have $M \lneq N_G(M) = G$, so M is normal.

Under the hypothesis that all maximal subgroups are normal, since G is an extension of $G/\varphi(G)$ by $\varphi(G)$, we have that G is an extension of an elementary abelian group E by its Frattini subgroup. Note that this elementary abelian group is certainly nilpotent.

$$\begin{tikzcd} E & G \arrow[l, two heads] & \varphi(G) \arrow[l, tail] \end{tikzcd}$$

Now by the exercise immediately after this proof, we have that for any Sylow subgroup $S <_{\text{Syl}} G$, $S \cap \varphi(G)$ is a Sylow subgroup of $\varphi(G)$. Since $\varphi(G)$ is nilpotent, we know that all of its Sylow subgroup are normal. Therefore $S \cap \varphi(G)$ is normal in $\varphi(G)$. But a Sylow subgroup is normal iff it is unique, so S is normal in G, and G is nilpotent. ☐

Exercise 7.7.1. Suppose an extension

$$G'' \twoheadleftarrow G \leftarrowtail G'$$

of finite groups is given. Show that for any Sylow subgroup $S <_{\text{Syl}} G$, we have $S \cap G' <_{\text{Syl}} G'$.

We will eventually show:

Theorem 7.4. *A group G is nilpotent iff the quotient of a group by its Frattini subgroup $G/\varphi(G)$ is nilpotent.*

Remark 7.4. This is nontrivial, because the category of nilpotent groups is not closed under extensions. It is however closed under quotients, so this gives us one direction.

Example 7.7. To see this, the simplest counterexample is:

$$C_2 \twoheadleftarrow S_3 \leftarrowtail C_3$$

S_3 is not nilpotent, yet it is an extension of nilpotent group by a nilpotent group.

7.8 Central extensions

Definition 7.3. An extension of groups $G'' \twoheadleftarrow G \leftarrowtail G'$ is said to be central iff $G' < Z(G)$.

Recall we have a notion of the category of extensions of a group G. So the objects are extensions:

$$G \twoheadleftarrow H \leftarrowtail H$$

and morphisms are homomorphisms between the three groups which preserve G and make the corresponding diagram commutative. These boil down to the homomorphisms between the extended groups which preserve the kernels:

$$\begin{tikzcd}
G \arrow[d, equal] & H \arrow[l, two heads] \arrow[d] & K \arrow[l, tail] \\
G & H' \arrow[l, two heads] & K' \arrow[l, tail]
\end{tikzcd}$$

If it exists, the universal central extension is the extension such that every other extension is a pushout from it. That is, this is universal in the sense that it is an initial object. Suppose that we have any homomorphism $f : K \to K'$. Then we form a pushout. Since the pushout of a monomorphism is a monomorphism, this gives us some H', and then the quotient of H' by K' is canonically equivalent to G.

Definition 7.4. A group is perfect iff it is equal to its own commutator subgroup.

Theorem 7.5. *A group G is perfect iff there exists a universal central extension of G. In particular, the kernel of this universal central extension is canonically isomorphic to $H_2(G;\mathbb{Z})$.*

We will write this universal central extension as:

$$\begin{tikzcd} G & \tilde{G} \arrow[l, two heads] & H_2(G;\mathbb{Z}) \arrow[l, tail] \end{tikzcd}$$

Let us denote $\tilde{G}$ by (G,G).

Warning 7.3. Don't confuse this this with the commutator.

In particular this construction first takes the free group $F(G\times G)$, and then we mod out by some relations. In particular, we want the identities which hold between commutators, which hold in every group. But these are precisely the relations which hold in the commutator group of the free group.

$$\begin{tikzcd} G & & F\{X\} \arrow[ll, two heads] \\ {[G,G]} \arrow[u, equal] & & {[F,F]} \arrow[ll, two heads] \arrow[u, tail] \\ & & F(F\{X\}\times F\{X\})/R \arrow[u, "\simeq"] \end{tikzcd}$$

for some relations R such that this is an isomorphism.

Now the commutator can be considered as an operation $G,G\to G$. Since this is a map, it certainly induces a map $F(G\times G)\to G$ which is actually a homomorphism of groups. The image of this in G is the commutator subgroup.

$$\begin{tikzcd} G,G \arrow[r, "{[\cdot,\cdot]}"] \arrow[d] & {[G,G]} \\ G\times G \arrow[r] \arrow[ur] & F\{G\times G\} \arrow[u, two heads] \end{tikzcd}$$

So we get an extension of $[G,G]$ with a huge kernel. Then if we divide by the universal relations which form a normal subgroup, then this is actually a central subgroup. Then we have the following theorem:

Theorem 7.6. *This kernel of the relations between commutators in G divided by relations which are universal, is canonically isomorphic to H_2G.*

This gives us the four term exact sequence:

$$\begin{tikzcd} 1 & H_1G \arrow[l] & G \arrow[l, two heads] & (G,G) \arrow[l, "{[\cdot,\cdot]}"'] & H_2G \arrow[l] & 1 \arrow[l] \end{tikzcd}$$

Note we have written H_iG for $H_i\left(G, \mathbb{Z}\right)$ to be the homology group with trivial coefficients.

But why do we care about central extensions? If we have any central extension of a group G, we can take any $g \in G$ and any $\tilde{g}$ which maps to it:

$$\begin{tikzcd}
G & H \arrow[l, two heads] & C \arrow[l, tail] \\
g & \tilde{g} \arrow[l, mapsto]
\end{tikzcd}$$

Then we consider the action of conjugation under this element $\tilde{g}$. Now any two such lifts to $\tilde{g}$ are not the same, but they only differ by an element of the center. As such, this conjugate action is independent of the choice of $\tilde{g}$, and depends only on g. So this provides us with a homomorphism from $G \to \operatorname{Aut}\left(H\right)$.

7.8.1 Algebraic approach

We can see this same story in the language of algebras. In particular, what we have seen already is homology of an algebra. In our four term exact sequence, we secretly have that $H_1G = \operatorname{Tor}_1^{\mathbb{Z}G}\left(\mathbb{Z}, \mathbb{Z}\right)$. Note for the augmentation ideal IG, we have $\operatorname{Tor}_1^{\mathbb{Z}G}\left(\mathbb{Z}, \mathbb{Z}\right) \cong IG/\left(IG\right)^2$ where

$$\begin{tikzcd}
\mathbb{Z} & \mathbb{Z}G \arrow[l, two heads, "\int"'] & IG \arrow[l, tail]
\end{tikzcd}$$

Now for non-unital algebras, there is a concept of annihilator extensions. This means some extension $\tilde{A}$ of A:

$$\begin{tikzcd}
A & \tilde{A} \arrow[l, two heads] & J \arrow[l, tail]
\end{tikzcd}$$

such that $J\tilde{A} = 0 = \tilde{A}J$. Note this is impossible in the unital case. So fix A, and consider the category of annihilator extensions. Then this category has initial object iff $A = A^2$.

Exercise 7.8.1. Show that $\left(I_{\mathbb{Z}}G\right)^2 = I_{\mathbb{Z}}G$ iff $G = [G, G]$

So it is clear, that for general algebras, if $\tilde{A}$ is the unitalization, we have:

$$\begin{tikzcd}
H_1G & & & H_2G & \\
A/A^2 \arrow[u, "\simeq"] \arrow[d, equal] & A \arrow[l] & A \otimes_{\tilde{A}} A \arrow[l, "\text{mult}"'] & \mathrm{HB}_2\left(A\right) \arrow[l] \arrow[u, "\simeq"] & 0 \arrow[l] \\
\mathrm{HB}_1\left(A\right) & & & &
\end{tikzcd}$$

where $\mathrm{HB}_i\left(A\right)$ denotes the ith Bar homology.

Warning 7.4. In general, multiplication is not a homomorphism of algebras unless they are commutative.

Theorem 7.7. *If $A = I_{\mathbb{Z}}G$ for any G, you get the canonical isomorphism in the above diagram.*

Now if we take $G = \mathrm{GL}(R)$ for some unital ring R. Then $[G, G] = E(R)$ is the group of elementary matrices. The fact that $E(R)$ is perfect is trivial. Then for G, we take universal central extension, and there is a model for this given by the Steinberg group $\mathrm{St}(G)$. Now the kernel is second homology of $E(R)$, this is comparable to the special linear group. This is the second K-functor in the sense of Milnor. Then we can follow this sequence to $\mathrm{GL}(R)$, and take the universal determinant homomorphism to get Whitehead's definition of the first K-functor.

$$\begin{tikzcd}
\mathrm{GL}(R)^{\mathrm{op}} \arrow[d, equal] & \mathrm{GL}(R) \arrow[l, "\det"'] & E(R) \arrow[l] & \mathrm{St}(R) \arrow[l, two heads] & H_2(E(R)) \arrow[l, tail] \arrow[d, equal] \\
K_1(R) & & & & K_2(R)
\end{tikzcd}$$

Note that Grothendieck gave a definition of the 0th K-functor as the group of stable isomorphism classes of finitely generated projective modules.

7.9 Fitting subgroup

Definition 7.5. Let G be a finite group and p be a prime. Then we define:

$$O_p(G) := \bigcap_{S <_{\mathrm{Syl}_p} G} S$$

We will sometimes write:

$$O_\pi(G) := \prod_{p \in \pi} O_p(G)$$

for any subset $\pi \subset \pi(G)$.

Definition 7.6. The *Fitting subgroup* of a group G is the group $F(G) := O_{\pi(G)}(G)$. This is also written as $\mathrm{Fit}(G)$.

Proposition 7.7. *$O_p(G)$ is characteristic.*

Proposition 7.8. *$O_p(G)$ is the largest normal p-subgroup of G.*

Proof. If $P \lhd G$ is some p-subgroup, then by the first and second Sylow theorems, $P < S$ for all Sylow p-subgroup S. Therefore $P < O_p(G)$. ☐

We now show some more involved results. Consider the extension:

$$\begin{tikzcd}
G/\varphi(G) & G \arrow[l, two heads, "\pi"'] & \varphi(G) \arrow[l, tail]
\end{tikzcd}$$

Suppose $P \lhd G/\varphi(G)$ is a normal p-subgroup. Let $\tilde{G} = \pi^{-1}(P)$. Then we take a pullback, and get the following diagram:

$$\begin{tikzcd}
G/\varphi(G) & G \arrow[l, two heads, "\pi"] & \varphi(G) \arrow[l, tail] \\
P \arrow[u, hook] & \tilde{G} \arrow[l, two heads] \arrow[u, hook] & \varphi(G) \arrow[l, tail] \arrow[u, equal]
\end{tikzcd}$$

We already know that for any normal subgroup of the quotient of an extension, the pre-image under the quotient map is also normal. We also know that a Sylow subgroup of $\tilde{G}$ will map to a Sylow subgroup of P. That is if S is a Sylow p-subgroup of $\tilde{G}$, then π restricted to S is still surjective, and in addition, for all $g \in G$, $P = \pi_*({}^gS)$. However, we have that in general:

$$\bigcap \pi_*({}^gS) \supsetneq \pi_*\left(\bigcap_{g\in G} {}^gS\right)$$

without equality.

Exercise 7.9.1. Show that a Sylow subgroup S of $\tilde{G}$ is normal in $\tilde{G}$.

Solution. Use the characterization of the Frattini subgroup which asserts that it is the maximal subgroup consisting of non-generators.

Exercise 7.9.1 shows us that if we look at any normal subgroup of this quotient, then its pre-image has a unique Sylow subgroup. In other words, P is the image of this unique group, and then we actually have the equality:

$$\bigcap \pi_*({}^gS) = \pi_*\left(\bigcap_{g\in G} {}^gS\right)$$

Now if we take any normal subgroup of G and its direct image, it would end up in a normal subgroup in the quotient. If you take any normal p-subgroup of G, its image is a normal p-subgroup. In every group, we have a maximal normal p-subgroup, which is exactly this intersection $O_p(G)$.

Exercise 7.9.2. Show that: $\pi_*(O_p(G)) = O_p(G/\varphi(G))$

Exercise 7.9.3. Let $\pi \subseteq \pi(G)$ be a nonempty subset. Show (by induction on the cardinality of π) that

$$\bigtimes_{p\in\pi(G)} O_p(G) \simeq O_\pi(G)$$

Clearly this implies:

$$|O_\pi(G)| = \prod_{p\in\pi} |O_p(G)|$$

Solution. We know that this map is always surjective, so we really just have to show this is injective. Proceed by induction on the cardinality of $\pi \subset \pi(G)$. The base case is showing for any two $p, p' \in \pi(G)$, we have

$$O_p(G)\, O_{p'}(G) = O_p(G) \times O_p(G)$$

These groups are normal, and we know every product of normal subgroups normalizes the original groups. That is if $H, K \lhd G$ are normal groups that avoid each other, then $H \subset C_G(K)$ and $K \subset C_G(H)$. In particular, every O_p and $O_{p'}$ centralize one another.

Now suppose we already have the result for some $\pi \subset \pi(G)$. So we have that this group has order as we said, and is isomorphic to the Cartesian product. Then suppose $p \in \pi(G) \backslash \pi$. If there is no such p we are done. Now prove this for $\pi' = \pi \cup \{p\}$. Normality is trivial. Intersection property follows from arithmetic of the orders. The order of O_p is a power of p, and the order of O_π is a number not divisible by p, so they must have trivial intersection.

Proposition 7.9. *Every nilpotent normal subgroup is contained in* $F(G)$.

Proof. By exercise 7.9.3, the Fitting group is normal and nilpotent in G. This observation combined with exercise 7.9.1 shows us that every nilpotent normal subgroup of G is contained in the Fitting group. ☐

We now know that we have the following extension:

$$\begin{tikzcd} F(G/\varphi(G)) & F(G) \arrow[l, two heads] & \varphi(G) \arrow[l, tail] \end{tikzcd}$$

So this is really the same as what we were doing before with the normal p-subgroup $P \lhd G$, and then getting the inverse image $\tilde{G}$, only instead of some normal p-subgroup, we are taking the largest nilpotent normal subgroup: $F(G/\varphi(G))$.

Exercise 7.9.4. Show that $F(G)$ is the preimage of $F(G/\varphi(G))$ under the quotient map π. I.e. show that we have the following diagram:

$$\begin{tikzcd} G/\varphi(G) & G \arrow[l, two heads, "\pi"'] & \varphi(G) \arrow[l, tail] \\ F(G/\varphi(G)) \arrow[u, hook] & F(G) \arrow[l, two heads] \arrow[u, hook] & \varphi(G) \arrow[l, tail] \arrow[u, equal] \end{tikzcd}$$

[Hint: This is essentially a corollary of previous results, so it is important that you specify exactly what statements imply this one.]

Theorem 7.8. *The set* $\pi(G/\varphi(G)) = \pi(G)$. *I.e. if* $p \in \pi(G)$, *then* p *divides* $|G : \varphi(G)|$.

Remark 7.5. So the Frattini subgroup is indeed somehow "inessential."

Proof. We know $O_p\left(G/\varphi\left(G\right)\right)$ is trivial iff $O_p\left(G\right)\subseteq\varphi\left(G\right)$. Now let $S<_{\mathrm{Syl}_p}G$. Suppose $S<\varphi\left(G\right)$. In particular, quotient by Frattini would not have p dividing the order. In that case, $G=N_G\left(S\right)\varphi\left(G\right)$ so $G=N_G\left(S\right)$ which implies S is normal in G. Since S is normal Sylow, we have the following extension:

$$\begin{tikzcd} G/S & G \arrow[l, two heads] & S \arrow[l, tail] \end{tikzcd}$$

and $\left(\left|G/S\right|,\left|S\right|\right)=1$, so by Schur-Zassenhaus, there is a complement K to S. Therefore $G=KS$, and since $|K|<|G|$ since S is nontrivial, meaning $K\neq G$, so $KS\subseteq K\varphi\left(G\right)$, so $G=K\varphi\left(G\right)$, so $G=K$. ☐

7.10 Morphisms in the category G-set

Recall the category G-**set**. We have $f\in\mathrm{Hom}_{G\textbf{-set}}\left(X,X'\right)$ iff f is G-equivariant, which means

$$f\left(gx\right)=gf\left(x\right)$$

for all $x\in X$ and $g\in G$.

Lemma 7.10. *Any morphism f induces maps on the spaces of fixed points and on the spaces of orbits.*

The diagram here is:

$$\begin{tikzcd} X'^G \arrow[d, tail] & X^G \arrow[l, "f^G"'] \arrow[d, tail] \\ X' \arrow[d, two heads] & X \arrow[l, "f"'] \arrow[d, two heads] \\ X'_G & X_G \arrow[l, "f_G"'] \end{tikzcd}$$

Lemma 7.11. *For every $\mathcal{O}\in X_G$ we have some $f_G\mathcal{O}\in X'_G$. This induces a map $f_{\mathcal{O}}:\mathcal{O}\to f_G\mathcal{O}$ as in the following diagram:*

$$\begin{tikzcd} f_G\mathcal{O} \arrow[d, tail] & \mathcal{O} \arrow[l, dashed, "f_{\mathcal{O}}"'] \arrow[d, tail] \\ X' & X \arrow[l, "f"'] \end{tikzcd}$$

Remark 7.6. Consider the space of all maps $X\to X'$, $\mathrm{Map}\left(X,X'\right)$. This is canonically equipped with a G-set structure. For any function f, gf is the unique function $X\to X'$ such that

$$\left(gf\right)\left(gx\right)\coloneqq gf\left(x\right)$$

or equivalently

$$gf\left(x\right)=gf\left(g^{-1}x\right)$$

If we look at the set of fixed points, by our simple calculation we have:

$$\mathrm{Map}\left(X,X'\right)=\mathrm{Hom}_{\textbf{Set}}\left(X,X'\right)\supset\mathrm{Map}\left(X,X'\right)^G=\mathrm{Hom}_{G\textbf{-set}}\left(X,X'\right)$$

Lemma 7.12. *For all $\mathcal{O} \in X_G$, $f_{\mathcal{O}}$ is a G-equivariant epimorphism. More precisely, if one picks $x \in \mathcal{O}$, then the fiber of $f_{\mathcal{O}}$ over $f(x)$ is identified with the space:* $\operatorname{Stab}_G x \backslash \operatorname{Stab}_G f(x)$

Lemma 7.13. *If we have:*

$$\begin{tikzcd} X' & X \arrow[l, "f"'] \\ f(x) & x \arrow[l, mapsto] \end{tikzcd}$$

then:

$$\operatorname{Stab}_G f(x) > \operatorname{Stab}_G x$$

Lemma 7.14. *$f_{\mathcal{O}}$ is an isomorphism of $\mathcal{O}$ with $f_G \mathcal{O}$ iff for every $x \in \mathcal{O}$,*

$$\operatorname{Stab}_G f(x) = \operatorname{Stab}_G x$$

Equivalently, there exists $x \in \mathcal{O}$ such that this equality holds.[7.2]

Definition 7.7. We call a point $x \in X$ a point of equi-stability

$$\operatorname{Stab}_G f(x) = \operatorname{Stab}_G x$$

This is also called a point of G-equi-stability or an equi-stabilizer point. We denote the set of such points by $X_f^{\mathrm{eqs}} \subset X$.

Lemma 7.15. *The set X_f^{eqs} is invariant under the action of G.*

Definition 7.8. Let f^{eqs} be the restriction of f to X_f^{eqs}.

The diagram here is:

$$\begin{tikzcd} & X^{\mathrm{eqs}} \arrow[dl, "f^{\mathrm{eqs}}"] \arrow[dd, tail] \\ X' & \\ & X \arrow[ul, "f"] \end{tikzcd}$$

We also write:

$$X_G^{\mathrm{eqs}} := \{\mathcal{O} \in X_G \mid f_{\mathcal{O}} \text{ isomorphism } \}$$

which is called the set of equi-stabilizer orbits. Of course notice:

$$\begin{tikzcd} X^{\mathrm{eqs}} \arrow[r, two heads] \arrow[d, tail] & X_G^{\mathrm{eqs}} \arrow[d, tail] \\ X \arrow[r, two heads] & X_G \end{tikzcd}$$

[7.2] This is a consequence of the homogeneous nature of each single orbit.

7.11 Epimorphisms in G-set

In a general category, a morphism η is an epimorphism iff given any α, β post-composable with η, we have that $\alpha \circ \eta = \beta \circ \eta$ implies $\alpha = \beta$.

$$\begin{tikzcd}
\bullet \arrow[r, "\eta"] & \bullet \arrow[r, shift left, "\alpha"] \arrow[r, shift right, "\beta"'] & \bullet
\end{tikzcd}$$

An epimorphism η is then said to be a split epimorphism when it admits a splitting. That is, it admits a right[7.3] inverse: $\eta \circ s$ is the identity on the target of η.

Now consider the forgetful functor $F : G\text{-}\mathbf{set} \to \mathbf{Set}$.

Exercise 7.11.1. Show that F preserves epimorphisms and is a reflector.

Recall that every epimorphism in **Set** splits, however this is not the case in G-**set**. Let f be any epimorphism in **Set**, and write Γ_f for the set of all set theoretic sections of f:

$$\Gamma_f := \{s : X \to X' \mid f \circ s = \mathrm{id}_{X'}\} \subset \mathrm{Map}\,(X', X)$$

Note that this is a G-invariant subset. The fixed points are precisely G-equivariant sections.

Lemma 7.16. *f is a split epimorphism in G-**set** iff Γ_f^G is nonempty.*

Lemma 7.17. *f is a split epimorphism iff $f^{eqs} : X^{eqs} \to X'$ is an epimorphism*

Lemma 7.18. *f^{eqs} is an epimorphism iff f^{eqs} is a split epimorphism.*

Proof. The necessity is clear so we only prove sufficiency. In the following diagram we have that f^{eqs} is an epimorphism iff the composition mapping $X^{\mathrm{eqs}} \to X'_G$ is surjective, which means all 4 of these morphisms are onto.

$$\begin{tikzcd}
X' \arrow[d, two heads] & X^{\mathrm{eqs}} \arrow[l, "f^{\mathrm{eqs}}"] \arrow[d, two heads] \\
X'_G \arrow[r, bend right, "\sigma"'] & X^{\mathrm{eqs}}_G \arrow[l, "f^{\mathrm{eqs}}_G"']
\end{tikzcd}$$

Now let σ be any splitting of the induced map between orbits f_G^{eqs}. We now use this σ to define a splitting of s_σ of f^{eqs}. For every orbit $\mathcal{O}' \in X'_G$, $\mathcal{O}' = f_G \sigma\,(\mathcal{O}')$. Then we have $f_{\sigma(\mathcal{O}')}$ is an isomorphism to some $\mathcal{O}$, so we can take an inverse which maps $\mathcal{O} \to \sigma\,(\mathcal{O}')$. Then we can embed this into X, so we really have a map $\mathcal{O} \to X$. So we have a family of morphisms of G-sets with a common target X. Now we define s_σ to be the universal map from the coproduct:

$$s_\sigma : \coprod_{\mathcal{O}' \in X'_G} \mathcal{O}' \cong X' \to X^{\mathrm{eqs}}$$

So we get a canonical bijection from $\Gamma_{f_G^{\mathrm{eqs}}}$ to Γ_f^G. $\square$

[7.3] If this was a left inverse this is sometimes called a retraction.

7.12 Application to quotient groups

Consider a subgroup $H < G$, and the right G-equivariant map $\pi : G \to H\backslash G$ regarded as an epimorphism in **Set**-G. Note that as a right G-set, this is free, i.e. $\mathrm{Stab}_G\, x = 1$. Now consider the subset $G_\pi^{\mathrm{eqs}} \subseteq G$ and map $\pi^{\mathrm{eqs}} : G^{\mathrm{eqs}} \to H\backslash G$. The fiber over any Hg is nonempty iff $\mathrm{Stab}_G\, Hg = 1$. But we know this stabilizer is exactly H^g. So unless H is trivial, there is no way that there is any equivariant splitting.

Now consider another subgroup $K < G$. Then π is still an epimorphism in **Set**-K, since this is of course right K-equivariant. Then $\mathrm{Stab}_K\, Hg = K^g \cap K$ is the fiber over any coset, which must be the identity for every $g \in G$.

Lemma 7.19. *$G \to H\backslash G$ is a split epimorphism in the category* **Set**-*K iff K avoids all conjugates of H.*

Recall the set of set theoretic splittings:

$$\Gamma_{H\backslash G} = \left\{ s : H\backslash G \to G \,|\, \pi \circ s = \mathrm{id}_{H\backslash G} \right\}$$

We know well that for any group which acts on π on the right, making it equivariant, we have that fixed points of the action on $\Gamma_{H\backslash G}$ are equivariant maps. So $\Gamma_{H\backslash G}^K$ are precisely the K-equivariant sections. Furthermore, this is nonempty precisely when K avoids conjugates of H. Recall that $\Gamma_{H\backslash G}$ is a left $\mathcal{H}$ torsor, where $\mathcal{H}$ is the gauge group $\mathcal{H} = \mathrm{Map}\,(H\backslash G, H)$ equipped with point-wise multiplication. Recall this means if you divide two K-equivariant sections, then we get that the difference is a unique element of $\mathcal{H}$. So $\Gamma_{H\backslash G}^K$ should somehow be a $\mathcal{H}^K$-torsor. But K doesn't operate directly on $\mathcal{H}$, so we consider the following setup:

$$\begin{tikzcd}
 & G \arrow[d, "\pi"] \\
{}_H G \arrow[r, equal] \arrow[d, two heads, "\rho"] & H\backslash G \arrow[d, two heads, "\rho"] \\
({}_H H)_K \arrow[r, equal] & H\backslash G/K
\end{tikzcd}$$

Then this ρ induces an injection:

$$\begin{tikzcd}
\mathrm{Map}\,(H\backslash G, H) & \mathrm{Map}\,(H\backslash G/K, H) \arrow[l, tail, "\rho^*"']
\end{tikzcd}$$

That is, ρ^* provides an isomorphism between $\mathrm{Map}\,(H\backslash G/K, H)$ and this $\mathcal{H}^K$. So equivariant sections form a torsor over functions on the set of double cosets.

Now let X be any set. If H is abelian, consider the group of all functions $\mathrm{Map}\,(X, H)$. Then we can take a sort of integral:

$$\begin{tikzcd}
\mathcal{H}_{X,0} \arrow[r, tail] & \mathrm{Map}\,(X, H) = \mathcal{H}_X \arrow[r, two heads, "\int_X"] & H
\end{tikzcd}$$

so we have that $\mathcal{H}_0^K$ is a normal subgroup of $\mathcal{H}^K$, such that $\mathcal{H}^K/\mathcal{H}_0^K = H$. Then $N_G(H)$ normalizes K-invariant ones. Similarly, it normalizes the kernel since we can calculate:

$$\int_{H\backslash G/K} {}^g\chi = {}^g\left(\int_{H\backslash G/K} \chi\right) = {}^ge = e$$

Now take:

$$X := \left(\Gamma_{H\backslash G}^K\right)_{\mathcal{H}_0^K}$$

This is a rather complicated set, but we do know that this is a $\mathcal{H}^K/\mathcal{H}_0^K$-torsor, Note X is a left $N_G(H)$-set. So we really have two actions. One comes from an action by functions which are constant on double cosets. The action of $g \in N_G(H)$ may be tricky, because we act on the value space, but this might not bring me to another fiber. But if we only consider the action of H, this clearly does keep us on the fiber. Therefore $H \hookrightarrow \mathcal{H}^K$ as constant functions. Now because every function in $\mathcal{H}^K$ acts on X via its integral, we need to calculate this. Since these functions are constant, this integral is just:

$$|H\backslash G/K| : H \to H$$

We have the following diagram:

$$\begin{tikzcd}
H \arrow[r, "|H\backslash G/K|"] \arrow[dr, bend right, "\tau"'] & H \arrow[d, "\text{torsor action}"] \\
 & \operatorname{Sym} X
\end{tikzcd}$$

where multiplication by $|H\backslash G/K|$ is isomorphism iff τ is a torsor action. And in this case, $N_G(H)$ would act on X, such that on a normal subgroup, H is a torsor, which implies

$$N_G(H) = H \operatorname{Stab}_{N_G(H)} x$$

for any $x \in X$ because $\operatorname{Stab}_H x = 1$. So H has a complement in its own normalizer. We have come upon the following theorem:

Theorem 7.9. *Let $H < G$ be an abelian subgroup, and $K < G$ any other subgroup which avoids H and its conjugates. Then if $(|H\backslash G/K|, |H|) = 1$, then there exists a complement of H in $N_G(H)$.*

Now how many elements are there over $|H\backslash G/K|$? Take Hg for any g, and look at the orbits under K. Consider this $HgK \subset H\backslash G$ as a single orbit. Then we are calculating the number of elements in a single orbit under the action of a single group. So we know we can just calculate this as the index of the stabilizer in the group. But the stabilizer of this action is precisely $H^g \cap K$. In other words, this map is $|K : H^g \cap K|$. This tells us that:

$$\int_{HgK} |K : H^g \cap K| = |G : H|$$

So we have established that the map from $G\backslash H \to H\backslash G/K$ has fibers of cardinality equal to $|K : H^g \cap K|$. which is equal to $|K|$ under the hypothesis which is already there.

Hence, $|G : H|$ is equal to the product of the cardinality of a fiber with the cardinality of the target. So this is saying that this is set-theoretically a product map. That is, we have $|H\backslash G| = |K|\,|H\backslash G/K|$. So now we need the additional hypothesis:

$$\left(\frac{|G|}{|H|\,|K|}, |H|\right) = 1$$

The avoidance only allows us to say that we get a torsor over H with normalizer acting on it, and containing a copy of H, which acts by the multiplicity $|H\backslash G/K|$. And if this is relatively prime to the order of the group on which it acts, then it is an automorphism. Therefore, the normalizer contains a subgroup which is a torsor over H. In other words we have the following theorem:

Theorem 7.10. *Suppose $H < G$ is abelian, and $K < G$ is any subgroup such that for every $g \in G$, ${}^gH \cap K = 1$. If:*

$$\left(\frac{|G|}{|H|\,|H|}, |H|\right) = 1$$

then there exists a complement L to H in $N_G(H)$.

In particular, if $H \lhd G$, the above theorem reads: If $H \cap K = 1$ and

$$\left(\frac{|G|}{|H|\,|H|}, |H|\right) = 1$$

then there exists a complement L to H in $N_G(H)$.

If L, L' are two such complements and $K := L \cap L'$, then since $G/HK = HL/HK \simeq L/L \cap K = L/K$, we have

$$|L : L \cap L'| = \frac{|G|}{(|H|\,|K|)}$$

Corollary 7.10. *If $(|L : L \cap L'|, |H|) = 1$, then L and L' are conjugate by an element of H.*

Proof. Consider $\Gamma_{H\backslash G}$ as a left $\mathcal{H}$ torsor. Then look at $\mathcal{H}_0 \subset \mathcal{H}$ which is the kernel of the integration map $\mathcal{H} \twoheadrightarrow H$. Now $\mathcal{H}_0$ is normalized by $N_G(H)$, and in particular, H acts on $\mathcal{H}_0$ in the same way as the subgroup $\underline{\underline{H}} \subseteq \mathcal{H}$ consisting of constant functions. Because $\mathcal{H}_0$ is normalized by the action of $N_G(H)$, the orbit quotient map passing to the orbit of the action on $\mathcal{H}_0$ is $N_G(H)$ equivariant, so the action of $N_G(H)$ on $\Gamma_{H\backslash G}$ passes to an action on $\left(\Gamma_{H\backslash G}\right)_{\mathcal{H}_0}$. So this is obtained by multiplying by certain gauge with total integral equal to zero. So now this is an $N_G(H)$ set. But how does H act on it? Well we know $\left(\Gamma_{H\backslash G}\right)_{\mathcal{H}_0}$. is an $\mathcal{H}/\mathcal{H}_0$ torsor. Now the integral gives us the identification between this quotient and H, therefore this is actually an H torsor.

Now in order to get that there is a complement to H in $N_G(H)$, we would have to know that the action of the copy of H which is a subgroup is also a torsor action. But now since H is constant functions, h acts on $\left(\Gamma_{H\backslash G}\right)_{\mathcal{H}_0}$ by $\int_{H\backslash G} g = |G:H|\, h$.

Now we have $(|G:H|, |H|) = 1$ iff H is a Hall subgroup of G. Recall that Schurr-Zassenhaus deals precisely with the case of normal abelian Hall subgroups.

Now given any complement L we get a splitting s_L. For such a splitting, action by an element of L won't change s_L. This means $L < \mathrm{Stab}_G\,(\text{orbit of } s_L)$, in fact this is equality. and for L' any other complement, $L' = \mathrm{Stab}_G\,(\text{orbit of } s_{L'})$ as well. So L and L' are indeed conjugate because they are stabilizers associated with a torsor action. $\square$

Now if you have partial complement, look for K invariant sections. This is nonempty iff K avoids all the conjugates of H. This is not invariant under the action of H, but it is a subgroup of the K-constant gauges $\mathcal{H}^K$. But these are in one to one correpsondence with functions from the double coset. That is, $\Gamma_{H\backslash G}$ is $\mathcal{H}^K$ torsor which is canonically isomorphic to $\mathrm{Map}\,(H\backslash G/K, H)$. So we have found that when H is normal, and K avoids conjugates of H, we have:

$$|H\backslash G/K| = |G:HK|$$

So here we took

$$\left(\Gamma^K_{H\backslash G}\right)_{\mathcal{H}^K_0}$$

Then the rest of the argument is the same. So the constant functions $h \in H < G$ acts on elements here as $\chi\,|G:HK|$ where $\chi \in \mathcal{H}^K/\mathcal{H}^K_0$ is the equivalence class associated to H. And therefore under this relatively prime assumption, we have that this is actually an H-torsor with respect to H as a subgroup of G, and therefore G acting on this space, is the product of any stabilizer of any orbit times K, and then because H acts with torsor action, the intersection of stabilizers with H, is the stabilizer under the action of H, which is trivial. Therefore G is represented as two groups.

So the original proof was providing existence of such stabilizers which are complements, without referring to their relationship to K. But since K is a partial complement it can be extended.

Corollary 7.11. *If L and L' are two complements, such that $K := L \cap L'$ satisfies the hypotheses that it avoids H, (which is automatically satisfied) and that $(|L:K|, |H|) = 1$, then each L stabilizes the orbit of s_L.*

7.13 Hall's theorem

Recall that we can start from a certain subcategory of groups $\mathbf{g_0}$ and some objects G'_0 G''_0. Then take extensions to get groups of the form G_1 as in:

$$\begin{tikzcd}
G''_0 & G_1 \arrow[l, two heads] & G'_0 \arrow[l, tail] \\
G''_1 & G_2 \arrow[l, two heads] & G'_0 \arrow[l, tail] \\
G''_{n-1} & G_n \arrow[l, two heads] & G'_0 \arrow[l, tail]
\end{tikzcd}$$

If we take $\mathbf{g_0}$ to be products of π and π' groups,[7.4] these are called π-separable.

Corollary 7.12 (Hall). *Fix a subset of primes $\pi \subseteq \pi(G)$. For every π-separable (π-solvable) group G there exists a Hall π-subgroup in G. Secondly, any two Hall π-subgroups are conjugate.*

Proof. Proceed by induction on the order of the group. Represent the group G as an extension with nontrivial kernel of a normal π-group. Then there are two scenarios. First consider H'' to be a Hall π subgroup. Then we take a pullback to get the following diagram:

$$\begin{tikzcd}
G'' & G \arrow[l, two heads, "\pi"'] & G'_0 \arrow[l, tail] \\
H'' \arrow[u, hook] & \pi^* H'' \arrow[l, two heads] \arrow[u, hook] & G'_0 \arrow[l, tail] \arrow[u, equal]
\end{tikzcd}$$

Now by simple arithmetic, we see that $\pi^* H''$ is also a Hall π-subgroup.

Now suppose we have two Hall π-subgroups H and H'. This means ${}^g H' \subset HG'_0$. Now there are two cases. If we are talking about π-groups, G'_0 is a π-group, H is a π-group, which means if you have any normal π-group, then it is contained in every one. As such, ${}^g H' \subset H$. But this must be equal to H since they have the same cardinality. ☐

7.14 Fusion

7.14.1 Factorization

Suppose we have two subgroups $H, K < G$. Recall the simple observation:

Proposition 7.10. *If $KH < G$, then $KH < G$, and they are equal.*

Proof. This follows from the fact that $(KH)^{-1} = H^{-1}K^{-1}$. ☐

[7.4] Recall that we write $\pi' = \pi(G) \setminus \pi$.

Now suppose that in fact $HK = G$, and define $J \coloneqq K \cap H$. We refer to these H, K as a J factorization. Then consider the single commutators:

$$[G, H]_1 = \{[g, h] \mid g \in G, h \in H\}$$

Recall that this is not the same as the subgroup group $[G, H]$ which is generated by such single commutators. Also recall that we have seen that:

$$[G, H]_1 = [HK, H]_1 \subseteq {}^H [K, H]_1 [H, H]_1$$

so if K is in fact a normal subgroup, then we have:

$${}^H [K, H]_1 [H, H]_1 = \left[{}^H K, H \right]_1 \subseteq [K, H]_1 [H, H]_1 \subseteq K$$

and:

$$\begin{aligned} [G, H]_1 \cap H \subseteq ([K, H]_1 [H, H]_1) \cap H &\subseteq ([K, H] [H, H]) \cap H \\ &= ([K, H] \cap H) [H, H] \end{aligned}$$

Now if we also have that H/J is abelian, then this is the same as saying

$$[H, H] \subset J$$

So we can write:

$$([K, H] \cap H) [H, H] \subset J$$

In other words we have shown:

Proposition 7.11. *Assuming $K \lhd G$, $J \supseteq [H, H]$ we obtain:*

$$[G, H]_1 \cap H \subseteq J$$

So now let $H < G$ and $J \lhd H$, then we look for K such that $J < K$ and $K \lhd G$. If such a K does exist, then this above condition holds. The explicit meaning of this is that for an element $h \in H$, if its conjugate ${}^g h$ in G belongs to H, then ${}^g h = h \bmod J$. That is,

$$J\, {}^g h = Jh$$

We say these two elements are *fused*.

7.14.2 Wielandt's transfer fusion theorem

Recall $\Gamma_{H \backslash G}$, and in particular that this is a left $\mathcal{H}$ torsor. This is of course also a right G-set. Consider this also as a left H-set, where H acts as constant functions. Really this is a $(N_G(H), G)$-biset, but we can just focus on H in this case. So let s be a section, and suppose $C \in H \backslash G$. Then

$$(sg)(Cg) = s(C) g$$

which is equivalent to saying that

$$(sg)(C) := s\left(Cg^{-1}\right)g$$

We also have a left action of $\mathcal{H}$ on $\Gamma_{H\backslash G}$, but this is not quite a $(\mathcal{H}, G)$ biset, since $\chi(sg) \neq (\chi s)g$. To see this, we first write:

$$(\chi s)g = (\chi g)(sg)$$

where χ is a function taking values in H. Then we have that:

$$(\chi g)(C) = \chi\left(Cg^{-1}\right)$$

so the difference is that

$$\chi(sg) = \chi \cdot sg$$

and

$$(\chi s)g = (\chi g)sg$$

so these differ by something of the form $\chi(\chi g)^{-1}$. This is important, because this shows us that the integration is indeed necessary. That is, understanding:

$$(\chi g)(C) = \chi\left(Cg^{-1}\right)$$

leads us to consider the following homomorphism with kernel denoted by $\mathcal{H}_{(J)}$:

$$\begin{tikzcd} \mathcal{H}_{(J)} \arrow[r, tail] & \mathcal{H} \arrow[r, two heads, "\int^{(J)}_{H\backslash G}"] & H/J \end{tikzcd}$$

where we map:

$$\int_{H\backslash G}^{(J)} : \chi \mapsto \prod_{C\in H\backslash G} \chi(C) \mapsto \prod \chi(C) \bmod J$$

This $\mathcal{H}_{(J)}$ is strictly speaking not an (H, G)-biset, but it is a G-invariant normal subgroup of $\mathcal{H}$. This means

$$\left(\Gamma_{H\backslash G}\right)_{\mathcal{H}_{(J)}}$$

inherits a right action by G, and in fact, by construction, this is a left H/J torsor, and a right G-set, and the two actions commute, so this is now an actual biset. The reason is, because the non-commutativity of the two actions is precisely by an element of $\mathcal{H}_{(J)}$.

Next we want to find some formula for how the left H acts. But where does $\underline{\underline{H}}$ map to in H/J under the integral? It won't necessarily be onto, but we do know it will map to the subgroup $|G : H|\, H/J$. In particular under the relatively prime hypothesis, this is onto. Now we have the following theorem:

Theorem 7.11 (Wielandt)**.** *Suppose* $(|G : H|, |H : J|) = 1$. *Then TFAE:*

1. *We have the following diagram:*

$$\begin{tikzcd}
H/J \arrow[r, equal] & H/J \\
H \arrow[u, two heads] \arrow[r, hook] & G \arrow[u, dashed, two heads] \\
J \arrow[u, tail] \arrow[r, hook] & K \arrow[u, dashed, tail]
\end{tikzcd}$$

   This is precisely saying there is a normal K containing J, such that $J = H \cap K$ and $G = KH$.

2. $[G, H]_1 \cap H \subseteq J$

3. *The left and the right actions of H on $\left(\Gamma_{H\backslash G}\right)_{\mathcal{H}_{(J)}}$ are the same.*

Proof. Fix $g \in G$ and take $s \in \Gamma_{H\backslash G}$. Consider the right action of G on $\left(\Gamma_{H\backslash G}\right)_{\mathcal{H}^{(J)}}$. We know g acts on $H\backslash G$, so now let $\mathcal{O} \subset H\backslash G$ be an orbit of the cyclic group $\langle g \rangle$. This will be made up of the following:

$$\left\{C, Cg, \cdots, Cg^{n-1}\right\}$$

where $n = |\mathcal{O}|$ divides $|g|$. Now notice

$$\int_{H\backslash G}^{(J)} \chi = \sum_{\mathcal{O} \subseteq H\backslash G} \int_{\mathcal{O}} \chi$$

These integrals are called *orbital integrals*. Then we are calculating the action of g on s, and comparing this with s itself. We consider the following:

$$s\left(Cg\right) \qquad s\left(Cg^2\right) \qquad \cdots \qquad s\left(Cg^n\right) = s\left(C\right)$$

Now do the same for sg. We can write:

$$sg\left(Cg\right) = s\left(C\right)g \qquad sg\left(Cg^2\right) = s\left(Cg\right)g \qquad \cdots \qquad sg\left(Cg^n\right) = sg\left(C\right)$$

And finally for $sg/s = \chi \in \mathcal{H}$ we calculate:

$$\begin{aligned}
\int_{\mathcal{O}} sg/s &= s\left(C\right)gs\left(Cg\right)^{-1}s\left(Cg\right)gs\left(Cg^2\right)^{-1}s\left(Cg^2\right)gs\left(Cg^3\right)^{-1}\cdots \\
&= s\left(C\right)g^{|\mathcal{O}|}s\left(Cg^n\right)^{-1} = s\left(C\right)g^{|\mathcal{O}|}s\left(C\right)^{-1} \\
&= {}^{s(C)}g^{|\mathcal{O}|}
\end{aligned}$$

Now if $[s]$ is the orbit of s in this set of orbits, then $[sg] = h\left[s\right]$ where

$$h = \prod_{\mathcal{O} \in H\backslash G} \int_{\mathcal{O}} sg/s = \prod_{\mathcal{O}} {}^{s_{\mathcal{O}}}g^{|\mathcal{O}|}$$

What we have done is completely general, so now we consider the implications from the theorem. Assuming the second condition holds, we have that

$$^{s}C\left(h^{|\mathcal{O}|}\right) \in H$$

which implies that this is the same as $h^{|\mathcal{O}|} \bmod J$. That is, modulo J, the orbital twisting has disappeared. And now we find, that the action of s doesn't depend on s, it is just multiplication by some element of H. That is, multiplication by the value of the integral modulo J. In other words, because of this biset condition, we have a homomorphism of groups from $G \to H/J$. Then we have the following diagram:

$$\begin{tikzcd}
K \arrow[r, tail] & G \arrow[r, "\text{transfer}"] & H/J \\
J \arrow[r, tail] & H \arrow[u, hook] \arrow[ur] \arrow[r] & H/J \arrow[u, "|G:H|"']
\end{tikzcd}$$

where the relatively prime condition implies the map $H/J \to H/J$ on the right is an isomorphism. Then the homomorphism $G \to H/J$ is called the transfer homomorphism. Denote the kernel by K. Then because H is a subgroup, and maps onto H/J, with kernel K, it is clear that $J = H \cap K$. We proved existence of such K, which is simply kernel of corresponding integral. □

Exercise 7.14.1. Show that every solvable group has a nilpotent subgroup which normalizes itself, and all such subgroups are conjugate.[7.5]

Definition 7.9. The focal subgroup of H in G is defined as follows:

$$\operatorname{Foc}_G H := \langle [G,H]_1 \cap H \rangle = \left\langle xy^{-1} \,|\, x, y \in H, \exists g \in G \text{ s.t. } gxg^{-1} = y \right\rangle$$

Exercise 7.14.2. Show that we have

$$[H,H] \subset \operatorname{Foc}_G H \subset [G,G] \cap H$$

Or even stricter, that

$$[H,H] \subset \operatorname{Foc}_G H \subset [G,H] \cap H$$

We can do this with bare hands and the transfer fusion theorem. So now, when does the transfer fusion theorem hold for $J = \operatorname{Foc}_G H$? In fact, for every group H, if there is a normal complement modulo $\operatorname{Foc}_G H$, we cannot get a better complement. That is, it cannot avoid the focal group.

Definition 7.10. We define the "fusion subgroup" to be the following kernel:

$$\operatorname{Fus}_G H := \operatorname{Foc}_G H / [H,H] \twoheadleftarrow \operatorname{Foc}_G H \leftarrowtail [H,H]$$

Since this is somehow the group generated by differences in Foc.

[7.5] This is like the Cartan subalgebra of a Lie algebra.

Theorem 7.12 (Alperin)**.** *Let* $P \in \mathrm{Syl}_p(G)$*,* $g \in G$*, and* $A, {}^{g}A \subseteq P$*. Then there exists* $Q_i \in \mathrm{Syl}_p(G)$*,* $1 \leq i \leq n$*, and* $x_i \in N_G(P \cap Q_i)$ *such that:*

1. $g = x_1 \cdots x_n$
2. $P \cap Q_i$ *is a tame intersection of* P *and* Q_i *for each* i*.*
3. $A \subseteq P \cap Q_1$ *and* ${}^{x_1 \cdots x_i}A \subseteq P \cap Q_{i+1}$ *for* $1 \leq i \leq n$*.*

Bibliography

[1] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton landmarks in mathematics and physics, Princeton University Press, 1999.

[2] M. Demazure, *Lectures on p-divisible groups*, Lecture notes in mathematics, Springer, 1972.

[3] M. Demazure and P. Gabriel, *Introduction to algebraic geometry and algebraic groups*, North-Holland Mathematics Studies, Elsevier Science, 1980.

[4] W. Fulton and J. Harris, *Representation theory: A first course*, Graduate Texts in Mathematics, Springer New York, 1991.

[5] L.L. Scott and J.P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, Springer New York, 1996.